İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

KKTC HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

Buğçehan ARIKLI
116692008

Dr. Öğr. Üyesi Mehmet Bedii Kaya

İSTANBUL
2019

KKTC Hukukunda Kişisel Verilerin Korunması

Personal Data Protection Law in TRNC

Buğçehan ARIKLI

116692008

Tez Danışmanı : Dr. Öğr. Üyesi Mehmet Bedii KAYA (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : Doç. Dr. Leyla KESER BERBER (İmza) .....
İstanbul Bilgi Üniversitesi

Doç. Dr. Mesut Serdar ÇEKİN (İmza) .....
Türk-Alman Üniversitesi

Tezin Onaylandığı Tarih : 26/06/2019

Toplam Sayfa Sayısı : .....150.....

Anahtar Kelimeler (Türkçe)

1) Mahremiyet
2) Kişisel Veri
3) Genel Veri Koruma Tüzüğü
4) Kişisel Verilerin Korunması Kanunu
5) Kişisel Verileri Koruma Kurulu

Anahtar Kelimeler (İngilizce)

1) Privacy
2) Personal Data
3) General Data Protection Regulation
4) Personal Data Protection Law
5) Data Protection Authority

ÖNSÖZ

Kişisel Verilerin Korunması ve mahremiyet yüzlerce yıl öncesinden bugüne aktarılan önemli ahlaki erdemlerdir. Günümüz teknolojisinde kişisel verileri korumak, devletlerin en önemli görevlerinden biri haline gelmiştir.

Kişisel verilerin korunması ilkesi, uluslararası sözleşmelerin bir parçasıdır. Uluslararası hukukun bir parçası olma iddiasındaki bütün devletlerin, bu sözleşmeleri imzalamak ve bunu iç hukuklarının bir parçası haline getirmek gibi bir yükümlülükleri vardır. Bugün, Birleşmiş Milletlere kayıtlı devletlerin yarısından fazlası bu konudaki gerekli yasal düzenlemeleri tamamlamışlardır.

Yaşamlarının birçok alanında devlet kurumlarına, özel ve tüzel birçok kuruluşa kişisel ve mahrem sayılabilecek bilgilerini vermek zorunda kalan bireyler, kişisel verilerinin saklanması konusunda ciddi bir tehlike ile karşı karşıyadırlar. Birçok kişi ve ticari kuruluş bu bilgileri kendi çıkar ve amaçları için kullanabilmektedirler. İşte devletin görevi de tam bu noktada başlamaktadır. Devlet, söz konusu kişisel verilerin nasıl toplanacağı, nasıl işleneceği ve nasıl korunacağının belli kurallara göre yapılmasını sağlamak ve yasal güvence altına almakla yükümlüdür.

Avrupa Konseyi'nin 28 Ocak 1981 tarih ve 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" ile 2001 tarihli "Kişisel Verilerin Korunmasına İlişkin Ek Protokol ve bunlara bağlı olarak 95/46/EC sayılı "Kişisel Verilerin Korunması Direktifi" esas alınarak gelişen kişisel verileri koruma konusu ve bunun hukuki altyapısı günümüz dünyasının oldukça önem verdiği konulardan birisidir. Çağdaş bir hukuk devleti olma yolunda emin adımlarla ilerleyen KKTC, 89/2007 Sayılı Kişisel Verileri Koruma Yasası'nı çıkararak hukuk sistemi içerisinde önemli bir eksikliği gidermiştir. Ne var ki; bu yasanın arzulanan ölçüde ihtiyacı karşılayabilmesi için başka bir takım düzenlemelerin de yapılması, örneğin bilişim suçları ile ilgili yasanın derhal çıkarılması şarttır. 89/2007 Sayılı Kişisel Verilerin Korunması Yasası'na destek

olacak Bilişim Suçları Yasa Tasarısı halen Meclis Komitesinde yasalaşmayı beklemektedir. Öte yandan her yasa bir takım tüzük ve yönetmeliklere atıfta bulunur. Gerek 89/2007 sayılı Kişisel Verileri Koruma Yasası, gerekse Bilişim Suçları Yasa Tasarısı ile ilgili tüzük çalışmalarının da bir an evvel tamamlanması gerekmektedir.

Üzülerek belirtmeliyiz ki Kuzey Kıbrıs Türk Cumhuriyeti'nde birçok yasa Meclis Komitelerinde yıllarca beklemekte, Meclis'ten geçirilse dahi yasanın öngördüğü tüzükler hazırlanmadığı için yasa işlevsel hale gelememektedir. Örneğin Yasa'da öngörülen Kişisel Verileri Koruma Kurulu'nun oluşturulması ancak 2019 yılının başında gerçekleşmiştir. Bu durum, Kuzey Kıbrıs Türk Cumhuriyeti'ndeki bürokrasinin ve Meclis çalışmalarının ne kadar hantal bir yapıda olduğunu göstermesi açısından önemli bir göstergedir.

Bu çalışma, alanında KKTC'de yapılmış ilk akademik çalışma olması açısından önem taşımaktadır. Alan çalışmalarında ilk olmanın birçok dezavantajı vardır. Bu dezavantajların en önemlisi yeterli kaynak olmamasıdır.

Bu çalışma bundan sonra bu alanda yapılacak akademik çalışmalara zemin hazırlamanın yanı sıra, kanun koyucuya da veri sağlama açısından oldukça önemlidir.

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
Akt.	: Aktaran
ABAD	: Avrupa Birliği Adalet Divanı
Bknz.:	: Bakınız
BM	: Birleşmiş Milletler
GDPR	: General Data Protection Regulation
KKTC	: Kuzey Kıbrıs Türk Cumhuriyeti
Md.	: Madde
OECD	: Organisation for Economic Cooperation and Developmen (Ekonomik Kalkınma ve İşbirliği Örgütü)
Yasa	: 89/2007 Sayılı Kişisel Verilerin Korunması Yasası

ABSTRACT

The protection of private information and secrets belonging to the person has become a legal responsibility in today's world and this right has been part of many international agreements led by the United Nations, European Council and the European Union.

Prior years many countries have resolved legal, political, technical and social aspects of this issue. However, Turkey and Northern Cyprus ignored this issue for a while and in the TRNC legal basis has been established very recently.

As it is known, the TRNC is an uncontrolled part of the Republic of Cyprus and the EU. During the negotiations in 2004, the state in the Southern part became a member of the European Union. This membership covers the whole island, not merely the South of the Island. However, as stipulated in Article 1 of Protocol No. 12003T / PRO / 10 on Southern Cyprus's conditions for accession to the EU, the application of the acquis will be suspended if the Government of the Republic of Cyprus does not exercise effective control of the territory of Northern Cyprus. Nevertheless, Turkish Cypriot citizens who are eligible for citizenship of the Republic of Cyprus have the rights of EU citizens.

However, in order to be part of the EU, former TRNC Governments have formed a separate Assembly Committee with the aim of harmonizing their laws with the EU. This Committee reviews all legal work and legislation together with the European Union Office operating in the TRNC.

The law on the protection of personal data that a modern state must possess is dealt with in this context and in 2007, the Law on the Protection of Personal Data No. 89/2007 was passed by the Assembly. However, it cannot be said that this law is taken seriously by the Governments and has been rendered operational. In order to

establish the Board stipulated by the Law, the appointment of the Chairman and the Members of the Board was completed only at the beginning of 2019.

In this study, we will look at the legal status of the Law on Protection of Personal Data issued in the TRNC in 2007, and try to compare it with the EU legislation.

Key Words: Privacy, Personal Data, General Data Protection Regulation, Personal Data Protection Law, Data Protection Authority

ÖZET

Mahremiyet adını verdiğimiz kişiye ait özel bilgilerin ve sırların korunması günümüz dünyasında yasal bir sorumluluk haline gelmiş, bu hak Birleşmiş Milletler, Avrupa Konseyi ve Avrupa Birliği'nin başını çektiği birçok uluslararası anlaşmaların da parçası olmuştur.

Dünyanın birçok ülkesinde bu konunun hukuk, siyasi, teknik ve sosyal yönleri yıllar öncesinde çözümlenmişken, kişisel veriler Türkiye ve Kuzey Kıbrıs Türk Cumhuriyeti'nde yeni yeni önemsenmeye başlanmış ve hukuki zemin oluşturulmuştur.

Bilindiği üzere KKTC, AB tarafından "Kıbrıs Cumhuriyeti'nin kontrol edilemeyen bir parçasıdır." AB üyesi Güney Kıbrıs ile KKTC'yi federatif bir çatı altında üniter bir yapıya kavuşturmak için BM gözetiminde sürdürülen müzakereler, 50 yıldan beridir devam etmektedir. Müzakereler sırasında 2004 yılında Güney kısımdaki devlet Avrupa Birliği üyesi olmuştur. Bu üyelik, Ada'nın Güney'ini değil, tüm Ada'yı kapsamaktadır. Ancak Güney Kıbrıs'ın AB'ye katılım şartlarını içeren 12003T/PRO/10 sayılı protokolün 1. maddesi ile belirtildiği üzere, Müktesebatın uygulanması, Kıbrıs Cumhuriyeti Hükümeti'nin Kuzey Kıbrıs topraklarında etkili kontrol uygulamaması durumunda, askıya alınacaktır. Bununla beraber, Kıbrıs Cumhuriyeti vatandaşlığı almaya uygun olan vatandaşlar, AB vatandaşlarının haklarına sahiptir.

KKTC Hükümetleri, müzakereler başarıya ulaşsa da ulaşmasa da AB'nin bir parçası olabilmek için yasalarını AB ile uyumlu hale getirmek maksadı ile Cumhuriyet Meclisi'nde ayrı bir Meclis Komitesi oluşturulmuştur. Bu Komite KKTC'de faaliyetini sürdüren "Avrupa Birliği Ofisi" ile birlikte bütün yasal çalışma ve mevzuatını gözden geçirmektedir.

Çağdaş bir devletin sahip olması gereken kişisel verilerin korunmasına dair yasa da bu çerçevede ele alınmıştır ve 2007 yılında 89/2007 Sayılı Kişisel Verilerin Korunması Yasası Meclis'ten geçirilmiştir. Ne var ki bu Yasa'nın Hükümetler tarafından tam manası ile ciddiye alındığı ve işlerlik kazandırıldığı söylenemez. Öyle ki, Yasa'nın öngördüğü Kurulun oluşturulması için Kurul Başkan ve Üyelerinin atama işlemleri ancak 2019 yılının başında tamamlanmıştır.

Biz bu çalışmada KKTC'de 2007 yılında Cumhuriyet Meclisi'nden çıkarılan Kişisel Verilerin Korunması Yasası'nın yasal durumunu ele alırken, AB mevzuatıyla mukayesesini de yapmaya çalışacağız.

Anahtar Kelimeler: Mahremiyet, Kişisel Veri, Genel Veri Koruma Tüzüğü, Kişisel Verilerin Korunması Kanunu, Kişisel Verileri Koruma Kurulu

GİRİŞ

Sır saklama ve mahremiyet insanlık tarihi kadar eskidir. Geçmişten günümüze, belirli meslek gruplarında mesleki bilgiler ve meslek mensuplarının kişisel bilgileri bir sır olarak saklanmaktaydı. Öyle ki; hekimin sır saklama yükümlülüğü, batı tıbbının kurucusu olarak kabul edilen Hipokrat yemininde dahi yerini almıştı. Osmanlı'da yapılan nüfus sayımları ve bunların işlendiği kütük defterleri arşivlerde tutulmaktaydı ancak; belirli kişiler bunları inceleyebiliyordu. Devletin vatandaşları hakkındaki bilgileri kaydetme geleneği sonraki yıllarda fişleme olarak algılanmaya başlandı. Almanya'nın Nazilere yönelik ırkçı tutumu ve soykırımı Alman devletinin kayıtlarından yola çıkılarak uygulamaya konulmuştu. Nazi Almanya'sında devletin elinde tuttuğu kişisel verilerin kötüye kullanılması; mahremiyetin bir yurttaşlık hakkı olarak Avrupa'da kabul görmesine yol açtı.[1]

Kişisel veri ifadesi; bireyi toplumun diğer üyelerinden ayıran bütün şahsi özellikleri kapsar. Kişisel verilerin bireyin izni ve iradesi dışında, başkaları tarafından bilinip paylaşıldığı bir ortamda kişi hak ve hürriyetinden bahsedilemez. 1960'lı yıllardan itibaren hayatımıza giren bilgisayar teknolojisi hayatı kolaylaştırmanın yanı sıra; kişi hak ve hürriyetleri için çeşitli riskleri de beraberinde getirmiştir. Bilgilerimizi elektronik ortamda sakladığımız ve elektronik ortamda başkalarına gönderdiğimiz durumda, bu bilgilerin üçüncü şahısların eline geçme riskini de göze almış olmaktayız. Bu risk elbette ki elektronik ortamla sınırlı değildir. Geleneksel yöntemlerle kayıt altında tutulan bilgilerimizin de paylaşılma riski de her zaman olmuştur ve olacaktır.

Teknolojinin devlete sağladığı, kişisel verilere daha hızlı ve kolay erişme imkanı; kişisel verilerin korunması konusunu gündeme getirmiştir. Hızla gelişen bilişim teknolojisinin bugün geldiği nokta ve sağladığı veri işleme, eşleştirme ve depolama

[1] Aksoy, H. C. (2008) Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara, s.56.

gibi fonksiyonların, kişisel verilerin toplanması ve işlenmesi için kullanımı, kişisel verilerin korunmasına dair düzenlemelerin yapılmasını zorunlu kılmıştır. Bu düzenlemelerin temel sebebi, bilişim sistemleri kullanılarak kişisel verilerin işlenmesi karşısında, temel hak ve özgürlüklerin, özellikle özel hayatın gizliliğinin korunmasıdır.[2]

Kişisel veri ve bilgilerin artan kapitalizmin doğurduğu rekabet ortamında bireyin rızası olmaksızın elden ele dolaşması ve bireyi potansiyel müşteri olarak gören kötü amaçlı kişi ve kurumların eline geçmesi, kişi hak ve özgürlüklerine zarar verebilmektedir. Bireyin kişisel verilerini kendi rızasıyla devlet ve/veya güvenebileceği kurum ve kuruluşlarla paylaşması olağandır. Bu bilgilerin ilgili kurum ve kuruluşlar tarafından bireyin rızası dışında üçüncü şahıslarla paylaşılması ise korkutucudur ve hayati riskler taşır. Bir devletin vatandaşlarının bilgilerini toplaması, icraatlarında ve planlamalarında bu bilgilerden faydalanması ve istatistik oluşturması elbette önemli ve gereklidir. Bir bankanın müşterilerinin mal varlığı, sermayesi, gelir durumu ve benzeri bilgilerini elinde bulundurması müşteri ilişkileri açısından önem taşısa da bu bilgilerin pazarlama şirketlerinin veya kötü niyetli kişi, kurum ve kuruluşların eline geçmesi etik değildir. Diğer yandan bilginin özgür akışının önüne geçmeden kişisel verilerin ulusal ve uluslararası düzeyde korunmasının nasıl sağlanacağı önemli bir soru işareti oluşturmaktadır. Gelişmekte olan ve her geçen gün yeni ürün ve hizmetler sunmaya devam eden bilişim teknolojilerinin bilgiyi daha hızlı kullanmak, işlemek ve yaymak için yarattığı olanaklar bir taraftan kişisel verilerin üzerindeki tehdidi güçlendirirken, diğer taraftan bireye sağlanan güvencenin etkinliğini de azaltmaktadır.[3]

---

[2] Bük, A. (2015) Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi, Doktora Tezi, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Ankara, s.12.

[3] Küzeci, E. (2010) Kişisel Verilerin Korunması, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı, Ankara. s. 126-127.

Teknolojiyi doğru kullanmak ve bunun için gerekli hukuki, sosyal, siyasal ve teknik altyapıyı hazırlamak, teknolojinin risklerini tamamen ortadan kaldıramasa da sınırlandırma noktasında önem taşır.

Kişisel verilerin korunması; temelde verilerin değil, bu verilerin ilişkili olduğu gerçek kişilerin korunmasını amaçlamaktadır. Bu koruma, kişileri onlar hakkındaki bilgilerin işlenmesinden doğacak zararlardan koruma anlamına gelmektedir. Kişisel verilerin korunması, veri sahiplerinin kişilik hakkının korunması ile bilginin serbest dolaşımı hakkındaki dengenin sağlanması açısından gerekli ve önemlidir.[4]

Tezin Özelliği

Kişisel verilerin korunması meselesi çağdaşlığın bir gereği olarak devletlerin yasal zeminde ele aldığı bir konudur. KKTC de çağdaş ve demokratik bir devlet olduğu iddiasındadır. Bu sebeple, kişisel verileri koruma ile ilgili yasayı 2007 yılında Meclis'ten geçirmiştir. Ne var ki, gerek toplumun bu konuda yasal haklarını bilmemesi ve gerekse devletin hantal bürokratik yapısı nedeniyle Kişisel Verilerin Korunması gibi birçok yasada işlevlik kazandırılamamıştır.

KKTC'de şu anda takriben 20 adet Üniversite, bu Üniversitelerin tamamında Hukuk Fakülteleri, bu Hukuk Fakültelerinden mezun olan binlerce hukukçu bulunmaktadır. Ne yazık ki KKTC'de kişisel verilerin korunmasıyla ilgili şimdiye kadar herhangi bir akademik çalışma yapılmamıştır. Bu çalışma, KKTC'de alanında yapılmış akademik çalışmaların ilki olma özelliği taşımaktadır.

Tezin Önemi;

Bu çalışma KKTC'de sahasında yapılan ilk akademik çalışma olması dolayısıyla bu alanda çalışma yapacak ardıllar için bir kaynak olacaktır. Ayrıca pratikte bu

[4] Aksoy, s.75-77.

konuda yasal haklarını bilmeyen kamuoyu ve devleti yönetenler için de iyi bir başvuru kaynağı olma iddiasındadır. Bu sebeple bu çalışma bize göre oldukça önemlidir.

Metodoloji ve Genel Sınırlamalar

Bu çalışmamızda konu edilen KKTC'deki kişisel verileri korumayla ilgili hukuki ve teknik altyapı çalışmaları yeni başladığı için konu ile ilgili materyaller son derece sınırlıdır. Konu gündeme geldiğinde KKTC kamuoyu, Üniversiteler ve basın yayın organları bu konuya son derece ilgisiz kalmışlardır. İlgili Yasa'nın Meclis'te tartışıldığı dönem ile ilgili yaptığımız taramada basın yayında bu konuyla ilgili herhangi bir görüş serdedilmemesi, kamuoyunun bu konuya ne kadar yabancı ve ilgisiz olduğunu göstermektedir. Bu konuda elimizdeki en önemli materyal Meclis Alt Komitesinde yapılan tartışmalar ile ilgili tutanaklardır. Çıkartılan 89/2007 Sayılı Yasa AB ile uyum yasaları tahtında ele alındığı için, bu Yasa'nın AB mevzuatıyla mukayesesi de bu çalışma açısından önemlidir. Dolayısıyla bu konuyu ele alan makale ve kitaplar önemli kaynaklarımız olacaktır. Öte yandan kişisel verilerin korunması çerçevesinde konuşulan, tartışılan ve ortaya atılan kavramların kapsamı ve hukuki olarak ne anlama geldikleri de yine aynı kaynaklarda incelenecek ve mukayesesi yapılacaktır. Çalışma kapsamında; bu alanda yapılan hukuki çalışmaların zaman içerisinde ortaya çıkardığı eksiklikler de değerlendirilecek ve bu amaçla bazı örnekler incelenecektir.
Çalışmamız KKTC'de kişisel verilerin korunması ile ilgili ilk akademik çalışma olması açısından da önemlidir. Bu nedenle bu konuda çalışma yapacak başka akademisyenlere, siyasilere ve hukukçulara kaynak olması amaçlanmaktadır.

Çalışma Planı

Çalışmada öncelikle kişisel verilerin korunması ile ilgili tarihsel süreç ele alınacak, konuyla ilgili kavramların anlamı, bunların hukuki, sosyal ve siyasal manada ne

anlama geldikleri incelenecektir. Daha sonra tez konumuz olan Kuzey Kıbrıs Türk Cumhuriyeti'nde kişisel verilerin korunması konusunun nasıl ele alındığı incelenerek, bu konudaki yasal çalışma AB mevzuatıyla mukayesesi edilecek ve ilerleyen süreçte Yasa'da çeşitli değişiklikler yapılması halinde bu değişikliklerin hangi alanlarda ve ne şekilde olması gerektiği konusu değerlendirilecektir. Çalışmamızın son bölümünde ise KKTC Cumhuriyet Meclisi'nden geçen 89/2007 Sayılı Yasa'nın uygulanıp uygulanmadığı, ihtiyaca cevap verip vermediği konuları ele alınacaktır.

I. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI ALANINDA ULUSAL VE ULUSLARARASI DÜZENLEMELER

1.1. Kişisel Verilerin Korunmasına Dair Ulusal Düzenlemeler

Kişisel verilerin korunması hususunda yapılan hukuki düzenlemeler, 1960'lı yıllarda otomatik veri işleme teknolojilerinin gelişmesiyle tartışılmaya başlanmıştır.[5] Hızla gelişmekte olan bilgisayar teknolojilerine karşı kişilerin yaşam ilişkilerini koruma ve oluşabilecek tehditlere yönelik sorunlar ilk defa 1960'lı yıllarda ABD'de tartışılmaya başlanmıştır. 1974 yılında özel hayatın güvence altına alınması için idareye yükümlülükler getiren Özel Yaşamın Gizliliği Kanunu (Privacy Act) kabul edilmiştir.[6]

ABD ile eşzamanlı olarak Avrupa'da da 1960'lı yılların sonunda, bilim ve teknolojinin gelişiminin artması sonrasında özel hayatın gizliliğine gelen tehditler nedeniyle kişisel verilerin korunmasına yönelik düzenlemeler başlamıştır.[7] Kişisel verilerin korunması hususunda Avrupa'daki ilk düzenleme 1970 yılında Almanya'nın Hessen Eyaleti'nde yapılmıştır.[8] Bu kanunun kabul edilmesindeki en önemli etken 1960'lı yılların sonunda federe düzeyde merkezi bir veri bankasının kurulması tasarısını içeren "Hessen Planı" adlı bir programdır. Kurulacak veri

---

[5] Küzeci, s. 106.

[6] Şimşek, O. (2008) *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul, Beta Basım, s. 7.

[7] Akgül, A. (2013) Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu Ve Yargısal Denetimi, Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, İzmit, s.31.

[8] Öztürk, B., Altınok, Ç, E. (2018) Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu, *Fasikül Hukuk Dergisi*, (100), s.279; Küzeci, s. 116; Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum. *Uyuşmazlık Mahkemesi Dergisi*, (3), s.11; Tekin, N. (2014). Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirmesi. *Uyuşmazlık Mahkemesi Dergisi*, (4), s.224.

bankasının özel hayatın gizliliği hakkı üzerindeki olası etkisinin veri korunmasına dair hükümlerin yasalaşmasında etkili olduğu söylenebilir.[9]

Artan tartışmalar ve Hessen eyaletinin verilerin korunmasına dair yapmış olduğu düzenleme, kısa bir sürenin ardından Almanya'da federal seviyede bir koruma öngörülmesini sağlamış ve 1977 yılında "Federal Almanya Veri Koruma Yasası" kabul edilmiştir.[10] Hessen eyaletinde kabul edilen yasadan sonra ilk ulusal düzenleme ise 1973 yılında İsveç'te yapılan Veri Koruma Kanunu'dur.[11] Bu düzenlemelerin yanında Amerika Birleşik Devletleri'nde "Özel Yaşamın Gizliliği Kanunu"(1974), Fransa'da "Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına İlişkin Fransız Kanunu"(1978) da çıkarılmıştır. 1980 yılının başlarında ise İngiltere, İrlanda ve İtalya dışında Avrupa Ekonomik Topluluğu'nun bütün üyeleri de bu konuda yasa çıkarmış ya da hazırlık yapmıştır.[12]

1.2. Kişisel Verilerin Korunmasına Dair Uluslararası Düzenlemeler

İnsan haklarının gelişimi, kişi haklarının korunmasını en üstün değer haline getirmiş ve böylece ulusal ve uluslararası hukukta ortak amaç haline gelmiştir.[13] Zira, her geçen gün sanal ve gerçek iletişim ağları ile birbirine bağlanan dünyada, bilginin hızlı akması sınır tanımaz hale gelmiş bulunmaktadır.[14] Sadece bir ülkenin kendi iç hukukuyla kişisel verileri koruyabilmesinin ve bu konudaki sorunların çözümünün zor olması[15] hususu, etkin korumanın ancak küresel düzeyde kabul edilecek bir veri koruma sisteminin oluşturulması ihtiyacını doğurmuştur.[16] Bu

---

[9] Küzeci, s. 118. Bu dönem Almanya'da devlet organlarınca çeşitli amaçlar doğrultusunda, bilgisayar sistemlerinin artan oranda kullanılmaya başlandığı görülür. Bunun en bilinen ve en çok tartışılmış örneklerinden biri, Bavyera eyalet yönetiminin, 1972 yılında Münih'te yapılan olimpiyatlar için kurmuş olduğu bilgisayar sistemini, daha sonra merkezi Bavyera bilgi sistemi olarak kullanmak istemesidir; Küzeci, s. 118.

[10] Küzeci, s. 118.

[11] Akgül, s.111.

[12] Küzeci, s. 108.

[13] Akgül, s.112.

[14] Küzeci, s. 123.

[15] Şimşek, s. 12.

[16] Küzeci, s. 124.

ihtiyaçtan hareketle Birleşmiş Milletler, Avrupa Konseyi, OECD, Avrupa Birliği gibi etkili uluslararası örgüt veya kuruluşlar, bir süredir gündemlerinde bulunan kişisel verilerin korunması konusuna ve özellikle kişisel verilerin uluslararası aktarımına dair kuralları art arta hayata geçirmişlerdir.[17] Bu örgüt veya kuruluşların amacı, hedef ve ihtiyaçlar ile uyumlu şekilde rehber ilkeler ve düzenlemeler yayınlanmasıdır.[18]

Bu amaca örnek olan AB bilgi politikaları, toplumu bilgi ile buluşturacak yöntemleri geliştirmeyi amaçlamaktadır. Bu sebeple bilgi kaynakları, bilgi sistemleri, bilgi altyapısı ve bilgi hizmetlerine dair bütün alanlarda iyileştirme, geliştirme çalışmaları hızlandırılmıştır. Çevrimiçi ekonominin canlandırılmasına duyulan ihtiyaç bu hedefin belirlenmesine etken olsa da toplum içerisinde e-ticaret kullanıcılarının internet üzerinden kişisel verilerini sunmalarından kaynaklanan kaygıların günden güne artması, 1990'lı yıllardan itibaren bilgi politikaları içerisinde kişisel verilerin korunmasına yönelik çalışmaların hızlanmasına sebep olmuştur. Bu çalışmalar arasında veri koruma direktifleri, uluslararası sözleşmeler, tavsiye kararları, denetimin sağlanması maksadıyla kurulan kuruluşlar yer almaktadır.[19]

Kişisel verilerin korunması hukukunun normatif temeli sayılan özel hayatın gizliliği hakkı, birçok önemli insan hakları metninde yer verilerek güvence altına alınmıştır. Bu metinlerde ilk akla gelenler BM Evrensel İnsan Hakları Bildirisi, BM Uluslararası ve Siyasal Haklar Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi'dir. Bu metinlerde yer alarak güvence altına alınmış özel hayatın gizliliği hakkının kişisel verilerin korunmasının hedef ve prensipleriyle yakından ilişkisi bulunmaktadır.[20]

---

[17] Küzeci, s. 123.
[18] Akgül, s.112.
[19] Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği*, 27(3), 451-471.
[20] Küzeci, s. 128.

1.2.1. Birleşmiş Milletler Mevzuatı

Birleşmiş Milletler, 2. Dünya Savaşı'nın bitiminde uluslararası barışın ve güvenliğin sağlanması,[21] uluslararası alanda işbirliğinin sağlanması,[22] insan haklarının koruma altına alınması maksadıyla 51 ülke tarafından 24 Ekim 1945 tarihinde kurulmuştur.[23] 2018 itibarıyla BM üyesi 192 üye ülke bulunmaktadır.[24] Türkiye kurucu üyelerinden olup, Güney Kıbrıs Rum Yönetimi ise 20 Eylül 1960 tarihinde Birleşmiş Milletlere üye olmuştur. Birleşmiş Milletler de veri koruma hukuku konusunda etkinlikleri olan uluslararası mercilerdendir.[25] Birleşmiş Milletler, bir üst hukuk normu olarak çalıştığı Birleşmiş Milletler İnsan Hakları Beyannamesini,[26] globalleşen dünyada bir standart olarak sunmuş ve bunu yaygınlaştırarak incelediği konularla hükümetlerin ve insanların gündem konularını belirlemekte önemli bir aktör haline gelmiş bir örgüttür.[27]

Bu beyannamenin 12. maddesi ile bireylerin mahremiyet, aile ve konut dokunulmazlığı koruma altına alınmış ve bu haklara dokunacak olası saldırılarda bireylerin hukuki korumadan yararlanma hakları hükme bağlanmıştır;[28] "Hiç kimse özel hayatı, ailesi, konutu veya haberleşmesi hususlarında keyfi müdahalelere, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu müdahale ve tecavüzlere karşı kanun ile korunmaya hakkı vardır. BM'nin 16 Aralık 1966 tarihli Bireysel ve Siyasal Haklar Hakkındaki Uluslararası Sözleşme'nin 17. maddesi de hemen hemen aynı koruma hükmüne yer vermiştir.[29]

---

[21] Çalık, T. (2015) Birleşmiş Milletler Organlarının İnsan Hakları ile İlişkisi, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 2, s.1091.
[22] Pazarcı, H. (2018) *Uluslararası Hukuk*, 17. Baskı, Turhan Kitabevi, Ankara, s.190.
[23] Çalık, s.1091.
[24] Birleşmiş Milletler, Birleşmiş Milletler Türkiye'nin refahı için Türkiye ile birlikte çalışıyor: <http://www.un.org.tr/bm-turkiye-kuruluslari/> son erişim 30.03.2019.
[25] Civelek, D. Y. (2011), Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Uzmanlık Tezi, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi Başkanlığı, Ankara, s. 68.
[26] Civelek, s. 68.
[27] Boz, A. (2014), Kişisel Verilerin Korunması: Türkiye, ABD ve AB örnekleri, Yüksek Lisans Tezi, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Ankara, s.55.
[28] Civelek, s. 68.
[29] Civelek, s. 68.

BM'nin kabul ettiği genel nitelikteki insan hakları metinlerini içeren sair düzenlemelerinin yanında, örgütün doğrudan kişisel verileri koruma hususunda bazı girişimleri de bulunmaktadır. Bu çerçevede 14 Aralık 1990 tarihinde BM Genel Kurulu 45/95 sayılı kararı ile "Bilgisayara İşlenen Kişisel Veri Dosyaları Hakkında Rehber İlkeler" yayınlamıştır.[30] BM'nin kişisel verilerin korunması konusunda yapmış olduğu ilk düzenlemesinde bilgisayarların aracı olarak kullanılmasının sebebi, teknolojinin kişisel verileri işlemedeki etkisidir denilebilir.[31] BM tarafından hazırlanan rehber ilkeler, üye ülkelerin bilgisayar aracılığıyla kişisel veri işlenmesi hususunda yapılacak olan düzenlemelerle birlikte dikkate alınacaktır, fakat bu ilkelerin uygulama usulleri devletlerin inisiyatifine bırakılmıştır.[32] Sözü geçen rehber ilkeler[33] şu şekildedir;

1- Yasallık ve Dürüstlük
2- Doğruluk
3- Amacın Belirli ve Haklı Olması
4- İlgili Kişilerin Erişme Hakkı
5- Ayrımcılıktan Kaçınma
6- İstisna Koyma Yetkisi
7- Güvenlik
8- Denetim ve Yaptırım
9- Sınır Ötesi Veri Aktarımı

---

[30] Dinkci, F. (2014) Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği, Ondokuz Mayıs Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Samsun, s. 23.
[31] Boz, s.55.
[32] Civelek, s. 68.
[33] Aydın, S. E. (2014) AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Sucu, Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul, s.23-24; Uygun, M. (2010) Avrupa Birliği'nin 95/46 sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, TC. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara, s.28-29.

1.2.2. Avrupa Konseyi Mevzuatı

Avrupa Konseyi, 2. Dünya Savaşı'ndan önemli ölçüde maddi ve manevi kayıplarla çıkan Avrupa'da oluşan parçalanmışlığın ve savaşla ortaya çıkan çatışma atmosferinin ortadan kaldırılması ve ortak kurumlar, standartlar ve sözleşmelere dayanan, güven ve işbirliği ortamının kurulması maksadıyla başlatılan çalışmaların sonucunda 10 Avrupa ülkesi tarafından 5 Mayıs 1949 tarihinde Londra'da imzalanarak kurulmuştur.[34] Konsey, Güney Kıbrıs Rum Yönetimi ve Türkiye'nin de üyesi olduğu, hükümetler arası bir örgüttür.

Konsey'in 2018 tarihi itibariyle 47 üyesi bulunmaktadır. Konseyin başlıca amacı hukukun üstünlüğü, insan hakları, çoğulcu demokrasi prensiplerini savunmak ve güçlendirmektir.[35]Avrupa Konseyi bu doğrultuda, 4 Kasım 1950 tarihinde Avrupa İnsan Hakları Sözleşmesi'ni kabul etmiştir. Bu sözleşme çerçevesinde kurulan Avrupa İnsan Hakları Mahkemesi, konsey bünyesinde faaliyet gösteren ve finanse edilen, uluslararası boyutta hukuksal koruma organıdır.[36]

Bunun yanında Avrupa Konseyi, kişisel verilerin korunması konusunda önemli çalışmalar yapan uluslararası bir kuruluş olarak karşımıza çıkmaktadır.[37] Konsey'in bu yönde yapılan en önemli çalışması 1981 yılında kabul edilen 108 Sayılı "Kişisel Nitelikli Verilerin Otomatik İşleme Tabi tutulması Karşısında Bireyleri Korunmasına Dair Sözleşme"dir.[38] 1995 ve 2001 yıllarında yürürlüğe giren 95/46/EC ve 2002/58/EC Sayılı direktifler, bu sözleşmeyi tamamlar niteliktedirler.[39]

---

[34] Dinkci, s.46.
[35] T.C Dışişleri Bakanlığı (2011) Avrupa Konseyi: <http://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa> son erişim 30.03.2019.
[36] Dinkci, s. 26.
[37] Dinkci, s. 25.
[38] Dinkci, s. 27.
[39] Henkoğlu, T. (2015), Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler için Bilgi Güvenliği Politikasının Geliştirilmesi, Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, Ankara, s. 44.

Konsey, 8 Kasım 2001 tarihinde 108 Sayılı sözleşmeye ek olarak 181 Sayılı "Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol'u kabul etmiştir.[40]

Avrupa Konseyi, verilerin korunmasının çerçevesini çizen bu Sözleşmeler yanında, ilerleyen yıllarda veri korumasının kurallarını sektörel bazda ele almış olduğu çeşitli tavsiye kararlarını da kabul etmiştir. "Tıbbi veri bankaları (1981), bilimsel araştırma ve istatistik (1983), doğrudan pazarlama (1985), sosyal güvenlik (1986), elektronik ödeme ve diğer işlemler (1990), verilerin kamu kuruluşlarınca üçüncü kişilere açıklanması (1991), kişisel verilerin telekomünikasyon alanında korunması (1995), tıbbi verilerin korunması (1997), internette özel hayatın gizliliğinin korunması (1999)" bu kurallardan bazılarıdır. Konsey üyesi gelişmiş devletlerin çoğu, özel yasaları olduğu halde, sayılan tavsiye kararları takiben konuları sektör bazında yeniden gözden geçirmiş ve düzenlemişlerdir.[41]

Konsey, 2018 yılında gelişen teknoloji ile kişisel verilerin işlenmesi karşısında bireylerin korunmasının zorlaşması nedeniyle 108 Sayılı Sözleşme'yi yenilemiş ve Sözleşme 108+ olarak anılan "The Modernised Convention 108" kabul edilmiştir. Kişisel verileri koruma konusunda oldukça önemli olan bu Sözleşmeler aşağıda incelenmektedir.

1.2.2.a 108 Sayılı Sözleşme (Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi)

108 Sayılı Sözleşme, Avrupa'da kişisel verilerin korunması konusuna ilişkin ilk uluslararası hukuk belgesidir.[42] Avrupa İnsan hakları Sözleşmesi'nde kişisel verilerin korunması hakkı bağımsız bir hak olarak yer almadığından, bu hakka 108

[40] Henkoğlu, s. 63.
[41] Civelek, s. 63.
[42] Başalp, N. (2004), Kişisel Verilerin Korunması ve Saklanması, Ankara, Yetkin Yayınları, s.24.

Sayılı Sözleşme'de yer verilmiş ve bu boşluk giderilmek istenmiştir.[43] 1 Ekim 1985 yılında yürürlüğe girmiş olan 108 Sayılı Sözleşme, kişisel verileri koruma alanında kabul edilmiş bağlayıcılığı olan ilk uluslararası belge olarak önem teşkil etmektedir.[44]

Sözleşmenin temel amacı; Avrupa Konseyi'ne üye olan her ülkede, uyruğu veya ikametgahı fark etmeksizin gerçek kişilerin, temel hak ve özgürlüklerini, özellikle kendilerini ilgilendiren kişisel mahiyetteki verilerin otomatik yollarla işleme tabi tutulması karşısında özel hayat haklarını güvence altına almaktır.[45] Sözleşme, kişisel verilerin tamamının veya bir kısmının otomatik yollarla kaydı[46], kişisel verilerin kullanılması ve depolanması[47], verilerin değiştirilmesi, silinmesi gibi işlemler karşısında bireyleri korumayı[48], bireylerin başkaları tarafından toplanmış olan verileri üzerinde kontrolünün sağlanmasını amaçlar.[49]

Sözleşme'ye Konsey üyesi bütün ülkeler ve Konsey dışından Uruguay olmak üzere toplam 47 ülke taraf olmuş, 46 ülke tarafından onaylanmıştır. Sözleşme'nin 4. maddesi Sözleşme'nin onaylanabilmesi için imzalayan devletlerin sözleşmede öngörülmüş olan ilkeler çerçevesinde bir yasayı kabul etmelerini zorunlu kılmıştır. Türkiye ise Sözleşme'yi imzalamış olmasına rağmen, uzun süre onay işlemlerini tamamlamadığından yürürlüğe koymayan tek ülke olmuştur.[50] Türkiye, Sözleşme'yi 17 Mart 2016 tarihinde yürürlüğe koyarak iç hukukuna dahil etmiştir.[51]

---

[43] Şimşek, s.21.
[44] Atak, S. (2010) Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, *TBB Dergisi*, 87, s.90.
[45] Kişisel Verileri Koruma Kurumu (2018) Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler: <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler> son erişim 08.03.2019.
[46] Civelek, s. 64.
[47] Oğuz, s.8.
[48] Civelek, s. 64.
[49] Oğuz, s.8.
[50] T.C Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü (2015) 31853594-101-30-3870 Sayılı Kanun Tasarısı: <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf> son erişim 28.03.2019.
[51] Kişisel Verileri Koruma Kurumu (2018) Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler:

1.2.2.b. 181 Sayılı Ek Protokol (Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol)

Ek Protokol 8 Kasım 2001 tarihinde imzaya açılmış ve ilk olarak Güney Kıbrıs Rum Yönetimi, Çek Cumhuriyeti, Almanya, Litvanya, Slovakya ve İsveç'in onaylamasıyla birlikte 1 Temmuz 2004 yılında ise yürürlüğe girmiştir.[52] Bu Ek Protokol'ün amacı, 108 Sayılı Sözleşme'nin geliştirilmesi, kişisel verileri ve mahremiyeti daha üst noktada koruma altına almak, başka bir ülkeye veri aktarılmasının standardizasyonu ve bağımsız bir denetleme otoritesinin oluşturulmasını sağlamaktır.[53] Bu Ek Protokol'de taraf devletler, ülkelerinde kişisel verilerin korunması konusunda görevlerini tam bağımsız yerine getirecek denetleyici bir otorite kurmayı taahhüt etmişlerdir.[54] 181 Sayılı Ek Protokol'e taraf olan ülkelerde kurulacak olan denetleyici otoriteler, özellikle araştırma ve soruşturma yapma, kişisel veri mahremiyetinin ihlal edildiği durumlarda yetkili yargı merciinin gündemine getirme yetkileriyle donatılmalıdır. Ayrıca otoriteler, kişisel verilerin işlenmesi konusundaki iddia ve itirazlara bakacak, bununla birlikte bu otoritelerin verdikleri kararlara karşı mahkemelere başvuru hakkı da saklı kalacaktır.[55]

Bu Sözleşme'ye taraf olmayan ülkelere kişilere ait veriler aktarılırken, o ülkede yeterli koruma düzeyinin olması gerekmektedir. Kişisel verilerin sınır ötesi aktarımı, veri sahibinin yararına olması, kamu yararı veya meşru bir yararın olması durumunda kolaylaştırılmalıdır.[56] 181 Sayılı Ek Protokol'ün onaylanmasının ön

---

<https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler> son erişim 08.03.2019.

[52] Boz, s.51.

[53] Henkoğlu, s. 160.

[54] Kişisel Verileri Koruma Kurumu (2018) Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler: <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler> son erişim 08.03.2019.

[55] Civelek, s. 66.

[56] Civelek, s. 66.

şartı, 108 Sayılı Sözleşme'nin de onaylanmasıdır.[57] Türkiye, 181 Sayılı Ek Protokolü 5 Mayıs 2016 tarihinde iç hukukuna dahil etmiştir.[58]

1.2.2.c. 185 Sayılı Siber Suç Sözleşmesi

Ceza yasaları başta olmak üzere ulusal yasalar, genel olarak yalnızca ülke sınırları içerisinde uygulanabilmektedir. Bu kurala *yasaların ülkeselliği (territoriality) ilkesi* denilmektedir. Halbuki siber uzayda işlenen herhangi bir suçun hangi ülkede işlenmiş olduğunun belirlenebilmesi için bir takım hukuksal tanımlar ve kabullerin yapılması ve bunların üzerinde anlaşılmış olması gerekmektedir. Siber uzayda işlenen suçların çoğunda suçun işlenmiş olduğu yer ile suçlunun yaşamakta olduğu ve vatandaşı olduğu ülkeler farklı olmaktadır. Bu suçun kimin tarafından işlendiği, nerede işlendiği ve sonuçlarının nerede etkili olduğunun saptanması büyük ölçüde mümkün olmakla birlikte, bu saptamanın yapılabilmesi için ilgili ülkelerin işbirliği yapmaları ihtiyacı ortaya çıkabilmektedir.[59]

Bu doğrultuda, 185 Sayılı Siber Suç Sözleşmesi, 23 Kasım 2001 tarihinde imzaya açılmış,[60] 1 Temmuz 2004 tarihinde ise yürürlüğe girmiştir.[61] Bu sözleşme ile "toplumun siber suçlara karşı korunması için atılacak diğer adımlarla birlikte gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yollarıyla ortak bir cezai politikanın öncelikli olarak kabul edilmesi" hedeflenmiştir.[62]

185 Sayılı Sözleşme hükümlerinin somut olaylarda uygulanabilmesi büyük ölçüde kişisel veriler ile bağlantılı olduğundan, kişisel verilerin işlenmesinde kişi haklarına

---

[57] Henkoğlu, s. 44.
[58] Kişisel Verileri Koruma Kurumu (2018) Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler: <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler>
[59] Civelek, s. 67.
[60] Civelek, s. 67.
[61] Küzeci, s. 140.
[62] Küzeci, s. 140.

dikkat edilmesi önemli gerekliliklerdendir. Bu sebeple özellikle amaç ile fiil arasında kurulan dengenin, başka bir deyişle orantılılığın ve amaç ile sınırlı olunmasının sağlanması, soruşturulan etkinlik ile bağlantısı olmayan üçüncü kişilerin haklarının korunması gibi hususlara dikkat edilmelidir.[63] Türkiye 185 Sayılı Siber Suç Sözleşmesi'ni 10 Kasım 2010 tarihinde imzalayarak sözleşmeye taraf olmuştur.[64]

185 Sayılı sözleşme sonrasında 28 Ocak 2003 tarihinde, 185 Sayılı Sözleşme'ye eklenen 189 Sayılı bir protokol ile siber alanda ırkçılık ve yabancı düşmanlığı ile mücadele edilmesi hedeflenmiştir.[65]

1.2.2.d. 108 Sayılı Sözleşmeyi Yenileyen Protokol (108+)

Yukarıda değinmiş olduğumuz 108 Sayılı Sözleşme'nin 1980 yılında kabul edilmesinden günümüze değin gelişen bilgi ve iletişim teknolojilerinin kişisel verilerin işlenmesinde bireylerin korunmasına yönelik ortaya çıkardığı zorluklar neticesinde bu sözleşmenin yenilenmesi ihtiyacı doğmuştur. 108 Sayılı Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması Sözleşmesi'ni yenileyen Protokol (CETS No.223) 2018 yılında Avrupa Konseyi tarafından kabul edilmiştir. Bu hususta Avrupa Birliği tarafından 2016 yılında kabul edilip 2018 yılında yürürlüğe giren GDPR'ın da etkisi olduğu görülmektedir.

Sözleşme'yi yenileyen Protokol, taraf olan devletlerin yargı yetkileri altında, hem otomatik hem de otomatik olmayan yöntemlerle kişisel verilerin işlenmesini kapsamaktadır. Protokol, kişisel verilerin kullanılmasında etkin önlemler sağlanırken, sınır ötesi veri akışının kolaylaştırılması için güçlü ve esnek yapıda çok taraflı yasal bir çerçeve sunmaktadır. Bu özelliğiyle de Protokol'ün dünyanın farklı bölgelerinde bir köprü oluşturması ve sınır ötesi veri akışında 108 Sayılı

---

[63] Küzeci, s. 140.
[64] Civelek, s. 67.
[65] 189 numaralı ek protokol 1 Mart 2006'da yürürlüğe girmiştir; Küzeci, s. 140.

Sözleşme'ye atıfta bulunan GDPR da dahil olmak üzere farklı normatif çerçeveler oluşturmaktadır.

Protokol'ün getirdiği bazı yenilikler ise şu şekildedir;

1. Verilerin işlenmesinde orantılı, sınırlı sayıda ve yasal işleme nedenleri ile ilgili daha güçlü gereksinimlerin varlığının aranmasını getirmiştir.
2. Hassas veri tanımı genişletilerek genetik ve biyometrik data, sendika üyeliği ve etnik köken gibi veriler de tanım kapsamına alınmıştır.
3. Veri ihlallerini bildirme yükümlülüğü getirilmiştir.
4. Veri işlenmesinde daha fazla şeffaflık aranacaktır.
5. Özellikle yapay zekanın gelişimi ile birlikte kişilere algoritmik karar konusunda yeni haklar getirmiştir.
6. Kontrolörlerin hesap verebilirliği güçlendirilmiştir.
7. "Tasarım yoluyla gizlilik" yani "privacy by design" ilkesinin uygulanması gerekliliği getirilmiştir.
8. Sınır ötesi veri akışı net düzenlenmiştir.
9. Veri koruma otoritelerinin yetkileri ve bağımsızlığı güçlendirilmiş ve uluslararası yasal dayanaklar artırılmıştır.
10. Ulusal güvenlik nedenleri, Sözleşme'nin öngördüğü şartların olası istisnalar ve kısıtlamalara tabi olması ve herhangi bir bağımsız ve etkili inceleme ve denetleme olması halleri dahil veri koruma ilkelerinin tüm işleme faaliyetlerine uygulanması

Sözleşme'yi Avrupa Konseyi üyesi olmayan ülkeler de imzalayabilmektedir. Güney Kıbrıs 09.01.2019 tarihinde Sözleşme'yi imzalayarak taraf olmuştur, Türkiye ise Sözleşme'yi henüz imzalamamıştır.[66]

1.2.3. OECD Mevzuatı

OECD, 14 Aralık 1960 tarihinde Paris'te imza edilen bir sözleşme ile kurulmuş ve 30 Eylül 1961 tarihinde yürürlüğe girmiş olan[67] ve OECC (Organization for European Economic Co-Operation/Avrupa Ekonomik İşbirliği Örgütü)'nün yerini alıp batılı tüm sanayileşmiş ülkeleri bir çatı altına getiren tek uluslararası kuruluştur.[68] 1961 yılında kurulmuş olan OECD'nin, ekonomik büyümeyi destekleme, iş alanlarını artırma, hayat standartlarını yükseltme, finansal dengeyi koruma, diğer devletlerin ekonomik gelişimine yardımcı olma, küresel ticaretin büyümesine katkı sağlama, demokrasiye ve pazar ekonomisine bağlı devletleri bir araya getirme gibi ana hedefleri bulunmaktadır. Kişisel verilerin korunması hususunu uluslararası bir konu olarak görülmesi yolunda ilk adımı OECD atmıştır.[69]

1980 yılında OECD tarafından "Özel Hayatın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeleri" kabul edilmiştir. Rehber İlkelerin kabulü, kişisel verilerin korunmasında ekonomik boyutun önemli olmasının işareti olarak da değerlendirilebilir.[70]

---

[66] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.
[67] Devlet Planlama Teşkilatı (2000), Sekizinci Beş Yıllık Kalkınma Planı: Türkiye'nin Dış Ekonomik İlişkileri Özel İhtisas Raporu:
< http://www.sbb.gov.tr/wp-content/uploads/2018/11/08_TurkiyeninDisEkonomikiliskileri.pdf>
son erişim 07.04.2019.
[68] Rıdvan, K. (2014) *Küreselleşen Dünyada Uluslararası Kuruluşlar*, İstanbul, Beta Basım Yayım, s.47.
[69] Küzeci, s. 130.
[70] Küzeci, s. 130.

OECD rehber ilkeleri üyeleri bakımından bir bağlayıcılığı olmayan[71], hukuksal açıdan tavsiye niteliği taşıyan[72] ve ulusal düzeyde veri koruma yasalarının birbiriyle uyumlaştırılmasını amaçlayan ilkelerdir.[73] Bu sebeple üye devletleri bu ilkeleri iç hukuklarına dahil edip etmemekte serbesttir.[74]

OECD Rehber İlkeleri, kişisel verileri her çeşit yerel bilgisayar ağından karmaşık ulusal ve uluslararası ağlara dayanan geniş bir alanda işlenmesi durumlarına dair bir içeriği barındırmakta, aynı zamanda da küresel ağlarda özel hayatın gizliliğinin korunmasına ilişkin temel belge olarak görülmektedir. Bu ilkeler, kişisel verilerin toplanması ve yönetilmesine ilişkin teknolojik gelişmeleri yakalayabilecek esnekliktedir.[75]

OECD tarafından kabul edilen ilkeler şunlardır;

1. Sınırlı veri toplama ilkesi
2. Veri kalitesi ilkesi
3. Amacın belirli olması ilkesi
4. Sınırlı kullanım ilkesi
5. Güvenlik ilkesi
6. Şeffaflık ilkesi
7. Bireyin katılımı ilkesi
8. Sorumluluk ilkesi

OECD Konseyi, üye devletlerin kişisel verilerin korunması ve temel hak ve özgürlüklerle ilgili bu ilkeleri kendi iç hukuklarında yapılacak düzenlemelerde dikkate almaları gerektiğini, sınır ötesi veri paylaşımının haksız yere engellenmemesini, var olan engellerin kaldırılmasını, bu ilkelerin hayata geçirilmesinde üyeler arası işbirliği yapılmasını tavsiye etmektedir. Üye devletlerin

---

[71] Aksoy, s.6.
[72] Küzeci, s. 130.
[73] Aksoy, s.6.
[74] Küzeci, s. 130.
[75] Civelek, s.61.

kişisel verilerin korunmasını koruma altına almak için en azından bu ilkeleri benimsemeleri gerektiği belirtilmektedir.[76] Sayılan ilkeler ile uluslararası belgede veri korumanın genel çerçevesi çizilmiştir.[77] 2013 yılında ise ilkeler "2013 OECD Gizlilik Kuralları" olarak yeniden düzenlenmiştir.[78]

1.2.4. Avrupa Birliği Mevzuatı

Avrupa Birliği, 2. Dünya Savaşı'ndan sonra Avrupa'da demokrasi, insan hakları, temel hak ve hürriyetlere saygı temeli üzerine kurulmuş,[79] teknolojinin gelişimiyle geleceğin bilgi toplumunda yeni politikaları ve düzenlemeleri ile öncü olmak istemektedir.[80]

Kuruluş yıllarında yalnızca 6 üyeden oluşan Avrupa Toplulukları[81], çeşitli tarihlerde yeni üyelerin katılımı ile 2013 yılında Hırvatistan'ın katılımıyla 23 üyeden oluşan bir birlik haline gelmiştir. Güney Kıbrıs Rum Yönetimi 2004 tarihinde Kıbrıs Cumhuriyeti adı ile birlik üyelerinden olmuştur.[82] Türkiye ise birliğe katılım müzakerelerini sürdürmektedir.[83]

---

[76] Küzeci, s. 130.
[77] Boz, s.45.
[78] Oğuz, s.8.
[79] Aydın, S.30.
[80] Civelek, s. 70.
[81] Boz, s.58.
[82] Kıbrıs Cumhuriyeti'nin AB'ne dahil olmasından kısa bir zaman önce nihai hale getirilen Kıbrıs sorunu için çözüm planı 24 Nisan 2004 tarihinde GKRY ve KKTC'nde referandumlarla Kıbrıs'taki iki halkın onayına sunulmuştur. Rum halkının %75,83'ü Planı reddederken, Kıbrıs Türk tarafı kendileri için getireceği pek çok zorluğa rağmen %64,91 çoğunlukla Plan'a "evet" demiştir. Rum tarafının Plan'ı büyük bir çoğunlukla reddetmesinde GKRY lideri Papadopulos'un 7 Nisan 2004 tarihindeki halka seslenişinde Rum halkını "güçlü bir hayır" demeye çağırması ve Rum liderliğinin devlet eliyle sürdürdüğü "hayır kampanyası" da önemli bir etki yapmıştır. Sonuçta, Rum toplumunun reddi karşısında, BM ve AB dahil tüm uluslararası camianın desteklediği bu kapsamlı çözüm planı geçersiz hale gelmiştir; T.C Dışişleri Bakanlığı (2011) Kıbrıs Meselesinin Tarihçesi, BM Müzakerelerinin Başlangıcı:
<http://www.mfa.gov.tr/kibris-meselesinin-tarihcesi_-bm-muzakerelerininbaslangici.tr.mfa> son erişim 30.03.2019.
[83] Avrupa Birliği Türkiye Delegasyonu (2019) Katılım Müzakereleri: <https://www.avrupa.info.tr/tr/katilim-muzakereleri-720> son erişim 30.03.2019.

Kişilerin, malların, sermayenin serbest dolaşımının sağlanabilmesi düşüncesi ile kurulan Avrupa Birliği'nde kişilere ait verilerin toplanması ve işlenmesi bir zorunluluktur.[84] Bu nedenle, AB'de kişisel verilerin korunması amacıyla oluşturulan kurallar, bilgi teknolojilerinin gelişmesiyle birlikte AB içerisinde ortak pazarın gerekliliklerini dikkate almak ve serbest veri akışının temel hak ve özgürlüklere uygun işletilmesi maksadıyla oluşturulmuştur.[85]

AB'nin direktifleri, tüzükleri, anlaşmaları ve normatif kuralları, hukuka uygun, tek düze veri dolaşımı ve verilerin işlenmesi hususundaki konuları düzenlenmektedir.[86] Bu anlamda veri koruma ile ilgili 24.10.1995 tarihinde 95/46/EC Sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Direktifii" kabul edilmiştir. 15.12.1997 yılında ise 97/66/EC "Telekomünikasyon alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi" yürürlüğe girmiştir.[87] Bu Yönerge, 95/46 Sayılı ana düzenlemenin telekomünikasyon alanındaki tamamlayıcısı mahiyetindedir.[88] Ayrıca, 2001/45 Sayılı Yönerge ile Birliğin kendi organları içerisinde kişisel verilerin korunmasına dair düzenlemeler yapılmış ve Birlik organlarının 95/46/EC Sayılı Direktif'e uyumunu denetlemesi amacıyla veri koruma otoritesi kurulmuştur.[89] 31.07.2002 tarihinde ise 2002/58/EC Sayılı " Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi" yürürlüğe girmiştir. Bu Yönerge de 95/46/EC Sayılı Direktif'in tamamlayıcısı mahiyetinde olup,[90] 97/66/EC Sayılı Yönergenin yerine geçmiştir.[91] 2006 yılında ise 2006/24/EC Sayılı "Halka Açık İletişim Hizmetleri veya İletişim Ağlarına İlişkin Olarak Üretilen veya İşlene Verilerin Saklanmasına İlişkin Direktif" yürürlüğe girmiştir. Son olarak da 2016 yılında kabul edilip 2018 yılında yürürlüğe giren "Genel Veri Koruma Regülasyonu" adlı Direktif, 95/46 Sayılı

[84] Civelek, s. 69.
[85] Uygun, s.32.
[86] Civelek, s. 70.
[87] Oğuz, s. 9-10.
[88] Uygun, s.32.
[89] Uygun, s.32-33.
[90] Oğuz, 9-10.
[91] Uygun, s.33.

Direktifi yürürlükten kaldırmıştır. Köklü ve sürekli kendini yenileyen bir sistem içerisinde olan AB Yönergeleri, kişisel veri kavramını, kişisel verilerin korunmasına ilişkin usul ve esasları belirleyerek veri aktarımı ilişkilerinden dolayı dünyanın diğer ülkelerindeki yapılanmaları ve düzenlemeleri de etkilemektedir.[92] Aşağıdaki bölümde, sayılan AB direktiflerinin özellikleri incelenmektedir.

1.2.4.a. 95/46/EC Sayılı Direktif

"Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına İlişkin 24 Ekim 1995 tarihli 95/46 Sayılı Avrupa Parlamentosu ve Konseyi Direktifi" AB'de kişisel verilerin korunmasına yönelik yapılan en köklü düzenlemelerin başında gelmiştir. 108 Sayılı Sözleşme ve OECD tarafından hazırlanmış olan ilkelere bağlı olarak hazırlanmış olan ulusal veri koruma direktiflerinin farklılıklarının giderilmesi maksadıyla 1990 yılında çalışmalar başlatılmış ve 1998 yılında 95/46/EC Direktif yürürlüğe girmiştir.[93] Bu Direktif'in içermekte olduğu esaslar bağlamında AB ile ilişkide olan tüm ülkelerin göz önünde tutması gereken bir nitelik arz etmiştir.[94] Direktif, sadece var olan veri koruma hukukunu güçlendirmekle kalmamış, yeni bazı haklar getirerek mevcut hukuku pekiştirecek ortak bir çerçeve sunmuştur.[95]

95/46/EC Sayılı Direktif'in hedefinde üye ülkelerin iç hukuk sistemleri olup, AB Kurum ve organları Direktif'in kapsamı dışındadır.[96] 95/46/EC Sayılı Direktif'in

---

[92] Gözüküçük, M. (2014) Veri İsleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı, İstanbul, s.29.

[93] Henkoğlu, s. 47.

[94] Direktif'e göre üye devletlerin 24 Ekim 1998'e kadar iç hukuklarındaki düzenlemeleri Direktif ile uyumlaştırmaları gerekiyordu. Ancak bu üye devletlerin büyük bir bölümü bu süreye kadar gereken düzenlemeleri tamamlayamamışlardır; Küzeci, s. 176.

[95] 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, madde 6. Bu çalışma boyunca 95/46/EC Sayılı Direktif ibaresi kullanılacaktır.

[96] Henkoğlu, s. 48.

asıl amacı, verilerin değil, kişilerin en başta mahremiyet hakkı olmak üzere temel hak ve hürriyetlerinin korunmasıdır.[97]

Direktif hükümleri, belirli veya belirlenebilir gerçek kişilerin verileri hakkında uygulanabilir, kişilerin belirlenemediği anonim veriler[98] veya tüzel kişiler için uygulanamaz.[99] Öte yandan üye devletler, Direktif hükümlerini iç hukuklarına dahil ederken tüzel kişileri de kapsayacak şekilde almalarında bir engel koyulmamıştır.

AB veri koruma modelinin kilit özelliği zorlayıcılığıdır. AB üyesi devletlerin tümünde kişisel verilerin korunmasını güvence altına alan kuralların uygulanmasını sağlayacak birimler bulunmakta, Direktif ile önleyici bir korumanın sağlanması hedeflenmektedir. [100]

AB üyesi devletler, direktiflerin belirlediği hedeflere ulaşabilmeleri için ulusal düzeyde hukuksal bir düzenleme yapma yetkisine sahiptirler. Bu doğrultuda ise, Direktif'in belirlediği hedefleri iç hukuklarına aktarırken hangi düzenleme şekliyle (yasa, bakanlar kurulu kararı gibi) yapacakları yönünde karar vermeye serbest bırakılmışlardır.[101] Yapılan ulusal düzenlemelerde, Direktif'in temel esaslarına riayet edilmiş, üye devletlere bırakılmış olan uygulamaya ilişkin kısımlar ise farklılıklar olacak şekilde düzenlenmiştir.[102]

Direktif'in etki düzeyi, ülkeler arası ya da AB ile diğer ülkeler arasında yapılmış olan her türlü siyasal, sosyal ve ekonomik çalışmada, Direktif'in sahip olduğu esasların ön koşullar arasında yer almış olmasında kendini göstermiştir.[103]

---

[97] Henkoğlu, s. 47.
[98] Aydın, s.131.
[99] Uygun, s.33.
[100] Küzeci, s. 180.
[101] Küzeci, s. 179.
[102] Boz, s.63.
[103] Boz, s.63.

1.2.4.b. 2002/58/EC Sayılı Direktif

AB, 25 Haziran 2002 tarihinde,[104] 97/66/EC sayılı Yönergenin yerine geçen 2002/58/EC sayılı "Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Direktifi"ni çıkarmıştır.[105] Bu Direktif, 95/46/EC Sayılı Direktif'i elektronik iletişim alanında tamamlayıcı nitelikte olup tüzel kişilerin bu alandaki haklarını korumaktadır.[106]

2002/58 Sayılı Direktif, elektronik komünikasyon sektöründe kişisel verilerin işlenmesi konusunu düzenlemek maksadıyla 95/46/EC Sayılı Direktifte değişiklik yapmış, elektronik haberleşme hizmetlerinde yaşanan problemlerin çözümünü sağlamıştır. Örneğin; *spam*[107] elektronik postalarda, *cookie*'lerin[108] ya da *spy-ware*'in[109] kullanımındaki problemlere çözüm bulunmuştur.[110] Bununla beraber Direktif, her çeşit kişisel veri işlenmesinde tüketicilerin özel yaşamlarının gizliliği hakkını korumak ve kontrol etmek amacıyla yeni tanımlamalar ve korumalar getirmiştir.[111]

İnternet teknolojisinin hızlı gelişimi, bireyler arasındaki iletişimin daha hızlı ve daha ucuz olmasını sağladığından e-mail yöntemiyle haberleşmenin tercih edilmeye başlamasına sebep olmuştur. Bu durum beraberinde getirdiği avantajla birlikte, *spamming* gibi problemleri de getirmiş ve potansiyel bir tehdit olarak hukuk içerisinde yer alması gerektiği kanaatini doğurmuştur. Bununla beraber,

---

[104] Akgül, s.151.
[105] Uygun, s.33.
[106] Başalp, s.24.
[107] Spam, özellikle reklam formunda gelen istenmeyen bir mesaj veya aynı siteden tekrar tekrar mesaj göndermek için kullanılan sistemler olarak tanımlanabilir. Spam'ın en yaygın olarak tanınan şekli e-posta spamı olsa da bu terim diğer medyadaki benzer suiistimallere uygulanmaktadır: anında mesajlaşma spamı, haber spamı, Web arama motoru spamı, İnternet forumu spamı, sosyal medya spamı, spam mobil uygulamalar vs.
[108] Kullanıcının bilgisayarında geçici olarak veya kalıcı olarak sabit diskte depolanan dosyalardır. Cookies, web sitesinin sizi tanıması ve tercihlerinizi takip etmesi için araçtır.
[109] Spyware, kötü amaçlı kullanım için bilgisayarlardan gizlice veri toplayan bir tür zararlı yazılım veya bilgisayar virüsü için kullanılan bir terimdir.
[110] Aydın, s.151.
[111] Aydın, s.152.

internet sayfalarında gezinti yapıldığı esnada işlenen kişisel verilerin *cookies* tarafından kaydedilmesi ve bu verilerin kontrolsüz şekilde paylaşılması hukuki sonuçların oluşmasına neden olmuştur.[112]

Bu Direktif'in amacı, AB üyesi ülkelerin, haberleşmenin gizliliğine yetkisi olmayan kişiler tarafından erişilmesini engellemeleri, kamu telekomünikasyon şebekeleri ve kamuya açık telekomünikasyon servisleri vasıtasıyla sağlanan telekomünikasyonun gizliliğini korumak maksadıyla tedbirleri almalarını sağlamaktır.[113]

Direktif'in getirdiği yükümlülüklere bakıldığında, elektronik iletişimin ve mesajlaşmaların güvenliğinin taraf ülkeler tarafından sağlanacak olması, AB üyesi ülkelerin bir başkası tarafından ilgili kullanıcının rızası olmadan iletişiminin ve ilgili trafik verisinin dinlenmesini, kaydedilmesini, saklanmasını, takip edilmesini ya da başka şekillerde gizlice dinlenmesini ve gözetlenmesini yasaklayacak olması şart koşulmaktadır. Zira; direktifte yer alan düzenlemelerin, üye devletlerce iç hukuklarına aktarılması gerekliliği de hüküm altına alınmıştır. Temel hak ve özgürlüklerin korunması kapsamında kişisel verileri kontrol edenlerin yükümlülükleri ve veri sahibinin haklarına ilişkin olarak 95/46/EC sayılı Veri Koruma Direktifindeki düzenlemelerin, 2002/58/AT sayılı direktif bakımından da geçerli kabul edileceği Direktifin 15. maddesinde belirtilmiştir. Bu Direktif, sadece kamuya açık iletişimler kapsamında uygulanacak olup yalnızca gerçek kişilerin değil, tüzel kişilerin de kişisel verilerinin korunmasını düzenlemiştir.[114]

1.2.4.c. 2006/24/EC Sayılı Direktif

---

[112] Boz, s.70-71; Dinkci, s. 60.

[113] Hayrunnisa, Ö. (2009), Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Doktora Tezi, T.C Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara, s. 175; Aydın, s.52.

[114] Aydın, s.53.

2006/24/EC Sayılı "İletişim Trafik Verilerinin Saklanması Direktifi" genel olarak "terörizmle mücadele amacıyla trafik verilerine ulaşılmasını sağlamak için üye devletlerde veri saklama kurallarını uyumlaştırma"[115] amacını gütmektedir. Bu Direktif'e göre, elektronik haberleşme sektöründe faaliyet gösteren işletmeciler, Direktif'in ilk maddesi kapsamıyla belirlenmiş kategorilerdeki verileri, belirlenmiş olan süre boyunca "ciddi suçların soruşturma, tespit ve kovuşturma" süreçlerinde kullanılmak üzere saklamakla yükümlüdür. Direktif'in 5. maddesine göre bahsi geçen veri kategorileri, "iletişimin kaynağını belirlemek, iletişimin hedefini belirlemek, iletişimin tarih, zaman ve süresini belirlemek, iletişimin türünü belirlemek ve iletişimin konumunu belirlemek" için gerekli olan "arayan numara, abonenin veya kayıtlı kullanıcının adı ve adresi, aranan numara, IP adresi, kullanıcı adı, görüşme esnasında atanmış telefon numarası, konuşmanın tarih ve süre bilgileri, internete erişimin tarih ve süre bilgileri, kullanılan telefon veya internet hizmet türü, hem arayan hem de aranan tarafların IMSI ve IMEI bilgileri, coğrafi konumu belirleyecek hücre bilgisi" verileridir. Madde 6'ya göre de işletmecilerin, bu verileri "6 ay ile 2 yıl arasında" saklamaları beklenmektedir.

Direktif'in somut bir suç şüphesi olmadan halka açık bütün iletişim verilerini kaydedilmesine imkan vermesi ölçülülük ilkesine aykırılık teşkil etmektedir. Ayrıca, somut bir şüphe olmadan ve meydana getireceği hukuki sorunlar açısından 6 aydan 2 yıla kadar böyle bir tedbirin alınabilmesine imkan vermesi, ceza hukukunun temel ilkelerinden olan hukuk devleti ilkesine de aykırılık teşkil etmektedir.[116]

Bu Direktif'in çok detaylı verilerin uzun bir süre saklanmasını öngörmesinden ötürü birçok eleştiriye uğramasının ardından Avrupa Adalet Divanı, 8 Nisan 2014 tarihli kararı ile "Direktif'te bahsi geçen verilerin saklanması ve bu verilere ulusal otoritelerin erişiminin sağlanmasının özel hayata saygı ve kişisel verilerin

[115] Küzeci, s. 207.
[116] Aydın, s.208.

korunması hususundaki temel hak ve özgürlüklerle ciddi oranda çeliştiğini" ifade ederek bu Direktif'i geçersiz ilan etmiştir.[117]

1.2.4.d. Genel Veri Koruma Direktifi (GDPR)

AB üyesi ülkelerin ulusal veri koruma mevzuatlarında farklılıkların bulunması, mevzuatların yeterince anlaşılır olmaması ve 95/46/EC Sayılı Direktif'in kullanıcılarda çevrimiçi alışverişe karşı oluşan endişeleri giderememe sebebiyle yeniden gözden geçirilmesine yönelik çalışmalar başlatılmıştır.[118] Kişisel verilerin korunması hususunda hukuksal düzenlemelerin, bilgileri depolama yöntemlerinin, sosyal medya ve bilgi sistemlerinde bulunan gelişimin ve toplumsal ihtiyaçların gerisinde kalmış olması nedeniyle 2010 yılından itibaren AB yeni bir veri koruma direktifi üzerinde çalışmaya mecbur kalmıştır.[119] 95/46/EC Sayılı Direktif'in güncellenmesi yoluyla gerçekleşmesi planlanan reformla; kişisel hakların genişletilmesi, iç pazarın canlandırılması, uluslararası işbirliğinin kolaylaştırılması, mevcut kuralların daha basit ve anlaşılır hale gelmesi, iş dünyasına fayda sağlaması ve verilerin korunmasına ilişkin hukuksal düzenlemelerin yeni bilgi teknolojilerine uyumlu hale getirilmesi hedeflenmiştir. 15 Aralık 2011 tarihinde ise AB'yi kapsayacak biçimde modern ve uyumlu hale getirilmiş veri koruma çerçevesi oluşturulmasına dair tarihi bir reform üzerinde uzlaşmaya varılmıştır.[120] 2012 yılında hazırlanmış olan Genel Veri Koruma Direktifi 24 Mayıs 2016 yılı Avrupa Birliği Parlamentosunda kabul edilmiştir. KKTC'de yürürlükte bulunan 89/2007 Sayılı Yasa'nın da dayanağı olan 95/46/EC Sayılı Direktif, 25 Mayıs 2018 tarihinde yürürlükten kalkmıştır. Genel Veri Koruma Direktifi'nin yani GDPR'ın yürürlüğe girdiği tarihten itibaren 2 yıl içerisinde AB üyesi tüm ülkelerde uygulanmak üzere

---

[117] Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Court of Justice of the European Union , Press Release No 54/14, Luxembourg, 8.4.2014.
[118] Henkoğlu, s. 58.
[119] Henkoğlu, s. 58.
[120] Ayözger, A. C. (2016) Elektronik haberleşme Sektöründe Kişisel Verilerin Korunması, Doktora Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul, s. 89.

mevcut veri koruma yasalarını kaldırılıp yerine tüm üye devletlerde geçerli olacak olan bu reformun yer alması planlandığı anlaşılmaktadır.

GDPR'ın 3. maddesine göre veriyi işleme tabi tutacak olan taraflar (kontrolör ya da işlemci) AB'de bulunmasa dahi, AB'de bulunan kişilerin kişisel verilerinin işlenmesi halinde GDPR kuralları uygulanacaktır. Direktif'in uygulama alanındaki esas hedef "GAFAM" olarak anılan Google, Apple, Facebook, Amazon ve Microsoft gibi dev şirketlerin taraf oldukları uyuşmazlıklarda GDPR maddelerinin uygulanmasına imkan sağlamaktır.[121] 3. maddenin 2. fıkrası, işleme faaliyetinin AB'de bulunan kişilere mal veya hizmet sunulmasına ya da AB sınırları içerisindeki davranışlarının gözlemlenmesine dair olmasının yeterli olduğunu düzenlemiştir.

GDPR'ın getirmiş olduğu en önemli yeniliklerin arasında unutulma hakkı (right to be forgotten) sayılmaktadır. 95/46/EC Sayılı Direktif'te "kişisel verilerin silinmesi, yok edilmesi, bloke edilmesi" talebi olarak veri sahibine sağlanmış olan müdahale hakkı, GDPR ile birlikte "Unutulma Hakkı" olarak yeni bir isim almış ve mevcut müdahale zeminini unutulma hakkı ile birlikte tamamlamaktadır.[122]

Bu konunun çıkış noktası, 2015 yılında Avrupa Adalet Divanı'nın bireyin silinmeyi talep edebilmesi hakkında vermiş olduğu karardır. Söz konusu dava, İspanya vatandaşı Mario Costeja Gonzalez'in Google İspanya ve Google Inc. Şirketine karşı açmış olduğu bir davadır. Bu önemli davanın konusu, 1998 yılında bir İspanyol gazetesinde Gonzalez'e ait bir gayrimenkulün, bu kişinin sosyal güvenlik kurumuna olan borçlarının tahsil edilebilmesi için açık artırma yolu ile satılacağı ilanı çıkmış, bu ilanlar ise gazetenin internet sitesinde de yayınlanmıştır. Kasım 2009'da ise Gonzalez, anlamını yitiren bu ilanların internet sitesinden kaldırılması için gazeteye talepte bulunmuş, fakat bu talebi ilanın İspanyol İş ve Sosyal

[121] Develioğlu, H, M. (2017) *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık, İstanbul, s.2.
[122] Başalp, N. (2015) Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, *Mühf-Had*, 21(1), s.93.

Güvenlik Bakanlığı'nın vermiş olduğu emirle yayınlandığı gerekçesiyle reddedilmiştir. Bu reddin ardından Gonzalez, Google İspanya'dan adı ile arama yapıldığında bu ilanların çıkmamasını talep etmiştir. Google İspanya ise konuyu Google Inc.'e iletmiştir. Gonzalez ise İspanyol Veri Koruma Otoritesi'ne konuyla ilgili şikayette bulunmuştur. Otorite yapılan şikayetleri kabul etmiştir fakat konu ABAD'a temyiz yolu ile iletilmiştir. ABAD ise vermiş olduğu kararda, arama motorlarının ve internet aracı hizmet sağlayıcıların kontrolör sayılması gerektiğini, veri sahiplerinin bir internet sitesinde bulunan kişisel verilerinin kaldırılmasa dahi, arama motorunda internet sitesine yönelik arama sonucunun silinmesini isteme hakkının olduğuna hükmetmiştir.[123] Arama motorları, kişisel verileri kontrol altında tutmakta olduklarından, ilgili AB hukuku arama motorlarında da uygulama alanı bulabilmektedir. Arama motorunun AB içerisinde şubesinin bulunması halinde, server olarak adlandırılan veri sunucusunun fiziksel olarak AB dışında olsa dahi veriyi toplayan şirket, ilgili AB organının yer bakımından yargı yetkisindedir. Kişiye ait bilginin hatalı, eksik, alakasız ya da aşırı olması durumunda, kişinin arama motorlarından veya diğer veri toplayanlardan, verilerinin silinmesini talep etme hakkı bulunmaktadır.[124] Bu karar, kişilerin verileri üzerindeki haklarını savunmaları ve çevrimiçi verileri üzerindeki kontrol yetkilerini artırması açısından önemli bir dönüm noktası olmuş ve GDPR'da unutulma hakkının çıkış noktası olarak kabul görmüştür.[125] İlgili kararda da belirtildiği gibi, bu talep hakkı her zaman uygulanmayabilir. Basın özgürlüğü, ifade özgürlüğü ile kişisel verilerin korunması hukuku arasındaki dengenin oluşturulabilmesi ya da özgürlük ve güvenlik dengesi açısından her vakanın kendi içerisinde değerlendirilmesi gerekmektedir.[126]

---

[123] Develioğlu, s.89; Akıncı, A. N. (2017) Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, T.C. Kalkınma Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Yayın No: 2968, Çalışma Raporu No: 6, s.11; Aydın, s.44-45; Henkoğlu, s. 96.

[124] Ceran, A. (2014) IKV Değerlendirme Notu: Kişisel Verilerin Korunması: Avrupa ve Türkiye, İktisadi Kalkınma Vakfı, Rapor No: 104, s. 6.

[125] Develioğlu, s.89; Akıncı, s.11.

[126] Ceran, s. 1.

GDPR'ın getirmiş olduğu bir diğer yenilik ise bilgi toplumuna ilişkin yapılacak işlemlerde çocuğun rızasının ne şekilde alınabileceği konusun ayrı bir madde altında incelenmiş olmasıdır. Bilgi toplumu hizmetleri, uzaktan ve elektronik araçlarla ve hizmeti alanın bireysel talebi doğrultusunda bir bedel karşılığı sunulan hizmetlerdir.[127] Bilgi toplumu hizmeti sunulurken kişisel verilerin rıza ile işlenebilmesi için rızası alınacak çocuğun en az 16 yaşında olması gerekmektedir. Hizmet sunulacak çocuk 16 yaşından küçük ise çocuğun velayetini tutan kişi rıza gösterecek ya da yetkilendirme yapacaktır. Aksi halde yapılan tüm işlemler hukuka aykırı olarak kabul edilecektir. Veriyi işleyecek olan taraf, mevcut teknolojiyi dikkate alarak, işleme için verilen rızanın çocuk üzerinde velayet hakkına sahip kişi tarafından verildiğini ya da onaylandığını doğrulamak amacıyla makul çabayı gösterecektir. Üye ülkelerin ulusal sözleşmeleri, çocuk ile yapılan sözleşmelerin oluşturulması, bu sözleşmelerin geçerliliği ya da etkisine dair kurallar GDPR'n bu düzenlemesi ile etkilenmeyecektir. Ayrıca, GDPR'ın 8. maddesine göre üye ülkeler, 13 yaşından küçük olmaması şartıyla bu yaş sınırını indirme hakkına sahiptirler. GDPR'ın ayırt etme gücünü genel kural olarak yeterli saydığı anlaşılmaktadır.[128]

Türkiye AB üyesi olmasa dahi, GDPR'ın kapsamı açısından şartları karşılaması halinde veriyi işleme tabi tutan tarafların GDPR maddelerine uymakla yükümlü olacakları, herhangi bir ihlal halinde bu Direktif'te öngörülen yaptırımlara maruz kalacakları bir gerçektir. Avrupa Birliği üyesi olan Güney Kıbrıs Rum Yönetimi ise

[127] Bilgi toplumu hizmetleri, GDPR'ın tanımlarını içeren 4. maddesinde de belirtildiği üzere Avrupa Parlamentosu ve Avrupa Konseyinin 2015/1535 sayılı yönergesinin 171(b) maddesinin b bendinde tanımlanmıştır; Develioğlu, s.54.

[128] Çekin, M. S. (2018) *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, On iki Levha Yayıncılık, İstanbul, s.63.

diğer üye devletler gibi, kişisel verilerin korunmasına dair Yasası'nı yürürlükten kaldırarak 2018 yılında GDPR kurallarını içeren yeni mevzuatını yayınlamıştır.[129]

KKTC'nin özel durumundan dolayı KKTC'de bulunan kontrolörlerin yukarıda belirtilen şartları karşıladığı durumlarda GDPR hükümlerine uymakla yükümlü olup olmayacağı konusu çok tartışılacak ve AB otoritelerinin üzerine karar üretmelerini gerektiren bir durum olarak karşımıza çıkmaktadır. Bilindiği üzere, Kıbrıs adası 1974 yılında gerçekleştirilen Barış Harekatı'nın ardından ikiye bölünmüş ve Kuzey'de ağırlıklı olarak Türkler'in yaşadığı, Güney'de ise Rumlar'ın yaşadığı bir ülke haline gelmiştir.[130]

GDPR'ın detaylarına aşağıdaki bölümlerde yer verileceğinden çalışmanın bu kısmında GDPR'ı ilke ve kurallarına değinilmeyecektir.

1.3. Diğer Ülkeler

1.3.1. ABD

Amerikan hukukuna bakıldığında kişisel verilerin korunmasına ilişkin hakkı da içeren özel yaşamın gizliliği hakkının anayasal bir hak olmadığı görülmektedir. Bu hak, 19. Yüzyılın sonlarında tartışılmaya başlanmış ve takip eden yıllarda içtihatlarla birlikte kabul görmüştür.[131]

---

[129]The Commissioner for Personal Data Protection (2018) The Regulation (GDPR): <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3g_en/page3g_en?opendocument> son erişim: 04.04.2019.

[130] Bu çalışmanın amacına aykırı olduğundan siyasi sebeplerin neler olduğuna değinilmeyecek, yalnızca çalışmada bahsedilen GDPR'ın uygulama alanını etkileyen kısımlardan kısaca bahsedilecektir.

[131] Küzeci, s. 68; Boz, s. 75.

ABD'de mahremiyet kanunlarının ihtiyaç duyuldukça çıkartıldığı görülmektedir.[132] Ayrıca, ABD, OECD Rehber İlkeleri'ni 1981 yılında imzalamış fakat iç hukukuna bu ilkeleri dahil etmemiştir.[133] ABD, özel yaşamın gizliliğinin korunmasına ilişkin düzenlemeleri, bir bütün halinde çıkarmak yerine parça parça geliştirmiş ve her sektörün farklı yasal ihtiyaçları olmasından dolayı ABD'de özel yaşamın gizliliğinin korunmasına ilişkin sektörel bir bakış açısı benimsemiştir.[134] AB ile ABD arasında kutuplaşma yaratan bu durum karşısında AB kişisel verilerin korunması hususunu temel bir hak olarak görürken, ABD bu hususa müşteri hakkı açısından bakmıştır.[135]

ABD, özellikle güvenlik kaygıları dolayısıyla, kişisel verilerin korunması meselesinde kendi çıkarlarını daha ön plana çıkartan bir yol izlemiş ve AB ile bu konuda ters düşmüştür. AB ile uzun süren müzakereler neticesinde 2000 yılında bir anlaşma yapılmıştır. AB Komisyonu'nun en yaygın "yeterlilik" kararı olan ve "*Safe Harbor*" olarak anılmakta olan bu anlaşma, kişisel verilerin korunması alanında farklı sistemler arasında uzlaşıya varılmasının önemli bir örneği sayılmaktadır.[136]

ABD'de 7 Ekim 2015 tarihinde *Safe Harbor* anlaşması geçersiz kılınmıştır. *Privacy Shield* adı verilen Gizlilik Kalkanı ilkeleri 12 Temmuz 2016'da Avrupa Komisyonu tarafından kabul edilmiş ve geçersiz ilan edilen *Safe Harbor (Güvenli Liman)*'ın yerine geçmiştir. Bu yeni çerçeveyle ABD'ye verileri aktarılan tüm AB vatandaşlarının temel hakları korunurken, transatlantik veri iletimine dayanan şirketlere de hukuki netlik kazandırılmaktadır. Bu anlaşma ile birlikte AB ve ABD

---

[132] Civelek, s. 81.
[133] Civelek, s. 81.
[134] Gözüküçük, s.32.
[135] Bununla birlikte ABD'nin California eyaletinde 1 Temmuz 2004 tarihinden bu yana yürürlükte olan "Çevrimiçi Mahremiyet Koruma Kanunu" (Online Privacy Protection Act, OPPA) bu eyalette yaşayan bireylerin kişisel verilerini toplayan ticari internet sitelerinin, belirlemiş oldukları mahremiyet politikalarını açıkça yayınlamaları, bunun yanında mahremiyete ilişkin kurallara uymaları gerektiğini hükme bağlamaktadır; Civelek, s. 81.
[136] Küzeci, s. 194.

Avrupa Komisyonu bu anlaşmanın ardından ABD için "yeterlilik kararı" vermiştir.[137]

1.3.2. Türkiye

Türkiye'de yakın zamana kadar kişisel verilerin korunmasına yönelik genel bir yasa bulunmamaktaydı. Bu konudaki ilk yasal düzenleme çalışmaları 2000'li yıllarda başlamış ve TBMM'ye müteaddit defa tasarısı sunulmuş olmasına rağmen yasalaştırma çalışmaları ancak 2016 yılında tamamlanabilmiştir.[138] 6698 Sayılı Kişisel Verileri Koruma Kanunu'nun yürürlüğe girdiği 7 Nisan 2016 tarihine kadar Anayasa, yasalar ve çeşitli yönetmeliklerle kişisel verilerin korunması konusu çözülmeye çalışılmıştır.[139]

Türkiye'nin hem Avrupa Birliği'ne üyelikle ilgili müzakerelerde kişisel verilerle ilgili yasal boşluğun kapanması zorunluluğu,[140] hem de veri koruma bakımından AB ülkeleri nezdinde "güvenli ülke" sayılması için karşılaması gereken kriterlerden biri 6698 Sayılı Kişisel Verilerin Korunması Kanunun yürürlüğe girmesi ile aşılmıştır.[141] Ancak, AB'de kişisel verilerin korunması hukukundaki gelişmeleri yakalama amacıyla yürürlüğe giren Kanun, GDPR'ın yürürlükten kaldırdığı 95/46/EC Sayılı Direktifi esas almış olup, GDPR'ın getirdiği yenilikleri içermemektedir.[142] Kanun'un temeli bu olsa da gerek Kişisel Verileri Koruma Kurulu'nun çalışmaları gerekse alanında uzman hukukçu ve akademisyenlerin çalışma ve eserleri ile GDPR'a uyum ve getirilen yenilikler Türkiye'de de kendini göstermektedir.

---

[137] European Commision (2018) EU-US Privacy Shield: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-data-transfers_en> son erişim 08.04.2019.
[138] Akıncı, s. 4.
[139] Ayözger, s. 96.
[140] Develioğlu, s.15.
[141] Akıncı, s. 26.
[142] Develioğlu, s.16.

1.3.3. Güney Kıbrıs

Güney Kıbrıs'ın 1 Mayıs 2004 yılında Avrupa Birliği üyesi olması nedeniyle 25 Mayıs 2018 yılında yürürlüğe giren GDPR, Güney Kıbrıs'ın da kişisel verileri koruma ile ilgili 2001 yılında yürürlüğe giren ve 2012 yılına değin 2 kez değişikliğe uğrayan mevzuatının yerini almıştır. 2001-2012 Yasaları olarak geçen Law 138(I)/2001 37(I)/2003, 105(I)/2012 sayılı yasalar, Law 125(I)/2018 Sayılı Yasa ile yürürlükten kaldırılmıştır.

GDPR hükümlerini iç hukukuna uyarlayan yeni Law 125(I)/2018 sayılı yasa ise 31 Temmuz 2018 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiştir. Yasanın geçici 37. maddenin 1. fıkrasında, 28.09.2015 tarihinde Bakanlar Kurulu tarafından atanan Kurul Başkanının (Commissioner) 4 yıllık görev süresi dolana kadar Başkanlığının geçerli olacağı belirtilmiştir. Yine aynı maddenin 2. fıkrasında yürürlükten kaldırılan yasa hükümleri uyarınca Başkanın yapmış olduğu eylemler öngörülen sürelerinin bitimine ya da değişikliklerine kadar geçerli olacaktır.

Yasanın kapsamına yer veren 3. maddesine göre, Yasa hükümlerinin GDPR'ın 2. ve 3. maddesi uyarınca Kıbrıs Cumhuriyeti'ni (Republic of Cyprus) kapsadığı belirtilmektedir. Bu konuda irdelenmesi gereken bir husus vardır ki, o da Kıbrıs Adası'ndaki siyasi, hukuki ve toplumsal bölünmedir.

II. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASINA DAİR TEMEL KAVRAMLAR

2.1. Mahremiyet

Mahremiyet, "kişinin herkesle paylaşmayacağı veya herhangi bir kimse ile paylaşmamak hakkının bulunduğu olay, inanç ve duygularının, isteği üzerine o kişiyle paylaşması" hususuna karşılık gelen "*intmacy*" deyimini ifade eder.[143]

Temel bir hak ve özgürlük olan mahremiyet hakkı, kişilerin kamusal alan ile özel hayatlarının ayrı kalmasını sağlayarak bu alanda özgürce tartışmalarını, konuşmalarını, düşünmeleri garanti altına almaktadır.[144] İnsanlar, kendileri hakkındaki verilerin adil bir biçimde işleneceği ve muamele göreceğinden emin olmalıdır.[145]

Kişisel verilerin, kişinin rızası dışında işlenmesine ilişkin her çeşit girişim, mahremiyetin ve özgürlüğün ihlal edilmesi anlamına gelmektedir. Mahremiyet, bilgisayarlaşmış toplumlarda tehdit altında olup, korunması yalnızca hukuksal düzenlemelerle sağlanamamaktadır.[146]

---

[143] Küzeci, s. 16.
[144] Civelek, s. 25.
[145] Tataroğlu, M. (2013) Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED), *Yönetim ve Ekonomi,* 20(1), s.263
[146] Henkoğlu, s. 23.

Son yüzyılda yükselmiş olan insan hakları kavramı, toplumları etkilemiş, "*birey*" kavramını merkeze yerleştirmiştir ve böylece mahremiyet kavramının da içselleştirilmesini sağlamıştır. Aynı zamanda da teknolojinin hızlı gelişimiyle insanlar, günlük hayatlarını daha rahat idame ettirme, yaşam standardını yükseltme ve kişi haklarını kullanma gibi sebeplere dayanarak, gündelik işleri için bilgilerini vermeyi, güvenlik gerekçesiyle kendi rızaları olmaksızın konuşmalarının ve davranışlarının kayıt altına alınmasını kabullenmiş ve hatta talep etmişlerdir. Kişilere ait bu bilgiler kayıt altına alınmakta ve yine teknoloji sayesinde depolanmakta, analiz yapılmakta, paylaşılmakta ve çok kısa bir sürede geniş toplum kesimlerine yaygınlaştırılmaktadır. Ayrıca, bu bilgilerin kimler tarafından ve nasıl kullanılacağı verinin sahibi tarafından tam olarak bilinememektedir. Devletler, teknolojiden yararlanarak bilgi toplama, depolama, kopyalama, transfer etme, internet aracılığıyla yayma işlemlerini toplum yararı temellendirmesiyle yapmaktadır. Şirketler ise, bu temellendirmeyi tüketici tercihlerine dayandırarak kendi veri tabanlarını oluşturmakta, verileri şirketler arası paylaşmakta ve her geçen gün bilgi edinme kaynaklarını ve bunları işleme yeteneklerini artırmaktadırlar.[147]

2.2. Özel Hayat

Devlet kavramının oluştuğu zamanlardan itibaren devletin güvenliğinin korunması ile bireylerin özel hayatının korunması arasında olan hassas denge her zaman gündemde olmuştur. Özel hayatın gizliliği hakkı, bireylerin özel hayatlarını devlete karşı koruduğu gibi, bireylerin birbirleri arasında da özel hayata müdahalelerinde ileri sürülebilmiştir.[148]

[147] İzgi, C. M. (2014), Mahremiyet kavramı Bağlamında Kişisel Sağlık Verileri, *Türkiye Biyoetik Dergisi*, 1(1), s. 27.
[148] Aras, Ü. Y. (2010) İnsan Hakları Temelinde Özel Hayat Hakkinin Ulusal ve Uluslararası Alanda Uygulamaları, Yüksek Lisans Tezi, T.C. Bahçesehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yüksek Lisans Programı, İstanbul, s.49.

Birçok kişi özel hayatın ne olduğunu algılayabilir fakat bu kavramı kelimelerle ifade etmekte zorlanır. Diğer bir ifade ile "özel yaşam, tanınması kolay, tanımlanması güç bir olgudur."[149] Özel hayat, "kişinin mutlak olarak gizli tuttuğu yaşam parçaları ile herkesin bilmesini uygun bulmadığı, yalnız kendi seçeceği kişilerle, belirlediği ölçü ve biçimde paylaşacağı yaşam parçalarının birlikte oluşturdukları yaşam alanı" olarak tanımlanabilir.[150]
Kişisel veri kapsamında olan birçok veri, kişinin özel hayatını ilgilendiren ve en mahrem kısımlarını açığa çıkarabilecek potansiyele sahip olan verilerdir. Dolayısıyla kişisel verilerin özel hayatın bir parçası haline gelmesi kaçınılmaz olmuştur.[151]

Kişisel verilerin korunmasının, bireylerin mahremiyet haklarının korunmasına hizmet etmekte olduğu ve mahremiyet ile mahremiyetin uzantısı olan özel hayatın, bireylerin kişilik haklarının bir görünümü olduğu belirtilmektedir.[152]

Özel hayatın gizliliği hakkı, modernleşme ve teknolojideki ilerlemelere paralel şekilde gelişmekte olan bir hak kategorisidir. Bilim ve teknolojideki gelişmeler, kişinin özel hayatına müdahaleyi kolaylaştırdıkça kişiye özel hayatının korunmasını talep etme hakkı tanınmıştır. Özel hayatın gizliliği hakkı, bireye kendisine ait her şeyin gizli kalmasını, ifade edilmemesini, kaydedilmemesini, gösterilmemesini ve ihlal edilmemesini isteme hakkı verir.[153] Teknolojinin ilerlemesinin insanlığa sunduğu avantajlar ile boyutu önemli olmaksızın veriler toplanabilmekte ve analiz yöntemleri ile korkunç sonuçlara ulaşılabilmektedir. İnsanlığa hizmet için kullanılabilecek bu durum, aynı zamanda insan haklarına aykırı olabilecek müdahalelere de neden olabilmektedir. Örneğin, bir ülkedeki vatandaşların kredi kartı verilerinin bulunduğu veri tabanının kullanılması ile yapılabilecek analizlerde kişileri özel hayatlarına müdahale edilerek kimlere para

[149] Küzeci, s. 79.
[150] Küzeci, s. 80.
[151] Boz, s. 13.
[152] Aksoy, s.75.
[153] Aras, s.31.

transferi yaptıklarını yani kimlerle ilişkilerinin olduğunu, ne kadar varlığa sahip oldukları ya da borçları olduğunu, yaşam tarzı, seyahat bilgileri gibi çeşitli verilere ulaşmak mümkündür. Bu durum, kişisel veriler kullanılarak ortaya çıkabilecek hak ihlali durumlarından sadece bir kısmını oluşturmaktadır.[154]

2.3. Kişilik Hakkı

Kişilik, kişi kavramını da içerisine alan, bir kişiyi toplumdaki diğer insanlardan ayırmaya yarayan, kişinin kendisine ait spesifik özelliklerini ve kişinin maddi ve manevi değerlerinin tümünü ifade eden bir kavramdır.[155] Kişilik hakkı ise, zaman, coğrafya ve toplum özelliklerine göre değişkenlik gösteren, yani sabit olmayan bir kavramdır.[156] Bu değişkenlik, kişinin doğumundan itibaren kazandığı, kendi kararı ile de olsa vazgeçemeyeceği, herkese karşı öne sürebileceği bir haktır.[157]

Kişisel verilerin korunması hukukunda tüm bireyler eşit korumada yararlanmaktadır. Kişinin eğitimi, ekonomik durumu, yaşı, cinsiyeti, vatandaşlığı gibi kriterlerinin kişisel verilerin korumasına ilişkin haktan yararlanmasında hiçbir etkisi, önemi bulunmamaktadır. Mesela; bir kimsenin kamuya mal olması o kişiye tanınan koruma hakkını azaltmaz.[158] Bununla beraber, toplumu yakından ilgilendiren bir durum söz konusu olduğu zaman, ifade özgürlüğü ve bilgi edinme özgürlüğü kapsamında veriyi işleme tabi tutan tarafın meşru menfaati ve veri sahibinin temel hak ve özgürlükleri arasında meşru menfaat dengesine bakılmalı, verinin işleme tabi tutulmasının yasal olup olmadığı değerlendirilmelidir.[159]

---

[154] Boz, s. 33.
[155] Doğu, A. H. (2016) *Bilişim Hukuku*, Ekin Yayınevi, Bursa, s.21.
[156] Şimşek, s. 9.
[157] Doğu, s.2.
[158] Develioğlu, s.32.
[159] Meşru menfaat dengesine örnek; bir zamanlar yaşadığı yerde ünlü olan amatör futbol takımının kaptanı hakkında yıllar öncesine ait bir haber çevrim-içi bir gazete sitesinde yayınlanmaktadır. Belirtilen haberde ilgili kişinin adı-soyadı ve dahil olduğu ceza yargılaması hakkında hikayenin tamamı yazmaktadır. İlgili kişinin artık sabıka kaydı bulunmamaktadır ve geçmişte gerçekleşmiş olan kanun ihlali sabıka kaydında yer almamaktadır. Bu sebeple, belirtilen olay gerçek olsa dahi, kontrolörün menfaati bilgiye konu kişinin temel hak ve özgürlüğüne zarar verici nitelikte olabileceği

Kişisel verilerin korunması hukukunun genel ve asli hedefi gerçek kişileri ve gerçek kişilerin mahremiyeti ve kişilik haklarını koruma altına almaktır.[160] Genel ilke olarak tüzel kişilere ait veriler, kişisel veri olarak kabul edilmemektedir.[161] Bununla birlikte; günümüzde tüzel kişilere ait veriler aracılığıyla gerçek kişilere ait verilere erişmenin kolaylaşması nedeniyle[162] tüzel kişilere ait gerçek kişi bilgilerinin de özenle korunmasına dikkat edilmelidir.[163] Örneğin; bir şirkete ait elektronik posta adresinden gerçek kişiye ulaşılabiliyorsa bu veri, gerçek kişiye ait bir veri olarak kabul edilmeli ve bu yasa gereği korunmalıdır.

2.4. Kişisel Veri

Kişisel veri (personal data), belirli veya belirlenebilir nitelikteki bir kişiye dair her türlü bilgidir.[164] Kişisel verinin kişisel olmayan veriden ayrılması için iki ölçüt kullanılabilir. Bunlardan biri; verinin bir kişiye dair olması, diğeri ise; bu kişinin belirli veya belirlenebilir olmasıdır. [165] Kişinin belirlenebilir olması, kişinin henüz belirlenmiş olmasa da kimliğinin belirlenebilmesi anlamına gelmektedir.

Genel anlamıyla kişisel veri kavramı kapsamına giren bilgiler, bir kişinin kimliği, etnik kökeni, fiziksel özellikleri, öğrenim durumu, ikameti, kredi kartı bilgileri, alışveriş alışkanlıkları, istihdam durumu olabileceği gibi, bir kişinin bireysel, sosyal ve aile içi yaşantısına dair bilgileri, başkası ile gerçekleştirdiği haberleşmeleri,[166]

---

için iki değer birbiri ile yarıştırıldığında ilgili kişinin menfaati ve hakları üstün gelmektedir. Bu sebeple, yapılan değerlendirme sonucu kontrolörün kişisel veriyi işlemesi hukuka uygun kabul edilemez.

[160] Civelek, s. 15.

[161] Uygun, s.44.

[162] Bir tüzel kişi şirket adına kayıtlı araç takip cihazı veya el terminali gibi cihazların konum verilerini işleyen bir firma, bu cihazı kullanmakta olan gerçek kişinin konum verilerini işlediğinden bu kapsama girecektir.

[163] Civelek, s. 15.

[164] Küzeci, s. 11; Aksoy, s.17.

[165] Küzeci, s. 294-295.

[166] Aksoy, s.1.

kişiyi belirleyebilecek niteliğe sahip ses kaydı, kişinin kamera kaydındaki görüntüsü,[167] Twitter/Facebook/Whatsapp gibi sosyal medya iletileri, e-posta adresi, parmak izi, biyometrik ve tıbbi bilgileri gibi yaşamın her alanındaki bilgiler kişisel veri kapsamına girmektedir.[168] Bununla beraber GDPR'da da yer alan gerçek kişiye ait konum verileri, çevrim içi tanımlayıcı verileri de kişisel veri kapsamındadır. Kişisel verileri elinde bulunduran kişiler maddi ve manevi anlamda güçlü konumdadır. Zira ele geçirilen kişisel veriler, hukuka uygun ya da aykırı yollarla kullanılmak suretiyle maddi yarar elde edilebileceği gibi, kişinin başkası ile paylaşmak istemeyebileceği verilerin üçüncü kişilerle paylaşılmasına yönelik tehlike de, veriyi elinde bulunduran kişi açısından manevi güç anlamına gelebilir.[169]

Bir verinin kişisel veri sayılması için bilginin doğru veya kanıtlanmış olması gerekmez. Zira ilgili mevzuatlara göre bilgiye konu kişinin kendisine ilişkin işlemeye tabi tutulmuş bilgilerini görme ve hatanın düzeltilmesini isteme hakkı bulunmaktadır.[170]

2.5. Hassas Kişisel Veri

Kişisel veriler içerisinde hassas veri (sensitive data) diye bir ayrıma gidilmesinin sebebi, bu tür verilerin daha katı kurallara tabi olması ihtiyacından ileri gelmektedir.[171] Hassas veri, kişileri bulundukları toplum içerisinde önyargıya, ayrımcılığa maruz bırakabilecek, telafisi mümkün olmayan durumları ortaya çıkarabilecek mahiyetteki, kişilerin temel hak ve hürriyetleri ve mahremiyetleriyle ilişkili verilerdir. Bu sebeple hassas verilerin işlenmesine yönelik şartlar

---

[167] Civelek, s. 17.
[168] Ceran, s. 2.
[169] Ticaret siteleri, kişinin alışveriş alışkanlıklarını keşfederek o kişiye özel reklamlar gönderebilir. Veyahut kişinin cinsel yaşamına ait bir gizli bilgiyi elinde bulunduran kişinin bu bilgiyi üçüncü kişilere açıklayacağına yönelik tehdit ile bir talepte bulunabilmesi hususları maddi ve manevi güce birer örnek olabilir. Bu nedenle bireylerin kişilik haklarının ihlal edilmesi, bu kişilerin maddi ve/veya manevi zararlarına yol açabilmektedir; Aksoy, s.4.
[170] Civelek, s. 142.
[171] Boz, s. 9.

mevzuatlarda ayrıca ele alınmıştır. Örneğin bir kişinin hastalığı veya cinsel eğilimi ile ilgili işlenmiş olan verilerinin korunamaması halinde kişi, toplumdan dışlanabilir, işini kaybedebilir veya ailevi sorunlar yaşamasına neden olabilir.

Bir kişinin sağlığına ilişkin bilgilerinin kişi ile ilişkili tutuluyor olması, hasta açısından faydalı olacaktır. Mesela doktorlar, hastaya doğru müdahalede bulunabilmek için hastalarının sağlık ile ilgili kişisel verilerine ihtiyaç duyabilirler.[172]

Bunun yanında tıbbi araştırmalar için sağlık verileri gerekebilmektedir. Sağlığa ilişkin veriler kişiler için oldukça hassas bir konu olup, kişilerin sağlık verilerini gizli tutma ve veriyi işleyenler açısından gizli tutulmasını isteme hakları vardır. Bu bilgiler nedeniyle kişilerin tehdit veya toplumdan soyutlanma durumu ile karşılaşabilecekleri düşünüldüğünde, bu bilgilerin başka kişilerin eline geçmesindeki tehlike boyutu anlaşılabilirdir. Bununla beraber, kişinin sağlığına ilişkin verilerinin yeteri derecede korunmadığını düşünmesi, sağlık hizmeti almaktan kaçınması gibi bir sonuç da doğurabilecektir.[173]

Hassas kişisel verilerin korunması hususu özellikle internetin kullanılması ve çevrimiçi bilgi paylaşılmasının artmasıyla daha önemli hale gelmiştir.[174] Veri

---

[172]Korkmaz, I. (2016) Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, *TBB Dergisi*, 124, s. 114.

[173] Bu konuya ilişkin AİHM'nin Finlandiya'ya karşı verdiği karar önemlidir. AİHM'e başvuru konusu olan olay, HIV virüsü ile ilgilidir. Mahkeme, bulaşıcı niteliği olan bu enfeksiyonla ilgili verilerin gizliliğinin korunmasının özellikle önemli olduğuna değinmiştir. Mahkeme'ye göre bu tür verilerin paylaşılması, kişinin özel ve aile yaşamının yanında sosyal durumunu ve iş durumunu da ciddi olarak etkiler. Bunun sonucunda, kişi toplumdan dışlanma ve adının lekelenmesi tehlikesi altına girebilir. Bu kararında AİHM, AİHS'ne taraf olan tüm devletlerin, tıbbi verilerin gizliliğine saygı göstermek zorunda olduğunu belirtmektedir. Sadece, hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de koruma şarttır. AİHM'e göre; böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar, doğru tedavi görmek için ve hatta tıbbi yardım almak için gerekli olan kişisel veya mahrem bilgileri açıklamaktan cayabilir; bu durumda hem kendi sağlıklarını hem de bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını tehlikeye atar. AİHM kararında bu tür kişisel verilere yapılan müdahalelerin önemli bir kamu yararı bulunmadığı sürece AİHS'nin 8. maddesine aykırı olacağını belirtmiştir. Dutertre, G. (2003) *Avrupa İnsan Hakları Kararlarından Örnekler*, Avrupa Konseyi Yayınları, Ankara, s. 310 – 312; Küzeci, s. 237; Akgül, s. 19; Korkmaz, s. 114.

[174] Küzeci, s. 251.

süjesinin ziyaret ettiği internet siteleri vasıtasıyla oluşturulan profilinde hassas kişisel verilerin bulunması bu kapsamda değerlendirilebilir.[175]

Biyolojik özelliklerden kaynaklanan biyometrik veriler de kişisel verilerdendir. Kişinin parmak izi, retinası, sesi, yüz hatları, elinin şekli, damarları, değişik yetenekleri, davranış karakteristiği (mesela el yazısıyla imzası, tuşa dokunma şekli, değişik yürümesi veya konuşma tarzı gibi veriler) kişinin biyometrik verileri olarak sınıflandırılabilecek kişisel verileridir.[176]

2.6. Kişisel Verilerin İşlenmesi

Günümüzde değerlendirilmesi gereken en önemli sorunlardan biri, bilgilerin depolanması ve ayrıştırılması suretiyle bireylerin gözetimidir. Kişisel verilerin işlenmesine dayanan bu gözetim, yalnızca devlet tarafından değil, özel kişi ve kuruluşlarca da yapılabilmektedir. Örneğin, bankalar arasındaki ortak bilgi paylaşımı sonucunda her banka bir kişinin diğer bankada ne kadar parası ya da bankaya borcu olduğunu görebilmektedir. Veyahut marketler ya da giyim mağazaları, müşterilerine verdikleri indirim kartları sayesinde indirim veya puan kazandırmak için kartı her barkottan geçirdiğinde kişinin alışveriş alışkanlıklarını kaydedip takip etme ve kişinin kişisel bilgilerinden yararlanarak pazarlama teknikleri geliştirmektedirler.[177]

Kişisel verileri işleme iki şekilde yapılabilmektedir. Bu yöntemlerden biri otomatik işleme, diğeri ise otomatik olmayan işlemedir.[178] Önceki bölümde ele alınmış olan 108 Sayılı Sözleşme'nin 2. maddesi, otomatik işlemeyi şu şekilde tanımlamıştır: "Tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen verilerin kaydı, bu

[175] Küzeci, s. 252.
[176] Belirli bir bireye özgü olması ve başka kimsede bulunmaması nedeniyle biometrik veriler kimlik doğrulayıcı (identifier) olarak kullanılabilirler. Ör: DNA verisi.; Civelek, s. 17.
[177] Bük, s.8.
[178] Boz, s. 11.

verilere mantıksal ve/veya aritmetik işlemlerin uygulanışı, verilerin değiştirilmesi, silinmesi, çıkarılması veya dağıtılması." Kişisel verilerin bu otomatik sistemler kullanılmadan işlenmesi, verilerin elden işlenmesi anlamına gelmektedir.[179] Bu yöntem, geleneksel dosyalama sistemi ile verilerin işlenmesi anlamına gelmektedir.[180] GDPR'ın 4. maddesi ise kişisel verilerin kısmen veya tamamen otomatik yollarla işlenmesinin yanı sıra, bir veri kayıt sisteminin parçası olması sebebiyle otomatik olmayan yollarla kişisel veriler üzerinde bir faaliyet yapılmasını da işleme olarak kabul etmiştir.

Avrupa Adalet Divanı karar konularında kişisel verilerin işlenmesi kavramı da yerini almıştır. Özellikle verilerin internet ortamına yüklenmesi de kişisel verilerin işlenmesi olarak sayılmıştır.[181] Ayrıca, kişisel veri olup olmadığı ayrımı yapılmaksızın internetteki verilerin sistematik şekilde arama motorları tarafından tarama yapılması ve liste halinde sunulması işlemi kişisel verilerin toplanması, kaydedilmesi, tasniflenmesi, açıklanması, elde edilebilir hale getirilmesi, kişisel verilerin işlenmesi olarak sayılmıştır. Bununla birlikte, verilerin daha önceden başka mecralarda aleni hale getirilmiş olması, veri işleme faaliyetinin varlığı açısından bir öneme sahip değildir. [182]

2.7. Kişisel Verilerin Korunması

Kişisel verilerin korunmasının temelinde "kişinin korunması" prensibi yer almaktadır.[183] Dolayısıyla, temelde "veri"lerin değil, bu verilerin ilişkili olduğu kişi ve kurumların korunması hedef alınmıştır.[184] Bu prensibe göre, herkesin diğer kişilerden saygı görmeyi talep etme hakkı vardır. Birey, kişilik değerlerinin zarar

[179] Başalp, s.33.
[180] Boz, s. 11.
[181] Çekin, s.40.
[182] Çekin, s.40.
[183] Civelek, s. 14.
[184] Küzeci, s. 15.

görmemesini talep etme hakkına sahiptir.[185] Kişisel verilerin korunması, kişileri onlara ilişkin bilgilerin gerek bilgisayar gerekse el ile işlenmesinden doğacak zararlardan koruma maksadına yönelmiş ve verilerin korunmasına ilişkin ilkelerde somutlaşmış yasal ya da yasal olmayan önlemi ifade etmektedir.[186] Bu bağlamda kişisel verilerin korunmasının, kişilere ilişkin bilgilerin toplanması, kullanılması, saklanması gibi veri işleme sürecinin tüm aşamalarını kapsayan ve kişilerin denetim hakkını yeniden kazandırmaya yönelmiş olduğu söylenebilir.[187]

Bireyin kişisel verilerinin korunması hakkı, toplumsal düzenin demokratik yapısı açısından önem teşkil etmektedir. Vatandaşların kendileri hakkında kimin, ne zaman, hangi amaca dayanarak, hangi verilere sahip olduğunu bilme olanağı yoksa böyle bir hukuk düzeni içerisinde kişinin verileri üzerindeki hakkının korunmasından söz edilemez.[188] Bireyin sahip olması gereken kişisel verilerinin korunması hakkı, devletin tüm veri işleme faaliyetleri karşısında geçerli bir temel hak olarak korunmalıdır.[189]

2.8. Veri Güvenliği

"Veri güvenliği" diğer bir deyişle "bilgi güvenliği" bir bilginin yetkisiz kişilerce ele geçirilmesini ve yetkisiz kişilerce değiştirilmesini, bozulmasını, ya da yok edilmesini engelleme, yetkili kişilerin istenilen zamanda ve istenilen şekilde bilgiye erişimini sağlama anlamına gelmektedir.[190] Kişisel veriler, devletlerin geliştirdiği bilgi güvenliği politikaları ve stratejileri içerisinde korunması gerekli görülen önemli bilgilerdendir. Bu nedenle de kazaya ya da kasta dayalı güvenlik risklerine

---

[185] Civelek, s. 14.
[186] Küzeci, s. 15.
[187] Küzeci, s. 15.
[188] Dinkci, s.6.
[189] Şimşek, s.111-113.
[190] Güldüren, C. (2015) Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi, Doktora Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Ankara, s.12.

karşı bir ağın veya bilgi sisteminin karşı koyabilme kapasitesi ile kişisel verilerin korunması sıkı sıkıya ilişkilidir.[191]

Kişisel verilerin korunmasında karıştırılabilen ve konuya bakış açısını saptıran "verilerin korunması" ile "verilerin ilişkili olduğu kişilerin korunması" ayrımına dikkat edilmesi önemlidir. Yapılan düzenlemelerin çoğu hukuki nitelik taşıyıp veriyle ilgili kişilerin temel hak ve özelliklerini korumaya çalışmaktadır. Yalnızca verilerin korunması ise hukuk düzenleri tarafından sadece bir araç niteliği taşımaktadır. Veri koruması konusunda yapılmakta olan çalışmalar, hukuki nitelikten farklı olup, teknik ve teknolojik imkanlar kapsamında ele alınan çalışmalardır. Veri güvenliği, doğrudan doğruya veri güvenliğini hedef alır. Burada amaç, kişileri değil verileri korumaktır. Ancak bu veriler, kişilerle ilişkili olduğu ölçüde veri güvenliğinin kişisel verilerin korunmasına hizmet ettiği söylenebilecektir.[192] Bu nedenle, dünyadaki mahremiyet ve veri koruma yasalarında ağ ve bilgi güvenliğine dair hükümler bulunmakta olup,[193] yine birçok hukuksal düzenleme içerisinde veri güvenliği temel prensipler arasında yer almaktadır.[194]

2.9. Rıza

Bilindiği üzere kelime anlamıyla rıza, isteme, razı olma anlamına gelmektedir.[195] Kişisel verilerin korunması hukukunda veri sahibinin rıza beyanında bulunması, veri işleme sürecine katılması açısından önemli bir unsurdur. Veri sahibinin rızası, kişisel verilerin işlenmesinde en önemli meşruluk sebeplerinden biridir. Bu doğrultuda da rıza, veri sahibinin kendisiyle ilgili veriler üzerinde denetim

---

[191] Civelek, s. 30.
[192] Küzeci, s.15.
[193] Civelek, s.31.
[194] Küzeci, s.15.
[195] Türk Dil Kurumu, Güncel Türkçe Sözlük: <http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c55a657c7f7a7.51989574> son erişim 05.04.2019.

sağlayabilmesinin önemli bir aracı ve "bilgilerin geleceğini belirleme" düşüncesinin bir karşılığıdır.[196]

GDPR'ın Giriş kısmında da rızanın geçerli olmasına dair örnekler verilmiştir. Örneğin, bir internet sitesinde karşımıza çıkan kutuların tıklanması, internetten hizmet satın alınacağında teknik ayarları belirtildiği şekilde seçilmesi gibi benzer davranışlarda bulunma rızayı ortaya koyma anlamına gelmektedir. Fakat birçok internet sayfasında karşılaşıldığı gibi, halihazırda işaretlenmiş kutulardaki işaretlerin kaldırılmaması gibi hareketsiz kalma eylemleri rıza anlamına gelmemektedir.[197]

Verilen rızanın geçerli olması için rızanın konuya özel olması şartı aranmaktadır. Genel bir onay olarak değil, hangi işleme faaliyeti için alındığının açıkça anlaşılmış olması ve o faaliyet için verilmiş olması gerekmektedir.[198]

[196] Küzeci, s. 238.
[197] Develioğlu, s.53.
[198] Develioğlu, s.53.

III. BÖLÜM

KKTC'DE KİŞİSEL VERİLERİ KORUMA HUKUKU

3.1. Kuzey Kıbrıs Türk Cumhuriyeti Hukuku

KKTC'nin hukuk sistemini açıklarken kısaca tarihsel geçmişinden de bahsedilmesi gerekir. Kıbrıs Adası, 1571 yılında Osmanlı İmparatorluğu topraklarına katılmış ve 1878 tarihine kadar Osmanlı İmparatorluğu hakimiyetinde kalmıştır. Daha sonra Osmanlı İmparatorluğu, 1878 yılında Kıbrıs Adası'nı İngilizlere kiralamıştır. 1. Dünya Savaşı'nın sonlarına doğru ise İngiltere, 5 Kasım 1914 tarihinde tek taraflı bir karar alarak adayı tek taraflı ilhak etmiştir. Yeni kurulan Türkiye Cumhuriyeti de, 1923'te imzaladığı Lozan Barış Anlaşması ile İngiltere'nin almış olduğu ilhak kararını tanımış ve Kıbrıs Adası hukuken İngilizlerin egemenliği altına girmiştir. Ada üzerindeki hakimiyeti Türkler kadar uzun sürmeyen İngiltere, Kıbrıs adasının idaresini 1958 Zürih, 1959 Londra ve 1960 Lefkoşa Antlaşmalarıyla kurulmuş olan Kıbrıs Cumhuriyeti'ne bırakmıştır.[199] Buna göre, Kıbrıs Adası 307 yıl Türklerin, 82 yıl İngilizlerin hakimiyetinde kalmıştır. 1960'ta kurulan Kıbrıs Cumhuriyeti, Türkler ve Rumların ortak gücüyle kurulmuş bir devlettir. Fakat; bu çalışmada yer verilmesine gerek görülmeyen sebeplerden dolayı Türkler, kurulan devletin idaresinden ayrılmıştır. Kıbrıs Cumhuriyeti'nden ayrılan Türkler ilk önce, 28 Aralık 1967 tarihinde "Kıbrıs Geçici Türk Yönetimi"ni, 3 Eylül 1974 tarihinde "Otonom

[199] Turhan, T. (2008) Tarihsel Bakış Açısıyla Kıbrıs Türk Hukuk Sistemi, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 57(2), s.254, 255.

Kıbrıs Türk Yönetimi"ni, 13 Şubat 1975 tarihinde "Kıbrıs Türk Federe Devleti"ni ve 15 Kasım 1983 tarihinde "Kuzey Kıbrıs Türk Cumhuriyeti"ni kurmuşlardır.[200]

Yukarıda yer verilen tarihsel gelişim süreci ile ilgili kısa açıklamalardan da anlaşılacağı gibi KKTC'nin hukuk sistemi, tek bir devlet çatısı altında kesintisiz bir şekilde oluşmamıştır.[201] Ada üstünde hakimiyet kuran her devlet, Kıbrıs Hukuk Sistemini etkilemiştir fakat 82 yıllık hakimiyeti olan İngiltere'nin etkisi daha büyük olmuştur. Adanın hukuk sisteminin temelinde İngiliz Hukuk Sistemi yatmaktadır.[202]

1985 yılında oluşturulan Kuzey Kıbrıs Türk Cumhuriyeti Anayasası'ndaki devlet yapılanmasının, Türkiye Cumhuriyeti'nin devlet yapılanmasına doğru eğilim gösterdiği anlaşılmaktadır. Zira; öngörülen yasaların Türkiye Cumhuriyeti'nde yürürlükte olan yasalardan etkilenilerek yapılması ya da kimi zaman tamamen kopyalanması neticesinde oluşan Hukuk Sistemi, Türkiye Cumhuriyeti'nin diğer bir deyişle Kara Avrupası Hukuk Sisteminin Kuzey Kıbrıs'ın hukuk sisteminin şekillenmesinde etkili olduğunu göstermektedir.[203]

Bugün dünyada Anglosakson Hukuk Sistemi ve Kontinental Hukuk Sistemi olmak üzere 2 farklı hukuk sistemi uygulanmaktadır. Anglosakson Hukuk Sistemi, İngiltere ve tüm eski İngiliz kolonilerinde uygulanan bir hukuk sistemidir. Bazı istisnalar dışında geriye kalan ülkelerde Kontinental Hukuk Sistemi

---

[200] Kuzey Kıbrıs'ın tarihsel gelişimi için bkz. Turhan, s. 255; Arıklı, E. (2011) Günümüzdeki Türk Halkları ve Tarihleri, Ankara: Nüans Kitabevi, s.265-274.

[201] Turhan, s. 281; Ekinci, B. E. (2016) Kuzey Kıbrıs Türk Cumhuriyeti Yüksek Mahkemesi Kararlarında Hukuk Devleti İlkesi, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 65(3), s.724.

[202] Türkiye Ekonomi Politikaları Araştırma Vakfı (2010) KKTC'de Yasa Hazırlama ve Yasa Yapma Süreci Kurumsal ve Fonksiyonel Analizi: <https://www.tepav.org.tr/upload/files/14550067272.KKTC_Enerji_Sektorunun_Kurumsal_ve_Fonksiyonel_Analizi.pdf> son erişim 07.04.2019; Necatigil, Z. (1988) *Kuzey Kıbrıs Türk Cumhuriyetinde Anayasa ve Yönetim Hukuku*, İstanbul, Çavuşoğlu Basım ve Yayım A.S., s.1; Kuzey Kıbrıs'ın hukuk sistemi gelişimi için bkz. Turhan.

[203] Türkiye Ekonomi Politikaları Araştırma Vakfı (2010) KKTC'de Yasa Hazırlama ve Yasa Yapma Süreci Kurumsal ve Fonksiyonel Analizi: <https://www.tepav.org.tr/upload/files/14550067272.KKTC_Enerji_Sektorunun_Kurumsal_ve_Fonksiyonel_Analizi.pdf> son erişim 07.04.2019.

uygulanmaktadır. Bu açıdan bakıldığında KKTC'de, eski bir İngiliz Kolonisi olarak Anglosakson Hukuk Sistemini uygulanmakla beraber, Türkiye Cumhuriyeti ile ilgili olan yakınlığından ötürü Kontinental Hukuk Sisteminden izler olduğu da görülmektedir.[204]

KKTC Anayasa Mahkemesi, 2005 yılında vermiş olduğu bir karar ile[205] KKTC'de uygulanmakta olan hukuk sistemini şu şekilde açıklar; "KKTC'de İngiliz usul yasalarını yani Anglosakson Hukuk Sistemini uygulamaktayız. Anayasa Mahkememiz, Anayasa Hukuku açısından Türkiye Hukukunu izlemekle birlikte usul hukuku ve prosedür açısından İngiliz hukukunu uygulamaya devam etmektedir."[206]

3.2. Kıbrıs Hukukunda Kişisel Veriler Hakkındaki Düzenlemenin Gelişimi

KKTC Anayasası kişisel hak ve hürriyetleri kayıt altına alarak çağdaş ülkeler seviyesindeki noktaya yükseltmiştir. Anayasa'nın 11. maddesi, temel hak ve özgürlüklerin özü ve bunların nasıl sınırlandırılabileceğini anlatırken yine Anayasa'nın 12. maddesi temel hak ve özgürlükler ile yetkilerin kötüye kullanılmamasını ilke olarak ortaya koymuştur.

Madde 11; "*Temel hak ve özgürlükler özüne dokunmadan kamu yararı, kamu düzeni, genel ahlak, sosyal adalet, ulusal güvenlik, genel sağlık ve kişilerin can ve mal güvenliğini sağlamak gibi nedenlerle, ancak yasalarla kısıtlanabilir*"

Madde 12; "*bu Anayasa'nın hiçbir kuralı herhangi bir gerçek veya tüzel kişiye, zümre veya sınıfa bu Anayasayla güvence altına alınan KKTC ve Kıbrıs Türk*

---

[204] Erginel, T. (2018) KKTC Yargısı, www.tanererginel.com: <http://www.tanererginel.com/> son erişim 28.03.2019.
[205] Anayasa Mahkemesi'nin 05.05.2005 tarihli 5/2003 (D. 1/2005) sayılı kararı, s.6.
[206] Ekinci, s.724-725.

halkının hak ve statüsünün değiştirilmesini veya bu anayasanın kurduğu düzenin yok edilmesini veya tanınan temel hak ve özgürlüklerin ortadan kaldırılmasını amaçlayan hareketlere girişmek ve faaliyetlerde bulunmak hak ve yetkisini verir biçimde anlaşılamaz ve yorumlanamaz"

Kişisel verilerin işlenmesinin Anayasa'da yer alması hususuna bakıldığında, KKTC Anayasası'nda böyle bir yasak bulunmadığı görülmektedir. Örneğin, TC Anayasası'nda 2010 yılında yapılan Anayasa değişikliğinde kişisel verilerin korunması Anayasal bir hak olarak mevzuata girmiştir. Özel hayatın gizliliği ve korunmasına ilişkin 20. maddenin 3. fıkrası "*herkes kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*" şeklindedir. Bu Anayasa değişikliğinin üzerinden uzunca bir zaman geçtikten sonra kişisel verilerin korunmasıyla ilgili 6698 Sayılı Kişisel verileri Korunması Kanunu 07 Nisan 2016 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Bu yasa ile birlikte Ceza Kanunu, Medeni Kanun, Vergi Usul Kanunu, İş Kanunu gibi mevzuattaki birçok kanun, Tüzük ve Yönetmelikler de değiştirilmiştir.

KKTC Anayasası'nın bu ve buna benzer birçok konuda Anayasa değişikliği gündeme gelmiş ama Anayasa'nın değiştirilmesi çok zor kurallara bağlı olduğu için KKTC Anayasasında herhangi bir değişiklik yapılamamıştır.

KKTC Anayasası'nın 90/5 maddesine göre, usulüne uygun olarak yürürlüğe konulan Uluslararası Anlaşmalar yasa hükmündedir. Bunlar hakkında Anayasa'ya aykırılık iddiasında bulunulamaz. Bu konuda Anayasa Mahkemesi'ne başvurulamaz.

1960 yılında kurulan Kıbrıs Cumhuriyeti de 1962 yılında yürürlüğe koyduğu 39/1962 Sayılı Yasa ile Avrupa İnsan Hakları Sözleşmesini Kıbrıs Cumhuriyeti'nin bir iç hukuku haline getirmiştir. KKTC'nin ilanından önce kurulmuş olan Kıbrıs Türk Federe Devleti Anayasası'nın geçici 1. maddesi 1960 yılında kurulmuş olan Kıbrıs Cumhuriyeti yasalarının, 1967 yılında Kıbrıslı Türklerin kurmuş olduğu Kıbrıs Türk Yönetimi mevzuatının ve tadillerinin ve son olarak Otonom Kıbrıs Türk Yönetiminin çıkardığı mevzuata uygun bütün yasalar KKTC Hukuk sisteminin bir parçası sayılmıştır. KTFD Anayasası'nın geçici 1. maddesi şu şekildedir: "16 Ağustos 1960 tarihli ve bu Anayasa'ya uygun olarak, 21 Aralık 1960 tarihine kadar kabul edilmiş mevzuatın; 28 Aralık 1967 tarihli Kıbrıs Türk Yönetimi temel kurallarının ve tadillerinin ve bunlara uygun olarak kabul edilmiş mevzuatın; Otonom Kıbrıs Türk Yönetimi Yürütme Kurulu ve Meclisi'nin 13 ve 18 Şubat 1975 tarihlerinde birleşik olarak yaptıkları toplantılarda alınan kararların ve bunlara uygun olarak yaptıkları toplantılarda alınan kararların ve bunlara uygun olarak kabul edilmiş mevzuatın; bu Anayasa uyarınca konulacak yasalara aykırı olmayanları, yürürlükte kalır."

KKTC her ne kadar AB tarafından tanınmasa da KKTC De Facto olarak tanınmakta ve Türkiye'nin bir alt yönetimi[207] olarak değerlendirilmektedir. Nitekim AİHM çeşitli tarihlerde verdiği kararlarda KKTC'yi Türkiye'nin bir alt yönetimi olarak kabul etmiş ve KKTC'deki hukuk ihlalleri dolayısı ile Türkiye'yi cezalandırmıştır. Bu durum bugün de geçerlidir. Bu kararlardan en önemlileri; AİHM'in Türkiye aleyhine 18.12.1996 tarihli *Loizidou* kararı, AİHM'in Türkiye aleyhine 31.3.2005 tarihli *Adalı* kararı, AİHM'in Türkiye aleyhine 6.7.2009 tarihli *Amer* kararı, AİHM'in Türkiye aleyhine 20.6.2011 tarihli *Elewa* kararı, olarak listelenebilir.

[207] 1974 Barış Harekatı'ndan sonra Kuzey'de mal bırakan Rumlar, Türkiye Cumhuriyeti'nin AİHM'nin kararlarını kabul edeceğini açıklamasından sonra AİHM'ne başvurarak Kuzey'deki mallarına ulaşamadıklarını ve kullanamadıklarını iddia ederek çeşitli davalar açmışlardı. AİHM pilot dava olarak seçtiği Loizidou davasında şu karara vardı; a- Kıbrıs'taki tek meşru hükümet Kıbrıs Cumhuriyeti'dir. Kuzey'deki yönetim AB ve AİHM tarafından tanınmamaktadır. b- TC, Kuzey Kıbrıs'ta dolaylı da olsa etkili kontrol kullanmaktadır. Bu sebepten dolayı Kıbrıslı Rumların Kuzey Kıbrıs'taki mülklerine ilişkin haklarının ihlali nedeniyle AİHM'de açılan davalarda Davalı statüsündedir. Gerek Loizidou ve gerek ondan sonraki Aresti ve Demoglos kararlarında KKTC'yi Türkiye'nin alt yönetimi olarak kabul etmiştir.

Kıbrıs Cumhuriyeti aleyhine verilen kararlara ise, AİHM'in Kıbrıs Cumhuriyeti'ne karşı 16.7.2002 tarihli *Selim* kararı örnek gösterilebilir. AİHM'in Türkiye ve Kıbrıs Cumhuriyeti'ne karşı 4.4.2017 tarihli *Güzelyurtlu* kararında ise hem Türkiye hem de Kıbrıs Cumhuriyeti mahkum edilmiştir.

AİHM'nin bu tür kararları ve KKTC'ye yaklaşımı şüphesiz KKTC siyasi makamları tarafından sert tepki görmüştür. KKTC Yargıtay/Ceza, 23.2.2001 tarihinde 2/2001 sayılı davanın kararında bu konu hakkında şu notu düşmüştür: "Görüleceği gibi 39/62 Sayılı Yasa KKTC'de halen yürürlüktedir ve Avrupa İnsan Hakları Sözleşmesi bizim iç hukukumuzun bir parçasıdır. Bu durum KKTC'nin Avrupa İnsan Hakları Sözleşmesine bağlı Avrupa Konseyi üyesi devletlerden biri olduğunu göstermektedir. Burada sorun, Avrupa Konseyi'nin KKTC'yi değil Kıbrıs Rum yönetimini üye olarak kabul etmesidir. Halbuki Kıbrıs Cumhuriyeti, iki toplum liderinin imzalarıyla kurulmuş bir ortaklık devleti idi. 21 Aralık 1963'de başlayan olaylar Kıbrıs Cumhuriyeti'nin ikiye bölünmesine neden olmuştur. Yasal açıdan Anayasa'yı değiştirmek isteyen ve zorla değiştirmeye teşebbüs eden Rum Yönetimi'nin değil, değişikliğe karşı direnen Türk Devleti'nin Kıbrıs Cumhuriyeti'nin devamı ve mirasçısı olması gerekiyordu. Buna rağmen Avrupa Konseyi, Rum Yönetimi'ni Kıbrıs Cumhuriyeti'nin devamı olarak tanımıştır. Ne var ki tanıma siyasi bir karar olup yasal bir karar değildir. Bu nedenle KKTC'nin Kıbrıs Cumhuriyeti'nin yasal devamı ve mirasçısı olduğunu, dolayısıyla Avrupa İnsan Hakları Sözleşmesi'ni uygulayan bir Konsey üyesi olduğunu, yasal bir zeminde öne sürmek mümkündür. Örneğin; bu iddia Avrupa İnsan Hakları Mahkemesi'nde tartışılabilir."[208] Bize göre KKTC Yargıtayı'nın bu gerekçeli hukuk kararı siyasiler için de önemli bir veridir.

3.3 KKTC'de Kişisel Verilerin Korunması Yasa Çalışmaları

[208] Ayrıca bkz. Necatigil, Z. M. (2015) *KKTC Cumhuriyeti'nde Anayasa ve Yönetim Hukuku*, Işık Kitabevi Yayınları, Lefkoşa, s. 42.

Kişisel verilerin korunması ile ilgili yasa tasarısı KKTC Cumhuriyet Meclisi Hukuk ve Siyasi İşler Komitesi'nin gündemine 21 Nisan 2006 tarihinde gelmiştir. Komite 4 Milletvekilinden oluşmuştu. O tarihlerde muhalefet partileri Meclisi boykot ettiği için Komitede muhalefete mensup Milletvekilleri bulunmuyordu.

Yasa tasarısının genel gerekçesinde bu yasanın amacının AB ile uyumu sağlamak olduğu şu cümleler ile açıklanmaktadır; "Avrupa Birliği, üyelerinin verilerin korunması mevzuatları arasındaki farklılık ve çelişkileri gidererek uyum sağlamak amacı ile 24 Ekim 1995 tarih ve 95/46/EC Sayılı Konsey Direktifini kabul etmiştir. İşbu yasa tasarısının hazırlık çalışmalarında söz konusu Avrupa Birliği Direktifi de göz önünde tutulmuştur."

Komite Başkanı mutat olduğu üzere her yasada olduğu gibi, bilirkişi ve bu konuda fikir beyan etmek isteyen herkesi Komite toplantısına davet edip onların görüş ve düşüncelerini almıştır. İlgili Komite'nin tutanaklardan anlaşıldığı üzere, yasa tasarısını hazırlayanlar AB mevzuatına uygun olarak bu yasa tasarısını önce Bakanlar Kuruluna ve oradan da doğrudan Meclise göndermiştir. Komitedeki 4 Milletvekilinin konu ile ilgili bilgilendirilmedikleri ya da konuya hakim olmadıkları ve komiteye katılan konuklara sorular sorarak bir takım bilgiler aldıkları görülmektedir.

KKTC'de yasalar hazırlanırken Hükümet genellikle kendisine Hukuk Danışmanlığı yapan Başsavcılığa yasa tasarısını gönderir ve Anayasaya uygun olup olmadığı konusunda görüş sorar. Bu yasa tasarısı da Başsavcılığa gönderilerek hukuki görüşü sorulmuştur. Başsavcılık ise verdiği görüşte yasa tasarısının birkaç noktada Anayasa'ya aykırı olduğunu beyan etmiştir. 7 Aralık 2006 tarihinde KKTC Cumhuriyet Meclisi Hukuk ve Siyasi İşler Komitesi toplantısına katılan görüş sahibi Başsavcı Yardımcısı komite üyelerine Anayasa'ya aykırılığı şu şekilde izah etmiştir; "... Bu yasaya baktığımızda bu verilerin derlenmesi ve işlenmesi ile ilgili hükümler de ihtiva etmektedir. Ve tabi yine de tekrarlamakta fayda var. Anayasanın

19. maddesi tahtında ben bu maddelerin özellikle kişisel veri ve hassas verilerin, kişilerin onayı olmadan, onay varsa sorun değil. Ama onayı olmadan bir takım prensiplere hatta istisna koyup da onlara rağmen ya da o istisnaların mevcudiyeti halinde bu bilgilerin derlenip bir yere kaydedilmesi Anayasanın o maddesine aykırı olduğu üzere de ben ısrarlıyım."

Tutanakların tamamını okuduğumuzda Komite toplantısına katılanların kişisel veri ve özel hayat kavramları arasındaki fark ve ilişkinin ayrıntında olmadıkları görülmektedir. Çünkü KKTC Anayasası'nın 19. maddesi tamamen özel hayatın gizliliği ve korunması ile alakalıdır.[209]

Nitekim dönemin Başsavcı Yardımcısı, 29 Kasım 2006 tarihli Komite toplantısında şu itirafta bulunmuştur; "...Yasaya baktığım zaman hakikatten sizin de, arkadaşların da belirttiği gibi teknik bir yasadır ve anlaşılması gerçekten güçtür. Maddeleri birkaç defa okumak zorunda kalıyorsunuz ve yine bir anlam çıkaramıyorsunuz..."

KKTC Savcılık makamı Cumhurbaşkanı'nın, Cumhuriyet Meclisi'nin, Hükümetin ve Devlet Kurumlarının hukuk müşaviridir. Bu makamlar herhangi bir yasal düzenleme, tüzük değişikliği, yönerge ve yönetmelik yayınlamadan önce ihtiyaç duymaları halinde Savcılıktan görüş alır ve buna göre gerekli düzenlemeleri yaparlar. Sayın Başsavcı Yardımcısı gibi tecrübeli bir hukukçunun bu ifadesinden ve tutanakların genel seyrinden de anlaşılıyor ki bırakın KKTC kamuoyunu, yasayı hazırlayanların ve yasa üzerinde hukuki görüş beyan eden Savcılık makamının dahi

[209] KKTC Anayasası md.19; (1) "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Adli kovuşturmanın gerektirdiği istisnalar saklıdır.*" (2) "*Yasanın açıkça gösterdiği durumlarda, usulüne göre verilmiş mahkeme veya yargıç kararı olmadıkça, ulusal güvenlik ve kamu düzeni bakımından gecikmede sakınca bulunan durumlarda da, yasa ile yetkili kılınan merciin emri bulunmadıkça, kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz.*"

kişisel verilerle ilgili temel kavramları ve yasanın ruhunu tam anlamıyla kavrayamamış oldukları görülmektedir.

Yasa'nın yürürlüğe girmesinden bu yana konuyla ilgili KKTC Mahkemelerinde yalnızca bir dava açıldığını ve Yargıtay'a (İstinaf Mahkemesine) götürüldüğünü tespit ettik. Buna göre Girne Kaza Mahkemesinde görülen bir davada emareler ile ilgili Davalılar şahsi elektronik posta yazışmasına gündeme gelmiş ve Mahkemenin emare ile ilgili vermiş olduğu karar istinafa konu olmuştur. Yargıtay mütalaasını yaparken oldukça geniş kapsamlı bir mütalaa hazırlamış ve kişisel verilerin korunması ile ilgili AB müktesebatını da göz önünde bulundurarak içtihat olabilecek bir karar üretmiştir[210]

[210] Yargıtay/Hukuk 7/2019 (D.8-2019).

IV. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI YASASI'NIN GENEL DEĞERLENDİRMESİ

KKTC Bakanlar Kurulu yukarıdaki bölümlerde de anlattığımız gibi AB uyum çalışmaları tahtında 2006 yılında Kişisel Verilerin Koruması Yasa Tasarısını Cumhuriyet Meclisine göndermiştir. Yasa tasarısı, ilgili dönemde AB'de yürürlükte olan 95/46/EC Sayılı Direktif temel alınarak hazırlanmıştır. Cumhuriyet Meclisi alt komitesinde paydaşların da görüşleri doğrultusunda yasa tasarısına son şekli verilmiş ve yasa nihayet 2007 yılında Cumhuriyet Meclisi'nde oylanarak yasalaşmıştır.

İlgili tarihte AB'de yürürlükte olan 95/46/EC Sayılı Direktif, daha sonra AB tarafından kabul edilen GDPR ile yürürlükten kaldırılmıştır. KKTC de esasen AB ile uyum içerisinde bu Yasa'yı GDPR ile uyumlu hale getirmesi gerekirken bu konuda herhangi bir düzenleme yapılmamıştır. Dolayısıyla biz Yasa'yı incelerken GDPR ile mukayese ederek Yasa'nın eksikliklerini ve önerilerimizi ortaya koyacağız.

4.1 Yasa'daki Temel Kavramlar

4.1.1 Bilgiye Konu Kişi

GDPR'da ve Yasa'nın kaynak mevzuatı 95/46/EC Sayılı Direktif'te "data subject" olarak kullanılan bu tanım, Türkiye'de ise "ilgili kişi", bazı çalışmalarda ise "veri sahibi" olarak kullanılmaktadır. Yasa'da ise, "bilgiye konu kişi" ifadesi tercih edilmiştir. Gerek güncel literatürün yakalanması gerekse Yasa'nın

düzenlemelerinin tam karşılayacağı bir tanımın olması açısından Yasa'da yer alan bu kavramın değiştirilmesi gerekliliği ortadadır. Bu kavramın güncel, anlaşılır, düzenlemeleri karşılayan terim "veri sahibi" ya da "ilgili kişi"dir. Bununla beraber, çalışmamızın devamında incelenmekte olan Yasa'da kullanılması tercih edilen "bilgiye konu kişi" terimi kullanılacaktır.

"Bilgiye konu kişi; bilgilerin ait olduğu ve kimliği bilinen veya dolaylı veya dolaysız olarak, özellikle kimlik numarası veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel, siyasal veya sosyal kimliğine dair bir veya birden fazla faktör esas alınarak tespit edilebilen gerçek kişiyi anlatır" şeklinde tanımlanmıştır. Yasa'nın tanımından da görülebileceği üzere, Kişisel Verilerin Korunması Yasası'nın genel ve asli hedefi gerçek kişileri ve gerçek kişilerin mahremiyeti ve kişilik haklarını koruma altına almaktır.

GDPR ise bilgiye konu kişi kavramına "kişisel veri" tanımının içerisinde yer vererek "kimliği belirli veya kimliği belirlenebilir bir kişi" olarak tanımlamıştır. Yasamız gibi GDPR da gerçek kişilerin kişisel verilerinin korunması hakkı ile birlikte gerçek kişilerin temel hak ve özgürlüklerini korumayı amaçlamaktadır.

4.1.2. Kişisel Veri

Yasa, kişisel veriyi GDPR ile aynı şekilde "*kimliği belirli veya kimliği belirlenebilir bir kişiye ilişkin tüm bilgiler*" olarak tanımlamıştır. Bu bilgiler, bir kimsenin kimliğine, sağlık, öğrenim, iş bilgilerine, ırk ve etnik kökenine, dini inancına ve siyasi görüşünü kısaca özel hayat alanı ve gizli hayat alanına dair bilgileri anlatır.[211]

Kişisel veri tanımının hangi tür verileri içerdiği bilgiye konu kişi kavramında sıralanmıştır. Buna göre kişisel veri kavramını da içerisine alan bilgiye konu kişi

[211] Beytar, E. (2017) *İşçinin Kişiliğini ve Kişisel Verilerinin Korunması*, On İki Levha Yayıncılık, İstanbul, s.48.

kavramı "bilgilerin ait olduğu ve kimliği bilinen veya dolaylı veya dolaysız olarak, özellikle kimlik numarası veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel, siyasal veya sosyal kimliğine dair bir veya birden fazla faktör esas alınarak tespit edilebilen gerçek kişiyi anlatır" şeklinde ifade edilmiştir.

Direktif'te de yine iki kavram birleştirilerek; 'kişisel veri' belirli veya belirlenebilir bir gerçek kişiye ('bilgiye konu kişi'); ilişkin her türlü bilgi anlamına gelir. Belirlenebilir gerçek kişi, özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişi" olarak ifade edilmiştir. Gerek Yasa'da gerekse Direktif'te belirtilen kişisel veriyi anlatan tanımlar yalnızca yol gösterici olup, bu sayılanlarla sınırlı değildir. Zira kişisel veri tanımında "her türlü bilgi" veya "tüm bilgiler" denilmektedir.

4.1.3. Hassas Veri

Yasa, mehaz Direktif ile paralel olarak "Hassas veri, ırksal veya etnik kökeni, siyasi görüşleri, dinsel veya diğer inançları ortaya koyan veya cinsel yönelim, sağlık veya cinsel hayatla veya cezai soruşturmayla ilgili konuları açığa çıkaran kişisel verileri anlatır" şeklinde ifade etmiştir.

GDPR'da ise hassas veri tanımına ayrıca gidilmemiş, verilerin işlenmesi şartlarının belirlenmesinde hassas nitelikteki verileri düzenleyerek genel nitelikli kişisel verilere göre daha sıkı koruma öngören şartlar belirlenmiştir. Madde 9'a göre hassas veri; "ırksal veya etnik kökeni, siyasal görüşü, dini veya felsefi inanışları veya sendikaya üyeliğini ortaya koyan kişisel verilerin işlenmesi ve genetik verilerin, biyometrik verilerin bir gerçek kişiyi ayırt edici şekilde tanımlamak

amacıyla ve sağlıkla ilgili verilerin veya bir gerçek kişinin cinsel hayatı veya cinsel tercihine ilişkin veriler" olarak belirlenmiştir.

Yasa'da yapılmış olan tanımın günümüz şartlarına göre yetersiz kaldığı açıktır. İlk olarak, 95/46 Sayılı Direktif'te yer almasına rağmen Yasa'daki tanıma eklenmeyen sendika üyeliği Direktif'in de hassas verilerden saydığı verilerdendir. KKTC'de özellikle siyasi konularda siyasi partiler kadar aktif olan sendikalara üye olan bireylerin, toplum içerisinde karşılaşabilecekleri tepkiler ve önyargılar nedeniyle herhangi bir sendikaya üyeliklerinin hassas verilerden sayılması gerektiği kaçınılmazdır.

Direktif, kişinin ceza mahkumiyetini ve güvenlik tedbirleriyle ile ilgili verileri ayrı bir madde altında düzenlemiştir. 10. madde altında bu tür veriler daha sıkı koruma altına alınarak, bu verilerin yasal işleme şartları altında işlenebilmesi, ancak resmi makamın kontrolü altında veya bilgiye konu kişinin hak ve özgürlüklerinin korunmasına yönelik uygun güvencelerin olması şartıyla mümkün olup, cezai hükümlere ilişkin kapsamlı sicillerin de sadece resmi makamın kontrolü altında tutulabileceği düzenlenmiştir.

Yasamızda düzenlenen hassas veriler tanımında yer alan "cezai soruşturma"nın kapsamının genişletilip Direktif'le paralel olarak temel hak ve özgürlüklerin korunması bağlamında daha sıkı korunmasına yönelik düzenlemenin yapılması gerekliliği kaçınılmazdır. Özellikle cezai soruşturma aşamasında kişilerin suçları sabitlenmemişken, birçok haber kanalı tarafından gerek resim gerekse açık isim paylaşılarak ilgili soruşturma tamamlanmış ve kişinin sanık olduğu kesinleşmiş gibi haberler yapılabilmektedir. Gazetecilik mesleğinin getirdiği haklar ve vatandaşın bilgilendirilmesinin önemli olduğu aşikar olmakla birlikte yukarıdaki bölümde hassas verilerin anlatımında belirtilmiş olduğu gibi, henüz soruşturma aşamasındaki bir meselede kişilerin afişe edilmesi, kişiyi ailevi, sosyal ve mesleki anlamda olumsuz etkileyebilecek mahiyettedir. Kişinin suçsuzluğu kanıtlanmış

veya soruşturmanın kapatılmasına karar verilmiş olsa da kişi halihazırda zarara uğramış olacağından bu olayın etkileri kolayına silinemeyecektir.

Diğer bir hassas veri türü ise 95/46 Sayılı Direktif'te ve dolayısıyla Yasa'da açıkça belirtilmeyen ancak güncel veri türlerinde yer alan genetik ve biyometrik verilerdir. GDPR da "bir gerçek kişinin belirlenmesi amacıyla işlenen genetik ve biyometrik verileri" hassas kişisel veri olarak belirlemiştir.

GDPR, biyometrik verileri, genetik veriler ve sağlık verileri ile ilgili spesifik tanımlamalar yapmıştır. Genetik veri "*bir gerçek kişinin fizyolojisi veya sağlığı hakkında ve özellikle söz konusu gerçek kişinin biyolojik numunesinin analizinden elde edilerek ona özgü bilgi veren, gerçek kişiye ait irsi veya edinilmiş genetik özelliklere ilişkin kişisel veriler*" olarak tanımlanmıştır. Biyometrik veri ise "*bir gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin belirli teknik işleme sonucu elde edilerek, yüz görüntüsü ve daktiloskopik verisi gibi söz konusu gerçek kişinin ayırt edici şekilde tanımlanmasına izin veren ya da bunu teyit eden kişisel veriler*" olarak tanımlanmıştır. Sağlığa ilişkin verileri ise "*aldığı sağlık hizmetleri dahil olmak üzere, bir gerçek kişinin sağlık durumu hakkında bilgi sağlayan, o kişinin fiziksel ve zihinsel sağlığına ilişkin kişisel veriler*" olarak tanımlamıştır. Bu 3 önemli veri türünün tanımlarının spesifik olarak Yasa'da yer alması ve uygulamada herhangi bir tanım veya anlam karışıklığına yol açmaması sağlanmalıdır.

Günümüz dünyasında veri aktarımının kontrolünün zorlaşması, bireylerin kişilik haklarının korunması için gerekli kuralların daha sıkı tutulması gerekliliğini getirmiştir. Bu bakımdan da kişisel verilerin korunmasının önemi artmakla birlikte özellikle hassas verilerin korunması daha dikkat edilmesi gereken veriler haline gelmiştir. Bu nedenle genetik ve biyometrik verilerin de Yasamızda hassas veriler arasında sayılması gerekmekle birlikte bu kavramların ayrıca tanımlanması, kavram karmaşasının önüne geçilmesi anlamında da faydalı olacaktır.

Bu veriler, Türkiye'deki 6698 Sayılı Kanun'da da hassas verilerden sayılmıştır. KKTC-Güney Kıbrıs ve KKTC-TC arasında sık sık hasta nakli yapıldığı ya da vatandaşlarımızın çeşitli sebeplerden dolayı Güney Kıbrıs ve Türkiye hastanelerinde tedavi olmayı tercih ettikleri, KKTC'de yapılan bazı tahlilin Türkiye'de anlaşmalı laboratuvarlara gönderildiği bilinmektedir. Ayrıca KKTC'de de gelişen teknolojiyle gerek iş yerlerinde gerekse çeşitli kurumlarda giriş çıkışların parmak izi alınarak sağlanması, kimlik kartlarının çipli sisteme geçilmesi ise biyometrik resim ile yüz şeklinin işlenmesi, parmak izlerinin alınması ve benzeri birçok örnek, yürürlükte bulunan Yasa'daki tanımın değiştirilmesi gerektiğini ortaya koymaktadır.[212]

Böyle bir durumda, ülkemizde mevcutta uyulan tıbbi verilerin korunması kurallarının güncel dünyada yetersiz olmasının yanında, GDPR'ın getirdiği kuralları uygulamakla yükümlü Güney Kıbrıs ve 6698 sayılı Kanunla veri koruma sağlama yönünde çok ciddi çalışmalar yapan Türkiye karşısında bizim de bu verileri aynı şekilde korumakla yükümlü olacağımız aşikardır.

Yasa'nın 4. maddesinin 15. bendi, sağlık ile ilgili konuları açığa çıkaran verileri hassas veri tanımında yer vermiştir, ancak biyometrik ve genetik veriler için belirtilmiş olduğu gibi, sağlık verilerinin ayrıca tanımlanması, bireyler için en fazla önem arz eden veri sayılabilecek olan sağlık verileri ile ilgili uygulamada yaşanabilecek kavram karmaşaların önlenmesine yardımcı olabilecektir.

4.1.4. Kişisel verilerin işlenmesi

[212] KKTC'den Güney Kıbrıs veya TC'ye tedaviye gitme, çeşitli tahlillerin veya genetik araştırmaların yapılması, Güney Kıbrıs'ta doğum yapma veya göbek bağının Güney Kıbrıs laboratuvarlarına gönderilmesi, aynı şekilde Türkiye'de Kıbrıs'a tüp bebek tedavisi için gelen birçok TC vatandaşının olması yaygındır. Böyle bir durumda söz konusu ülkelerin uymakla oldukları mevzuatla ülkemiz mevzuatında yer alan hassas veri kapsamının paralel olması önemlidir.

Yasa, 95/46/EC Sayılı Direktif'teki tanımlara yakın olarak işleme faaliyetini "kişiye ilişkin tüm verilerin toplanması, kaydedilmesi, işlenmesi, saklanması, silinmesi, değerlendirilmesi, kullanılması, uyarlanması veya değiştirilmesi, durdurulması, yok edilmesi gibi işlevlerden herhangi birisinin, birkaçının veya hepsinin, herhangi bir yöntem ve araç kullanılarak uygulanması" olarak ifade etmiştir.

Kişisel verilerin işlenmesi Direktif'in 4. maddesinde "otomatik yollarla olsun veya olmasın, kişisel veriler veya kişisel veri setleri üzerinde veri toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama (yayınlamak), yayma veya diğer bir şekilde kullanıma sunma, uyumlaştırma veya birleştirme, sınırlama, silme veya imha etme gibi işlem veya işlemler kümesi" olarak sayılmıştır.

95/46/EC Sayılı Direktif ile GDPR'da sıralanan işleme faaliyetlerine bakıldığında hemen hemen aynı eylemleri içeren maddeye yer verildiği görülmektedir. "*structuring*" yani verinin yapılandırılması eylemi GDPR'da olup 95/46/EC Sayılı Direktif'te yer almamaktadır. Bununla birlikte 95/46/EC Sayılı Direktif'te yer alan "*blocking*" *(engelleme)* eylemi yerine GDPR'da "*restriction*" *(sınırlama)* eylemine yer verildiği görülmektedir. Yasa'nın ise 95/46/EC Sayılı Direktif'te yer alan işleme faaliyetlerinden bazılarına yer vermediği görülmektedir. Kişisel verilerin işlenmesi yöntemleri çok çeşitli olduğundan, "gibi işlem veya işlemler kümesi" ifadesiyle sayılan işleme faaliyetinin sayılanlarla sınırlı olmadığı kastedilmektedir. Ancak, bilinen ve uygulamada kullanılan işleme faaliyetlerinin mevzuatlarda açıkça yazılması, uygulamada olabilecek herhangi bir sorunun önüne geçebilir, özellikle kişisel verileri işleyecek kişilerin işleminin hukuka uygun olması ya da verisi işlenecek kişilerin haklarını koruyabilmeleri bakımından Yasa metninin açık olması gerekmektedir. Bununla beraber, konunun mahkemeye havalesi durumunda yapılan işlemin sakatlığı ya da Yasa'da açıkça sayılmayan bir eylem olduğu iddiasıyla yapılan işlemin yasal dayanaktan yoksun şekilde yapıldığı ileri sürülebilir.

4.1.5. Birleştirme

Yasa, "Birleştirme" kavramını "*Birleştirme, bir dosyalama sistemindeki verilerin diğer bir kontrolör veya kontrolörler tarafından tutulan veya aynı kontrolör tarafından başka bir amaçla tutulan verilerle bir araya getirilmesine imkan verecek şekilde işleme bağlı tutulmasını anlatır.*" şeklinde tarif etmektedir. Bu tanımın, 95/46/EC Sayılı Direktif'te ya da GDPR'da yer almadığı ancak Yasamızda bu tanıma yer verildiği görülmektedir.

4.1.6. Kişisel veri dosya sistemi

89/2007 sayılı Yasa'nın 2. maddesine göre, kişisel veri dosya sistemini 95/46/EC Sayılı Direktif ve GDPR ile aynı şekilde "*işlevsel veya coğrafi esaslara göre merkezi veya dağınık olarak bir sistemde muhafaza edilen ve belirli yöntemlerle ulaşılabilen kişisel veri topluluğu*" olarak tanımlamıştır. Veri kayıt sistemleri elektronik ve fiziksel ortamlarda oluşturulabilmektedir.

4.1.7. Kontrolör

89/2007 Sayılı Yasa'da kontrolör kavramı, "*kendi başına veya başkalarıyla birlikte, kişisel verilerin işleme tabi tutulmasının amaç ve yöntemlerini belirleyen, kişisel veri dosya sistemini oluşturma, işletme, denetim hak ve yetkisine sahip olan Kamu Kurum ve Kuruluşları ile gerçek ve tüzel kişileri anlatır.*" şeklinde ifade edilmiştir.

Tanımdan da anlaşıldığı üzere, kontrolör, kişisel verileri elinde tutuyor olmasından dolayı değil, kişisel verilerin işleme amaçlarını ve vasıtalarını belirlemesinden

dolayı bu sıfatı kazanmaktadır. Bir örnekle açıklamak gerekirse, bir firma müşterilerine ait iletişim bilgilerini liste halinde tuttuğunda bu bilgileri ne şekilde kullanacağına karar verdiği için kontrolördür. Firma bu listeyi bir bulut veri tabanında bulunan kendi kontrolündeki hesabına aktardığı zaman hala kontrolör kalmaya devam eder. Bulut veri tabanının sahibi olan firma, kişisel verilerin işlenmesinin amaç ve vasıtalarını belirlemediği için kural olarak kontrolör haline gelmez. Ancak, bulut veri tabanı sahibi olan firma, listede bulunan bilgileri kullanırsa örneğin bu kişilere tanıtım mesajları göndermeye başlarsa böyle bir durumda kontrolör kabul edilecektir.[213]

GDPR'ın 26. maddesinde, iki veya daha fazla kontrolörün işleme amaçlarını ve vasıtalarını birlikte belirledikleri durumlarda, müşterek kontrolör olacakları belirtilmiştir.

GDPR'ın 4. maddesinde bu kişi "Controller" olarak geçmekte ve kişisel verilerin işlenmesinin amaçlarını ve vasıtalarının tek başına veya başkalarıyla birlikte belirleyen kişi olarak ifade edilmiştir. Aynı mevzuata göre bu kişi gerçek veya tüzel kişi olabileceği gibi kamu makamı, kurumu veya bir diğer kamu kuruluşu da olabilecektir.

Kontrolör tanımının 95/46/EC Sayılı Direktif'te yer alan "controller" ifadesinin Türkçeleştirilmiş haliyle Yasa'da yer aldığı görülmektedir. Ancak, bu gibi ifadelerin manasının daha net anlaşılabilir olacağı şekliyle mevzuata alınması, gerek kişilerin gerekse verilerin işlenmesinden sorumlu yükümlülerin yasal zorunlulukları daha net anlayabilmesi açısından önem teşkil etmektedir. Yasa'nın iyileştirilmesi maksadıyla "kontrolör" ifadesinin, TC 6698 Sayılı Kişisel Verileri Koruma Kanunu'nda da yer aldığı gibi "veri sorumlusu" olarak değiştirilmesi önerilmektedir.

---

[213] Develioğlu, s.42.

4.1.8. İşlemci

Kontrolörün kişisel verileri bizzat işlemesi gerekmemektedir. İşlemci, 89/2007 Sayılı Yasa'da "şahsi veriyi kontrolör adına işleyen kişi" olarak tanımlanmıştır. GDPR'da ise "kontrolör adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi kamu kurumu"nun da işlemci olabileceği belirtilmiştir. İşlemci, kişisel verilerin kaydedilmesi, saklanması, sıralanması ve birleştirilmesi gibi işlemenin teknik yönlerini yürütmek üzere kontrolör tarafından görevlendirilen uzmanlaşmış kişi veya kurum olacaktır. Kontrolörün bilgisayar sisteminin güvenlik ve yönetimi ile görevlendirilmiş çalışanı, işlemci olarak düşünülemeyecektir.[214]

4.1.9. Üçüncü Taraf ve Alıcı

89/2007 Sayılı Yasa'da üçüncü taraf "*bilgiye konu kişi, kontrolör ve işlemci haricindeki her türlü kişiyi anlatır.*" şeklinde ifade edilmiştir. Her türlü kişi denilerek genelleme yapılmıştır ancak, Yasa'daki tanımlarda bu ayrım yapılmamış olsa da 8. ve 13. maddelerde alıcı ve alıcı kategorilerinden bahsedilmektedir. Bu nedenle Yasa'da yer alan "üçüncü taraf" ve "alıcı" tarafların ayrımının açık bir şekilde yapılması, verilerin aktarıldığı kişilerin ve bu aktarımda uyulacak kuralların ayrımı açısından önemli olacaktır.

95/46/EC Sayılı Direktif ve GDPR'da yer alan "üçüncü kişi" kavramına bakıldığında "üçüncü kişi", bilgiye konu kişi, kontrolör ve işlemci dışındaki kontrolör ya da işlemcinin doğrudan kontrolü altında kişisel verileri işlemeye

---

[214] Berber, L. K., vd. (2009) *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, İstanbul, Karakter Color AŞ, s.123.

yetkisi olan kişiler haricinde, kişisel verileri işlemeye yetkili olan bir gerçek ya da tüzel kişi, kamu, kurumunu, kuruluşunu ya da diğer herhangi bir organı anlatır. "Alıcı" kavramı ise, üçüncü bir kişi olsun ya da olmasın, kişisel verilerin açıklandığı bir gerçek veya tüzel kişiyi, kamu kurumunu, kuruluşunu ya da diğer herhangi bir organı anlatır.

GDPR'da üçüncü kişi ve alıcı kavramları ayrımına gidilme sebebi, kişisel verilerin üçüncü kişilere açıklanması durumlarında ortaya çıkar. Kişisel verilerin üçüncü kişilere açıklanmasında her zaman bir hukuki dayanak ortaya koyulmalıdır fakat alıcılara yapılan açıklamalarda bu gerekli olmayabilir.[215] Örneğin, kontrolörün şirket çalışanlarına veya diğer bölümlerine kişisel verileri aktarırken, bu işlem için ilgili kişinin yeniden rızasının alınmasına ya da başka bir işleme şartına uygunluk sebebine dayanıyor olması gerekmez.[216] GDPR'da alıcı kavramındaki tanıma ek olarak "Birlik veya üye devlet hukuku uyarınca belirli bir sorgulama çerçevesinde kişisel verileri alabilen kamu kuruluşları alıcı olarak nitelendirilmez; bu verilerin söz konusu kamu kuruluşları tarafından işlenmesi işleme amaçlarına göre geçerli veri koruma kurallarına uygun olarak yapılır" ifadesi yer almaktadır.

4.1.10. Rıza kavramı

Elde edilen kişisel verilerin işlenmesinde bilgiye konu kişinin rızasının alınması yapılacak olan işlemi yasal hale getirir. 89/2007 Sayılı Yasa'da veri işleme şartlarında bilgiye konu kişinin şüpheye sebebiyet vermeyecek şekilde onay vermesi ve hassas veriler için de açık rıza denilmiş fakat açıklayıcı hiçbir tanıma yer verilmemiştir. 95/46/EC Sayılı Direktif'te tanımlar bölümünde bilgiye konu kişinin rızası yer almasına rağmen Yasa'da bu tanıma yer verilmemiş olduğu görülmektedir.

---

[215] Develioğlu, s.43.
[216] Develioğlu, s.44.

GDPR, 95/46/EC Sayılı Direktif'te yer alan tanımla aynı şekilde, 4. maddenin 11. bendi altında 'bilgiye konu kişinin rızası' kavramını bilgiye konu kişinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren, özgür bir şekilde verilmiş, konuya özel, bilgilendirilmiş ve belirsiz olmayan, açık gösterge olduğunu belirtmiştir.

4.1.11. Kişisel Veri Güvenliğinin İhlali

Kişisel verilerin korunmasından bahsedilirken, bu verilerin güvenliğinin sağlanması gerektiğinden de bahsedilmektedir. Bu nedenle, hangi durumların veri güvenliğinin ihlal edilmesi anlamına geldiğinden de bahsedilmelidir. Yasa'da böyle bir tanıma yer verilmediği görülmekle birlikte, "işlemenin gizliliği ve güvenliği" ile ilgili madde içerisinde kontrolörün sorumluluklarından bahsedilirken, belirtilen vakalar sayılmıştır, ancak bir madde özelinde olmayacak şekilde tanımlanması faydalı olacaktır.
GDPR, 4. maddenin 12. bendi altında, kişisel veri ihlalini; "depolanan, aktarılan ya da başka yöntemlerle işlenen kişisel verilerin yasa dışı veya kazara imha edilmesi, kaybolması, değiştirilmesi, ifşa edilmesi ve yetkisiz erişimine yol açan güvenlik ihlali" şeklinde tanımlayarak bir kişisel verinin güvenlik ihlalinden söz edildiğinde ne anlaşılması gerektiğini belirtmiştir.

4.1.12. Bilgi Toplumu Hizmeti

GDPR, bilgi toplumu hizmetinin tanımı ile ilgili Avrupa Parlamentosu ve Avrupa Konseyi'nin 2015/1535 Sayılı Yönerge'nin 1(1) (b) maddesindeki "hizmet" tanımına atıf yapmıştır. Söz konusu Yönerge'ye göre bilgi toplumu hizmeti, uzaktan, elektronik vasıtalarla ve bireyin talebi üzerine ücret karşılığı sunulan hizmettir.

Bu tanımda belirtilen ücret karşılığı hususu ile ilgili olarak belirtilmesi gerekir ki, sunulan hizmetin karşılığında bir ücretin alınmış olması şart olmayıp, normalde ücret karşılığı sağlanan ücret olması yeterlidir. Örneğin, bir sosyal hizmet ağı sunduğu hizmet karşılığında kullanıcılardan bir ücret talep etmese de reklam verenlerden gelir elde ediyorsa, sunduğu hizmet bilgi toplumu hizmeti sayılacaktır.[217]

Bu kavram, özellikle çocuğun rızasının alınması hususunda karşımıza çıkmaktadır. Yasa'ya eklenmesi gerektiği değerlendirilen çocuğun rızası şartlarında yer alabileceğinden, tanımlara eklenmesi faydalı olacaktır.

4.1.13. Anonim Hale Getirme

Verilerin kimliği belirli veya belirlenebilir kişiyle ilişkilendirilemeyecek hale getirilmesi, verilerin anonim hale getirilmesi anlamına gelmektedir. GDPR'ın veri koruma ilke ve kuralları anonim bilgiler için geçerli değildir.[218] Kişisel verilerin işlendikleri amaç doğrultusunda artık ihtiyaç kalmaması halinde, sınırlılık ilkesi gereği silinmesi gerekmektedir. Ancak bazı durumlarda verilerin kişiden bağımsız olarak kullanılması ihtiyacı duyulabilmektedir. Örneğin firmalar istatistik, analiz gibi çalışmalar için bazı verilere ihtiyaç duyabilir. Bu durumda verileri silmek yerine anonim hale getirme yöntemini tercih edebilirler. Bu nedenle bu tanımın Yasamıza girmesi gerekeceği aşikardır.

4.1.14. Psödonimleştirme

[217] Develioğlu, s.54.

[218] Giakoumopoulos, C., vd. (2018) *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union, s.83.

GDPR'ın 4. maddesinin 5. bendi, psödonimleşirme tanımını "*ek bilgilerin ayrı olarak saklanması ve belirli veya belirlenebilir bir gerçek kişiye atfedilmemesini sağlamaya yönelik ve teknik ve organizasyonel tedbirlere tabi olması şartıyla, kişisel verilerin, ek bilgiler olmadan belirli bir ilgili kişiye atfedilemeyeceği şekilde işlenmesi anlamına gelir*" şeklinde ifade etmiştir. Psödonimleştirme yöntemine takma ad vasıtasıyla ya da diğer deyişle sahteleştirme ile verilerin işlenmesi de denilebilir.

Kişisel veriler, isim, doğum tarihi, cinsiyet, adres veya kimliği belirli hale getirebilecek diğer niteliklerdir. Kişisel veride psödonimleştirme süreci, bu nitelikleri psödonim yani takma ad ile yer değiştirilmesi anlamına gelmektedir. GDPR, bu tür psödonim verilerin, anonim verilerin aksine, kişisel veri olduğu kabul etmiştir ve bu veriler veri koruma mevzuatına tabidir. Bununla birlikte, takma isimlendirme veri korumaya yönelik riskleri azaltabilir ancak her şekilde Direktif kapsamında yer alacaktır.[219]

4.1.15. Profilleme

GDPR, kişisel verilerin kullanılması yöntemlerinden olan profilleme tanımına ayrıca yer vererek; profillemeyi "*kişisel verilerin gerçek bir kişiye ilişkin belirli kişisel özellikleri değerlendirmek, özellikle bu gerçek kişinin işteki performansına, ekonomik durumuna, sağlığına, kişisel tercihlerine, ilgi alanlarına, güvenilirliğine, davranışlarına, konumu veya davranışlarına ilişkin hususları analiz veya tahmin etmek için kullanılması şeklinde otomatik vasıtalarla herhangi bir surette işlenmesi anlamına gelir*" şeklinde tanımlanmıştır.

Günümüz teknolojisinde ve şartlarında kişisel verilerin işlenmesi ve yöntemlerinin çoğalması, bu çeşitliliğe duyulan ihtiyacın artmış olduğu gerçeği karşısında bu tür kavramlar Yasa kapsamına alınması gerekmektedir.

---

[219] Giakoumopoulos, s.94.

4.2. Kişisel Verilerin Korunması Yasası'nın Kapsamı

4.2.1. Kapsam

89/2007 sayılı Yasa'nın kapsamını ele alan 4. maddesi, Yasa kapsamını; kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kurum veya kuruluşlar ile gerçek ve tüzel kişiler olarak belirlemiştir. Buradan da anlaşıldığı üzere, kişisel verileri işlenen tüm kişiler ile bu verileri işleyen tüm devlet kurumları, şirketler, avukat, doktor gibi gerçek kişiler bu Yasa hükümlerine tabi olacaklardır. Yasa kapsamının istisnası ise aşağıdaki bölümde değerlendirilecektir.

GDPR'ın kapsamı ise 2. maddesinde ele alınmış ve "Bu Direktif, tamamen veya kısmen otomatik vasıtalarla kişisel verilerin işlenmesi ve bir veri kayıt sisteminin parçası olan veya bir veri kayıt sistemi halinde gelmesi planlanan kişisel verilerin otomatik vasıtalar dışında işlenmesi hallerine uygulanır" denilmiştir. Direktif'teki kişisel veri ve veri sahibi tanımlarına bakıldığında da görülecektir ki Direktif gerçek kişilerin verilerinin korunmasına yönelik hazırlanmıştır.

4.2.2. İstisnalar

Yasa'nın kapsamını düzenleyen 4. maddede, yasaya bir istisna getirilmiş ve buna göre bir gerçek kişi tarafından, herhangi bir ticari veya mesleki kazanç amacı olmaksızın, başkalarına aktarmamak şartıyla ve sadece kendisi tarafından kullanılmak üzere işlenmiş olan kişisel veriler istisna tutulmuş ve Yasa kapsamı dışında sayılmıştır.

Bu istisna kuralı sınırlandırılmazsa tehlikeli boyutlara ulaşabilecek esneklikte yorumlanabilecek bir kuraldır. Dolayısıyla bir kişi kişisel verileri kendisi için işliyor olsa dahi, kimin verilerini işleyebileceği sınırlandırılmamış ve işlediği verileri başkalarına paylaşmamak haricinde herhangi bir koruma sağlama yükümlülüğü getirilmemiştir. Bununla beraber bu kurala uymayan kişiye getirilebilecek yaptırım da havada kalacak, geniş yorumlanan bir madde olduğundan Kurul'un vereceği her karar rahatlıkla itiraza konu olacaktır.

Yasa'da kişisel verilerin işlenebileceği halleri düzenleyen bir istisna maddesi bulunmaması önemli bir eksiklik olarak değerlendirilmektedir. Özellikle devletin kamu güvenliği, milli güvenlik, mali güvenlik gibi nedenlerle ya da yargı makamlarının işleyişleri açısından verilerin güvenliğini korumaları şartıyla kişisel verileri işleyebilmeleri için hak ve yetkilerinin olması gerekmektedir.

GDPR'ın kapsamı için getirilen istisnaya bakıldığında; bir gerçek kişi tarafından yalnızca kişisel veya ailevi faaliyetler sırasında yapılan işleme ve yetkili makamlar tarafından kamu güvenliğine yönelik tehditlere karşı önlem alınması ve engellenmeleri dahil olmak üzere, yetkili makamlarca suçların engellenmesi, soruşturulması, saptanması ya da kovuşturulması veya cezaları uygulanması maksadıyla verilerin işlenmesi halinde Direktif kuralları uygulanmayacaktır.

Görüldüğü üzere gerek GDPR'a uyum gerekse verilerin tam korunmasının sağlanması maksadıyla Yasa'nın getirdiği istisna düzenlemesi yeniden düzenlenmeli, diğer yandan ise kamu güvenliği, milli güvenlik gibi nedenlerden dolayı verilerin işlenmesinin Yasa kapsamının dışında tutulabileceği açık bir şekilde düzenlenmelidir.

4.2.3. Kısmi İstisnalar

Yasa'nın belirli maddeleri kısmi istisnalara da yer vermektedir. Kişisel verilerin işlenmesinde uygulanması gereken ilkeler arasında sayılan verilerin tutulma süresinin istisnası olarak Başkan'ın kişisel verilerin tarihsel, bilimsel veya istatistiki amaçlarla saklanmasına izin verebilmesidir.

Diğer bir kısmi istisna, yine aynı maddede, ilkelere aykırı olarak işlenen verilerin imhası hususunda Başkan'ın tarihsel veya bilimsel amaçlı muhafazasının Milli Arşiv ve Araştırma Dairesi (Kuruluş, Görev ve Çalışma Esasları) Yasası ile oluşturulan Milli Arşiv Kurulu Başkanı tarafından gerekli görmesi halinde bu verilerin Milli Arşivde saklanmasına izin verebilmesidir. Bu kabul edilemeyecek bir istisna olarak değerlendirilmektedir. Kamu güvenliği, bir kimsenin hayati tehlikesinin olduğu durumlar gibi önemli kabul edilebilecek durumlar haricinde hangi sebeple olursa olsun kişisel verilerin işlenmesinde uyulması gereken temel ilkelerin göz ardı edilmesini, tabiri caizse ilkelerin çiğnenmesini yasal kılacak hiçbir istisna kabul görmemelidir. Ayrıca bu madde özelinde düşünüldüğünde, ilkelere aykırı işlenmiş veya derlenmiş kişisel verilerin muhafazasının gerekli görülmesi hususu Milli Arşiv Kurulu Başkanı'nın hak ve yetkisine girmemelidir, zira böyle bir talep gelmesi halinde Kişisel Verileri Koruma Kurul Başkanı'nın bu talebi reddetme ihtimali düşük görülmekte, Başkan'ın takdir yetkisini başka bir Kurul Başkanı'nın talebi üzerine doğrudan kabul edecek şekilde kullanmasını sağlayacak bir ortam oluşturacağı muhakkaktır.

Bir diğer istisna, hassas verilerin işlenmesi şartının istisnası olan sağlık verilerinin işlenmesidir. Bu tür hassas verilerin meslek olarak sağlık hizmeti veren ve gizlilik yükümlülüğü bulunan ya da bu tür davranış ilkeleriyle yükümlü olan kişi veya kurumlarca derlenebilmesi veya işlenebilmesidir. Örneğin, doktor hasta gizliliği, psikolog danışan gizliliği, eczacı müşteri gizliliği, hastane/klinik hasta gizliliği gibi kişilerin sağlıklarıyla ilgili verileri korumakla yükümlü olan kişiler mesleklerini layıkıyla yapabilmeleri açısından sağlık verilerini işlemek zorunda olabilirler. Böyle bir durumda bilgiye konu kişinin bu verilerinin işlenmesine onay vermese dahi verinin işlenmesi hukuken mümkün olmaktadır. Fakat böyle bir durumda,

özellikle en hassas verilerden sayılan sağlık verilerinin güvenliğinin ve gizliliğinin sağlanması koşullarının sıkı denetime sahip olması gerekmektedir. Özellikle KKTC gibi küçük ve herkesin birbirini tanıdığı bir ada ülkesinde bir kişiye ait sağlık verisinin hızla yayılmasının olası olduğu göz önünde bulundurulduğunda, kişileri toplumdan dışlayabilecek, kişileri belki de intihara sürükleyebilecek ölçüde önemli verilerin gizliliğinin önemli olması yadsınamaz bir gerçektir.

Yasa'da yer alan bir diğer kısmi istisna Bilgilendirme yükümlülüğünü düzenleyen 13. Maddede yer almaktadır. Madddede üç kısmi istisna bulunmaktadır. Bunlardan ilki bilginin üçüncü taraflardan alınması halinde bilgiye konu kişiye bilginin kaydı sırasında veya bilginin üçüncü taraflara iletilmesinin beklendiği sırada yapılacak olan bilgilendirmenin, işlemenin istatistiki ve tarihi amaçlarla veya bilimsel araştırma amacıyla yapılması durumunda eğer bilgiye konu kişiyi haberdar etmek imkansız ise ya da onu haberdar etmek orantısız bir çaba gerektirmekteyse veyahut bilginin iletilmesi başka bir yasa ile mümkünse yapılmayabilir fakat her koşulda bu bilgilendirmeden muafiyet durumu Başkan'dan alınacak izni bağlıdır. Bu fıkrada belirtilen "bilginin başka bir yasa ile iletilmesi mümkünse" cümlesinin ne ifade etmekte olduğu, yasa koyucunun bu kuralla neyi amaçladığının net olmadığı değerlendirilmektedir.

Bilgilendirme yükümlülüğü maddesinin ikinci istisnası ise, Devletin savunması, ulusal ihtiyaçları veya ulusal güvenliği veya cezai suçların önlenmesi, tespit edilmesi, soruşturulması ve kovuşturulması maksadıyla kontrolörün yapacağı başvuru ve Başkan'ın kararı üzerine bilgilendirme yükümlülüğünün kısmen veya tamamen göz ardı edilmesidir. Yasa'nın bu istisnası son derece yerindedir.

İlgili maddenin üçüncü ve son istisnası ise, gazetecilik mesleğini icra eden kişiler içindir. Bilgiye konu kişinin erişim ve itiraz hakkını düzenleyen maddelerdeki haklarının korunması kaydıyla, kişinin mahremiyet hakkı ve aile yaşamının ihlal edilmemesi koşuluyla ve yalnızca gazetecilik amacıyla derlemenin yapılması durumunda, gazetecinin bilgiye konu kişiyi haberdar etme yükümlülüğü

bulunmamaktadır. Sağlık verilerini işleyen kişilerin istisnasında da belirtilmiş olduğu gibi, bu verilerin yalnızca bu amaçlar doğrultusunda kullanılmasının denetlenmesinin ve bu haberciliğin kişinin mahremiyetine ve aile hayatına zarar verip vermediğinin tespitinin önemine vurgu yapılmalıdır. Aksi halde, verilebilecek olası yaptırım kararları her türlü itiraza açık olacak ve bilgiye konu kişinin geriye dönüşü imkansız zararlara uğraması kaçınılmaz olacaktır.

4.3. Genel İlkeler

Kişisel verilerin işlenmesinde uyulması gereken ilkeler ile ilgili olarak, Yasa 95/46/EC Sayılı Direktif'te öngörülen ilkelere dayanarak 5. maddede yer alan ilkeleri düzenlemiştir. Direktif'in 6. maddesinin 1. bendinde yer alıp GDPR'da da korunan ilkelerden olan "kişisel verinin toplandıkları ve/veya işlendikleri amaçlarla ilişkili olmak kaydıyla yeterli ve ilgili olmalı; aşırı olmamalıdır" ilkesinin Yasa'da yer verilmediği görülmektedir. Yasa'ya göre kişisel veriler işlenirken kontrolör aşağıdaki ilkelere uymak zorundadır;

- Verilerin yasal ve adil yoldan elde edilmesi ve işlenmesi;

- Verilerin belirli, açık ve meşru amaçlarla derlenmesi ve bu amaçlara aykırı şekillerde işlem görmemesi;

- Verilerin doğru ve gerektiğinde güncel olması;

- Kişisel verilerin işlenme ve derlenme amaçları yerine getirilmesi sağlanırken Başkan'ın takdiriyle verinin sahibinin kimliğinin belirlenmesine izin verecek şekilde gereğinden uzun bir süre tutulmaması. Bu sürenin bitiminde Başkan'ın bilgiye konu kişinin veya üçüncü tarafın haklarına halel gelmediğine kanaat getirmesi durumunda, gerekçeli bir kararla kişisel verinin tarihsel, bilimsel veya istatistiki amaçlarla muhafazasına izin vermesi halinde veriler tutulmaya devam edilebilmektedir.

Bu ilkelere aykırı biçimde derlenmiş veya işlenmeye devam edilmiş kişisel veriler, kontrolör tarafından imha edilmelidir. Başkan, resen veya bir şikayet üzerine bu kurallara aykırı hareket edildiğini belirlemesi durumunda derleme veya işlemenin durdurulması ve derlenmiş veya işlenmiş olan kişisel verinin imha edilmesi talimatını verir. Bu verilerin tarihsel veya bilimsel amaçlı muhafazasının Milli Arşiv ve Araştırma Dairesi (Kuruluş, Görev ve Çalışma Esasları) Yasası ile oluşturulan Milli Arşiv Kurulu Başkanı tarafından gerekli görülmesi halinde Başkan, bunların Milli Arşivde muhafazasına izin verebilir.

GDPR'da yer verilen ilkelere gelince, temel çerçevede 95/46/EC Sayılı Direktif'te yer alan prensiplerle benzerdir. Ancak GDPR bir yenilik getirerek şeffaflık prensibini, verilerin güvenliğini ve kontrolörün sorumluluğunu gerektiren prensipleri de kişisel verilerin işlenmesinde uyulması gereken ilkeler kapsamına dahil etmiştir. GDPR'ın 5. maddesinin 1. bendinde öngördüğü prensipler şu şekildedir;

- Madde 5 (1) (a): Hukuka uygunluk, adalet ve şeffaflık; kişisel veriler hukuka ve hakkaniyete uygun olarak ve veri sahibiyle kişiyle bağlantılı olarak şeffaf bir şekilde işlenmelidir.

- Madde 5 (1) (b): Amacın sınırlı olması; Kişisel veriler belirli, açık ve meşru amaçlar için toplanmalı ve bu amaçlara uygun olmayacak şekilde işlenmemelidir. 89 (1) madde kapsamında kamu yararı için arşivleme amacıyla veya bilimsel veya tarihi veya istatistiki amaçlarla işleme, toplanma amacına aykırı yapılmış işleme olarak kabul edilmez.[220]

[220] Ayrıca GDPR madde 89 (1) der ki; "kamu yararı için arşivleme yapılması amacıyla, bilimsel veya tarihi araştırma amacıyla veya istatistiksel amaçla işlemeler, bu Tüzük'e uygun olarak kişinin hak ve güvencelerine yönelik uygun güvencelere tabi olmalıdır. Bu güvenceler, özellikle veri minimizasyonu prensibine uyulmasını sağlamak için alınanlar başta olmak üzere teknik ve organizasyonel tedbirlerin alınmasını sağlar. Bu güvenceler, bu şekilde amaçların gerçekleştirebilmesi şartıyla psödonimizasyonu da içerebilir. Söz konusu amaçların, veri sahiplerinin kimliklerinin saptanmasına imkan vermemiş veya artık imkan vermeyen sonraki işlemeler ile gerçekleştirilebilmesi halinde, bu amaçlar ilgili yöntemle gerçekleştirilir."

- Madde 5 (1) (c): Verilerin minimizasyonu; veriler, yeterli, ilgili ve işlendikleri amaçla bağlantılı olarak gereken şekilde sınırlı olarak işlenmelidir.

- Madde 5 (1) (d): Doğruluk; veriler, doğru ve gerektiği hallerde güncel olarak tutulmalıdır. Veriler, işlendikleri amaçlar göz önünde bulundurularak, yanlış olan verilerin gecikmeksizin silinmesinin veya düzeltilmesinin sağlanması için makul tüm adımlar atılmalıdır.

- Madde 5 (1) (e): Sınırlı süre saklama; veriler, işlendikleri amacın gerektirdiği süreyi aşmayacak biçimde, veri sahibinin belirlenmesini sağlayacak şekilde tutulmalıdır. Kişisel verilerin 89 (1) madde uyarınca kamu yararı için arşivleme amacıyla veya bilimsel veya tarihi veya istatistiki amaçlarla işleneceklerinde, veri sahibinin hak ve özgürlüklerin güvence altına alınması için GDPR tarafından belirlenmiş olan teknik ve organizasyonel önlemlerin alınması suretiyle daha uzun süre saklanabilir.

- Madde 5 (1) (f): Gizlilik ve bütünlük; verilerin, yetkisiz ve hukuka aykırı işlenmesi, kazara kaybı, imhası veya zarar görmesi ihtimallerine karşı uygun teknik ve organizasyonel önlemlerin alınması dahil, verilerin güvenliğini sağlayacak şekilde işlenmelidir.

- Madde 5 (2): Hesap verilebilirlik; Kontrolör, yukarıda belirtilen ilkelere uygun davranmalı ve buna uygun davrandığını gösterebilmelidir.

Prensiplerin detayına bakıldığında, verilerin hukuka uygun olarak işlenmesi, sonraki bölümde incelenecek olan yasal işleme şartlarının olması halinde karşılanmaktadır. Verilerin şeffaflık prensibiyle işlenmesi ise GDPR'da detaylı şekilde düzenlenmektedir. 12. maddenin 1. bendine göre kontrolör, kişisel verilerin işlenmesi ile ilgili veri sahibine yapması gereken tüm, özellikle bir çocuğa iletilen bildirimlerde, kısa, şeffaf, anlaşılır ve kolay erişilir bir şekilde açık ve sade bir dil kullanarak sağlamak için makul önlemleri almalıdır. Vatandaşların, özellikle çocukların anlayabileceği açıklıkta bildirimlerin yapılması, bireylerin sahip oldukları hakları bilmeleri, bireylerin verilerinin işlenmesine izin verip vermeme

noktasında bilgilendirilmiş olmaları zorunlu olmalıdır. Bu sebeple Yasa'da yer alan prensipler arasına şeffaflık ilkesinin de eklenmesi önemlidir.

Diğer bir prensip olan verilerin belirli, açık ve meşru amaçlarla derlenmesi yani amaçla sınırlı olma prensibine göre, verilerin işleme amaçları işleme yapılmadan önce belirlenmelidir. Kamu yararı için arşivleme, bilimsel veya tarihsel veya istatistiksel araştırma amaçları için öngörülen istisna dışında, önceden belirlenmiş amaçtan farklı bir amaçla veri işlenemez. Ayrıca, veriler elde edilirken belirlenmiş amaçların arından, daha sonraki bir zamanda işleme yapıldığı takdirde, işleme de aynı amaç doğrultusunda olmalıdır.

Örneğin, bir havayolu şirketi, uçuşu düzgün şekilde ayarlayabilmek için yolcularından bilgi toplamalıdır. Böyle bir durumda olan havayolu şirketi, yolcularının koltuk numarası, tekerlekli sandalye ihtiyacı gibi özel fiziksel engeller, helal et gibi özel yiyecek tercihleri gibi verilere ihtiyaç duyar. Bu şirket, yolcuların isim kayıtlarını varış limanındaki göçmenlik bürosuna aktarmak isterse, böyle bir durumda veriler ilk baştaki amaçtan farklı olarak, göçmenlik kontrolü amacı için kullanılmış olur. Verilerin göçmenlik bürosuna aktarılması yeni ve ayrı bir yasal dayanak gerektirecektir.[221]

95/46/EC Sayılı Direktif'te olmasına rağmen Yasa'da yer verilmeyen ancak Yasa'da belirtilmiş ilkelere dahil edilmesi gereken veri minimizasyonu yani verilerin yeterli, ilgili ve sınırlı şekilde, işlendikleri amaçla bağlantılı olacak şekilde işlenmesi ilkesinde, veri işlenmesi meşru bir amacı yerine getirmek için gerekli olduğu ölçüde sınırlandırılmalıdır. İşlemin başka şekilde yerine getirilmesinin mümkün olmaması durumunda kişisel verilerin işlenmesinin zorunlu ise kişisel veriler işlenmelidir.[222] Böyle bir durumda ise amaca ulaşmak için gerekli olan en az sayıda verinin kullanılması gerekmektedir. Bu yaklaşımla, gereksinim duyulandan daha fazla sayıdaki kişisel verinin kullanımı önlenmektedir. Eğer bir

[221] Giakoumopoulos, s.123.
[222] Giakoumopoulos, s.125.

veri birden fazla amaç için kullanılmaktaysa, yine bunların gerektiği kadarıyla sınırlandırılması gerekmektedir.[223] Örneğin, iş başvuru formları, müşteri bilgi kartları veya internet ortamındaki kayıt sayfaları hazırlanırken bu ilkeye dikkat edilmeli ve amaca ulaşmak için gerekli olandan fazla bilgi talep edilmemelidir. Aynı şekilde, güvenlik gerekçesiyle gizli kameraların konumlandırılmasında, amacı aşacak şekilde veri toplamasına imkan vermeyecek şekilde çekim yapmasına dikkat edilmelidir.[224]

Bir diğer prensip olan doğruluk ilkesine göre, kişisel veriler doğru ve gerektiği takdirde güncel tutulmalıdır. Bu ilke uyarınca kontrolör, tüm işleme süreçlerinde bu prensibin yerine getirmelidir. Bununla beraber verinin işlenme amacı dikkate alınarak, doğru olmayan verilerin gecikmeden silinmesi ya da düzeltilmesi gerekmektedir. Ayrıca veriler düzenli olarak kontrol edilmeli ve bu ilkeye uygunluğunun devam edilmesi için güncel tutulmalıdır. Yasa'nın veri sahibinin itiraz hakkını düzenleyen 15. maddesinde kendisine ait kişisel verisi hakkında düzeltme talebinde bulunabilme hakkı, GDPR'ın 16. maddesinde yer alan düzeltme hakkının bu prensibin bir yansıması olduğu görülmektedir.

GDPR'ın öngördüğü sınırlı süre saklanması prensibine göre, veriler, gerektiğinden daha uzun süre veri sahibinin belirlenmesine izin verecek şekilde tutulmamalıdır. Verilerin toplanma amaçları sona erdikten sonra en kısa sürede silinmeleri ya da anonim hale getirilmeleri gerekmektedir. Bu amaçla, verilerin gereğinden uzun tutulmadığından emin olunması için kontrolörün silme veya periyodik inceleme için zaman sınırlamasını belirlemesi gerekmektedir.[225] Bu prensibe göre verinin saklanması süresi belirlenirken mevzuata bakılır ve mevzuatın öngörmüş olduğu bir süre var ise o süre boyunca veri tutulabilir. Böyle bir sürenin bulunmaması halinde ise amacın gerçekleşmesi için gereken süre boyunca veriler saklanmalıdır. Kişisel veriler, gelecekte kullanma ihtimaline dayanarak saklanamazlar.[226]

---

[223] Küzeci, s.220.
[224] Küzeci, s.220-221.
[225] Giakoumopoulos, s.129.
[226] Korkmaz, s.24.

Yasa'da yer alan maddeye bakıldığında ise, gereğinden uzun süre tutulmaması ile ilgili olarak bu sürenin belirlenmesini Başkan'ın takdirine bıraktığı görülmektedir. Yasa maddesinin uygulanabilirliği veya pratikliği açısından bunun doğru bir yöntem olmadığı açıktır. Bununla beraber, böyle bir sürenin Başkan'ın takdirine bırakılacak bir husus olmadığı, her işin kendine özgü durumların gerektirdiği süre ya da mevzuatın belirleyeceği sürelere göre saklanma süresinin belirlenmesi gerekmektedir.

Aynı maddenin devamında ise, kişisel verinin tarihsel, bilimsel veya istatistiki amaçlarla saklanmasında Başkan'ın, bilgiye konu kişi ya da üçüncü kişinin haklarına zarar gelmediğine kanaat getirmesi halinde vereceği gerekçeli bir kararla, bu tür verilerin saklanmasına devam edilebileceği öngörülmüştür. Verilerin bu sebeplere dayanarak daha uzun süre saklanma ihtiyacının doğması karşılaşılabilecek durumlardır ancak bu konuda yine Başkan'ın inisiyatifine bırakılarak bir karar üretilmesi söz konusu olmuştur. Bilgiye konu kişinin veya üçüncü kişinin haklarına zarar gelmeyeceğine yönelik kanaati nelere dikkat ederek getireceği belirli değildir. Ayrıca iznin gerekçeli karar ile verilmesinden ziyade, veriler saklanırken uyulması gereken yükümlülüklerin belirleneceği, veriye daha fazla ihtiyaç duyulmaması halinde verinin silinme yöntemleri, verilerin bu amaçlar için kullanılmak üzere muhafaza edilmesi durumunda alınması gereken güvenlik tedbirlerinin yer alması ve böylece verilerin saklanma amacı gerçekleştirilirken aynı zamanda güvenliğinin sağlanacağı bir zemin oluşturulmalıdır. Bununla beraber Yasa metninde, verilerin muhafaza edileceği sürenin sınırlanmasına ilişkin bir ifadenin yer almadığı, sonsuza dek o verinin saklanabileceği gibi bir anlam çıktığı dikkat çekmektedir. Oysa verilerin işlenmesinde uyulması gereken prensiplerin varlık amaçları arasında verilerin gerektirdiği kadarının gerektirdiği süre için işlenmesi ve saklanmasının sağlanması bulunmaktadır.

GDPR'ın, verilerin saklanma süresine getirdiği istisnası da aynı yöndedir; verilerin belirtilen sebeplerle daha uzun süre muhafazasına devam edilmesi, veri sahibinin hak ve özgürlüklerinin güvence altına alınması şartıyla olabilmektedir.

GDPR'ın öngördüğü prensiplerden bir diğeri, bütünlük ve gizlilik prensibidir. Bu prensibe uyum için alınabilecek tedbirlere örnek olarak verilerin her koşulda ayrıca değerlendirilmek ve teknik ve organizasyonel imkanlar el verdiği ölçüde, verileri psödonomleştirme veya encrypt etme, verinin güvenliği için koyulan tedbirlerin etkisini ölçmek için düzenli test yapılması gibi önlemler sayılabilir.[227] Yasa'da ise bu prensibin tam karşılığı olmasa da, işlemenin gizliliği ve güvenliğine ilişkin maddede yer alan düzenlemelerle bu prensipteki koruma sağlanmaya çalışılmıştır ancak hesap verilebilirliğin temini ve gerektiğinde yaptırım uygulanması için ilgili maddelerde yeni düzenlemenin yapılmasına ihtiyaç duyulmaktadır. Ayrıca, Yasa'nın 12. maddesinde işlenmiş olan verinin gizliliği ve güvenliği ile ilgili hükmün usulü içerdiği, bu denli önemli bir kuralın Yasa ilkelerinden olması gerektiği, teknolojinin hızlı gelişimi ve verilerin yasal olmayan yollardan elde edilerek kötü niyetli kullanımlara mal olması nedeniyle verilerin güvenliğinin temin edilmesi yoluyla verinin bütünlüğünün ve gizliliğinin ilkeler kapsamına alınması gerektiğini değerlendirmekteyiz.

GDPR'da yer alan diğer bir prensip kontrolörün veya işlemcinin sorumluluğunu gerektiren hesap verilebilirlik prensibidir. Kontrolörün ve işlemcinin veri işleme süreçlerinin veri koruma hukukuna uyumluluğunu gözetmeleri, prensiplerin ve yükümlülüklerin yerine getirilmesi için gerekli tüm teknik ve organizasyonel tedbirleri almaları ve işleme faaliyetleri ile ilgili kayıt tutması gerekmektedir.[228]

Yasa'da ise bu prensibin tam karşılığı olmasa da, kontrolörü Yasa'da düzenlenen prensiplere aykırı şekilde derlenen veya işlenmeye devam edilmiş kişisel verileri imha etmekle yükümlü tutmuştur. Kurul Başkanı'nın bu maddeye aykırı hareket

[227] Giakoumopoulos, s.131.
[228] Giakoumopoulos, s.134-135.

edildiğini tespit etmesi durumunda derleme veya işlemenin durdurulması ve derlenmiş veya işlenmiş bulunan kişisel verilerin imha edilmesi talimatını verme yetkisi bulunmaktadır.

Ancak bu kuralın devamında, bu tür verilerin tarihsel veya bilimsel amaçlı saklanmasının Milli Arşiv Kurul Başkanı tarafından gerekli görülmesi halinde Başkan'ın bu verilerin Milli Arşivde muhafazasına izin verebileceği düzenlenmiştir. Böyle bir istisnanın Yasa'da yer alması sakıncalıdır. Öncelikle bir kişisel verinin belirtilen ilkelere aykırı olmasına rağmen bu verinin her ne sebeple olursa olsun muhafazasına izin verilmesi mümkün olmamalıdır. Bununla beraber Milli Arşivde muhafazasına ilişkin onayın Kişisel Verileri Koruma Kurulu Başkanı tarafından verileceği belirtilmişse de, çalışmamızın önceki bölümlerinde de belirtilmiş olduğu üzere Milli Arşiv Kurul Başkanı tarafından gerekli görülmesi durumu kabul edilebilir bir durum olmamalıdır. Zira, ilkelere aykırı işlenen veriler kişilerin temel hak ve özgürlüklerine aykırılık teşkil edebileceğinden, bu alanda denetleyici bir makam varken bu verilerin başka bir Kurul Başkanı tarafından değerlendirilmesi ve talep iletilmesi makul görünmemektedir.

4.4. Kişisel ve Hassas Verilerin İşlenme Şartları

4.4.1 Kişisel Verilerin İşlenme Şartları

Kişisel verilerin işlenmesinde hukuka uygunluk sebepleri düzenlenmiştir. Bu sebeplerden birinin varlığı halinde kişisel verilerin yukarıda belirtilen hukuka uygunluk ilkesi gerçekleştiği söylenebilir. GDPR, 95/46/EC Sayılı Direktif'le benzer şekilde kişisel verilerin işlenmesinde hangi hallerin hukuka uygun kabul edilebileceğini saymıştır. Yasa ise 95/46/EC Sayılı Direktif'e uygun şekilde yasal işleme şartlarını düzenlediğinden, iki mevzuat arasında paralellik olduğu görülmektedir. Bu nedenle her iki mevzuatın 6. maddelerinde belirlenen şartlarına birlikte değinilecektir.

- bilgiye konu kişinin rızası; Yasa, bilgiye konu kişinin şüpheye sebebiyet vermeyecek şekilde onay vermesi demektedir. Ancak ileride de değinileceği üzerinde rızanın şartları Yasa'da belirtilmemiş ve tanımlarda da rızaya yer verilmemiştir. GDPR ise rızanın tanımına yer vermiş, aynı zamanda da detaylı şekilde rızanın şartlarını belirlemiştir.

- kontrolörün yasal bir yükümlülüğünün yerine getirilmesi için verinin işlenmesinin gerekli olması.

- veri sahibinin taraf olduğu bir sözleşmenin ifası için gerekli olması veya veri sahibinin talebi üzerine sözleşmeye taraf olmadan önce tedbir alınması amacıyla işlenmesi

- veri sahibinin hayati çıkarları için işlemenin gerekli olması; GDPR ayrıca diğer bir gerçek kişinin de hayati çıkarlarının korunması için gerekli olması haline yer vermiştir.

- kamu çıkarı adına bir görevin ifası veya kontrolöre veya üçüncü bir tarafa verilmiş olan kamu yetkisinin ifası için verinin işlenmesinin gerekli olması

- veri sahibinin hakları, çıkarları ve temel özgürlüklerinin üstün geldiği durumlar hariç, kontrolör veya verinin iletildiği üçüncü tarafça izlenen yasal çıkarlar amacıyla verinin işlenmesinin gerekli olması; GDPR'ın 6. maddesinin 1. bendinin (f) fıkrası özellikle veri sahibinin çocuk olduğu durumlarda, hak, çıkar ve temel özgürlüklerin korunmasını ayrıca belirtmiştir. Ayrıca bu bendin kamu kuruluşları tarafından görevlerinin ifası sırasında gerçekleştirilen işlemelere uygulanmayacağı düzenlenmiştir.

4.4.2. Hassas Verilerin İşlenme Şartları

Yukarıda Temel Kavramlar bölümünde detaylı bahsedilen hassas verilerin işlenmesi gerek Yasa'da gerekse GDPR'da genel kural olarak yasaktır. Ancak bazı istisnai durumların varlığı halinde hassas verilerin işlenmesi mümkün olabilmektedir. 95/46/EC Sayılı Direktif ile GDPR'ın istisna halleri benzer olmakla birlikte GDPR ek istisnalar da eklemiştir. Bununla beraber Yasa'nın 7. maddesi bu istisnalara yer verirken, 95/46/EC Sayılı Direktif'e göre daha az istisnaya yer vermiş olduğu görülmektedir. Hassas verilerin işlenme yasağına ilişkin istisnalar şöyledir;

a) veri sahibin açık rızasının bulunması;

GDPR, açık onay konusunda Yasa ile aynı istisnaya sahip olmakla birlikte, ek olarak 95/46/EC Sayılı Direktif'te de olduğu gibi, üye devletin bu yasağın veri sahibi tarafından kaldırılamayacağına ilişkin karar verme yetkisi olduğunu belirtmektedir.

b) veri sahibinin fiziksel ya da yasal olarak onay veremediği durumlarda, kendisinin veya diğer bir kişinin hayati çıkarlarının korunması için işlemenin gerekli olması;

Yasa'da bu istisna ile ilgili "onay vermediği durumlar" ifadesi geçmektedir ancak bu hususun bir yazım hatasından kaynaklanmış olma ihtimalinin olduğu düşünülmekle birlikte her halükarda veri sahibinin onay verme konusunda fiziksel veya hukuksal elverişsizliğin aranması gerektiğinden, bir yorum karmaşasının önlenmesi açısından Yasa'nın yeniden düzenlenme çalışmalarında bu düzeltmenin yapılması faydalı olacaktır.

c) Üye Devlet hukukuna göre veri sahibinin temel hak ve menfaatleri için uygun tedbirler barındıran bir toplu sözleşme ile izin verildiği ölçüde işleme, kontrolörün veya veri sahibinin iş ve sosyal sigorta ve güvenlik hukuku alanlarındaki yükümlülüklerinin yerine getirilmesi ve belli haklarının kullanılması için işlemenin gerekli olması;

Bu istisnanın benzerinin 95/46/EC Sayılı Direktif'te de yer almasına rağmen Yasa bu istisnayı yasal işleme şartları açısından saymamıştır. Ancak Yasa "yasal bir yükümlülükten kaynaklanması halinde hassas veriler derlenebilir veya işlenebilir" demektedir. Burada belirtilen yasal yükümlülük hususu 95/46/EC Sayılı Direktif veya GDPR'da bahsedilen şekildeki yasal zorunlulukların geneli olarak yazılmış olabilir. Fakat daha önce de belirtildiği üzere hassas veriler, derlenmesi veya işlenmesi daha sıkı şartlara bağlanan veri kategorilerindendir. Bu nedenle Yasa'da yer alan yasal yükümlülük konusunun spesifik hale getirilmesi gerekmektedir.

d) işlemenin, meşru faaliyetleri kapsamında uygun tedbirler alınarak bir vakıf, dernek veya herhangi bir başka kar amacı gütmeyen kuruluş tarafından politik, felsefi, dini veya ticaret birliği amaçları ile gerçekleştirilmesi halinde hassas veriler işlenebilir. Ancak işlemenin sadece kuruluşun üyeleriyle veya eski üyeleriyle ya da düzenli olarak temasta oldukları kişilere ilişkin olması ve veri sahiplerinin rızası olmadan dışarıya açıklanmıyor olması şartı koşulmaktadır;

Bu istisna da 95/46/EC Sayılı Direktif'te yer almasına rağmen Yasa'da yer verilmeyen istisnalardandır.

e) işleme, veri sahibi tarafından açıkça aleni hale getirilen hassas kişisel veriye ilişkinse;

Bu istisna da 95/46/EC Sayılı Direktif'te olup Yasa'da yer almayan bir istisnadır. Bu istisna Yasa'nın uygulanmamasından dolayı denetlenmeyen ancak halihazırda uygulamada yer alan bir durumdur. Örneğin sağlık verilerinin ya da yaşanılan istismar vakalarının konuyla ilgili kişi tarafından toplumsal farkındalık maksadıyla sosyal medyadan yayınlanarak yardım kampanyaları başlatılması ya da diğer mağdurları yüreklendirmek için söyleşiler organize edilmesi durumları yaygınlaşmıştır. Böyle bir durumda, dernekler ya da kamu kurumları ya da gazetecilik maksadıyla bu gibi verilerin gerek istatistik gerekse yasal boşluğun giderilmesi amacıyla düzenleme taslaklarının yapılması için derlenmesi söz konusu

olabilmektedir. Bu hallerin normal şartlarda yasak olması gerekirken veri sahibinin kendisi tarafından alenileştirilmiş olması yasağı kaldıran unsurlardan olmalıdır.

f) işlemenin hakların tesisi, kullanılması veya korunması için gerekli olması ya da mahkemelerin yargı yetkileri kapsamında hareket etmesi halinde;

Bu istisna benzer şekilde 95/46/EC Sayılı Direktif'te de yer almaktadır ancak Yasa bu istisnaya yer vermemiştir. Ancak yukarıda (c) bendinde belirtildiği gibi yasal yükümlülük ifadesi ile bu istisnaların kapsama alınması hedeflenmişse de bu veri kategorisi açısından spesifik hale getirilmelidir.

g) kamu yararı için hassas kişisel verilerin işlenmesine yönelik istisna hem Yasa'da hem GDPR'da yer almaktadır. Ancak her ikisinin de şartlarını düzenlemesi farklıdır;

GDPR'a göre işleme hedeflenen amaç ile orantılı olması, kişisel verilerin korunması hakkının özüne bağlı olması ve veri sahibinin temel hak ve menfaatlerine uygun ve spesifik önlemler alınması şartıyla, Üye Devlet hukuku temelinde önemli bir kamu yararı sebepleri için işleme gerekli ise yapılabilmektedir.

95/46/EC Sayılı Direktif'in 8. maddesinin 4. bendinde üye devletin uygun koruma tedbirlerinin sağlanması koşuluyla ve önemli bir kamu yararının bulunması durumunda, ulusal mevzuat ya da denetleme makamının kararıyla sayılan istisnalara ek başka istisnalar düzenleme yetkisinin bulunduğu belirtilmiştir. Yasa'da ise 95/46/EC Sayılı Direktif'ten de farklı olarak, Bakanlar Kurulu'nun, Kurulun oybirliği ile alacağı bir karar doğrultusunda yapacağı tavsiye üzerine, kamu çıkarını ilgilendiren konularda hassas verilerin işlenmesine yönelik düzenlemeleri içeren kararlar alabileceği belirtilmiştir. Bu noktada kamu çıkarını ilgilendiren durumların çok geniş olabileceğinin göz önünde bulundurulması gerekmektedir. Eğer kamu yararının bu verilerin işlenmesini gerektirdiği değerlendirilecekse de, kararda yer alan düzenlemelerin hazırlanıp karara bağlama

noktasına gelinceye değin, Kurulun görüşlerini alması gerekmektedir. Örneğin kişisel verilerin korunmasında yer alan tüm prensiplerin karşılanmakta olduğu, bireylerin temel hak ve menfaatlerine zarar gelmeyeceği, alınması gereken güvenlik tedbirleri gibi hususların da düzenlemede yer alması gerekmektedir.

h) sağlık verilerinin meslek olarak sağlık hizmeti veren ve sır saklama yükümlülüğü altında olan kişilerce işlenebileceği hem Yasa hem de GDPR tarafından istisna olarak sayılmıştır. Ancak kapsam açısından bakıldığında GDPR daha spesifik gerekçeler belirlemiştir; Birlik veya Üye Devlet hukukuna dayanarak veya bir sağlık uzmanı ile yapılan sözleşme uyarınca ve 3. paragrafta belirtilen şartlara[229] ve güvenlik önlemlerine tabi olunması kaydıyla, işleme önleyici ya da mesleki hekimlik, çalışanların çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık veya sosyal güvenlik sunulması veya tedavi ya da sağlık veya sosyal güvenlik sistemlerinin ve hizmetlerinin yönetilmesi için gerekliyse hassas veriler işlenebilir denilmiştir.

Yasa'da ise sağlık ile ilgili hassas verilerin yasak kapsamı dışında olduğu belirtilerek, bu tür verilerin meslek olarak sağlık hizmeti veren ve gizlilik yükümlülüğü bulunan veya ilgili davranış ilkelerine tabi olan kişi ya da kurumlarca derlenebileceği veya işlenebileceği düzenlenmiştir.

Görüldüğü üzere GDPR sağlığa ilişkin verilerin işlenmesini çok sıkı şartlara bağlamış ve işleme maksadını daha spesifik hale getirmiştir. Yasa'da gizlilik yükümlülüğüne sahip herkesin işlemesine izin verildiği gibi bir anlam çıkmaktadır ki uygulamada önemli ölçüde mağduriyetlere ya da şikayetlere yol açabilir. Bu nedenle bu kısmın yeniden gözden geçirilmesi faydalı olacaktır.

---

[229] GDPR madde 9 (3); hassas verilerin bu maddenin 2(h) bendinde belirtilen amaçlar için Birlik veya Üye Devlet hukuku veya ulusal yetkili kuruluşlar veya bunlar tarafından belirlenen kurallar uyarınca sır saklama yükümlülüğü altında bulunan diğer bir kişi tarafından belirlenen kurallar uyarınca sır saklama yükümlülüğüne tabi olarak mesleki yükümlülük ile veya yükümlülük altında işlenebileceği belirtilmiştir

i) GDPR'da yer alan diğer bir istisnaya göre işleme, başta mesleki gizlilik yükümlülüğü olmak üzere, veri sahibinin hak ve özgürlüklerinin güvenliği için uygun ve spesifik önlemlerin alınmasını sağlayan Birlik veya Üye Devlet hukukuna dayanan, ciddi sınır ötesi sağlık tehditlerine karşı korunma, sağlık hizmeti ve tıbbi ürün veya tıbbi cihazların yüksek kalite standardı ve güvenliğini sağlamak gibi halk sağlığı alanında kamu yararı nedenleri için gerekliyse hassas veriler işlenebilir.

j) GDPR'da yer alan son istisnaya göre işleme, hedeflenen amaç ile uyumlu, veri koruma hakkının esasına itibar eden ve veri sahibinin bireysel hak ve menfaatlerinin uygun ve spesifik güvenliğin sağlanması şartıyla Birlik veya Üye Devlet hukukuna dayanan ve GDPR'ın 89(1)'nci maddesi uyarınca, kamu yararı için arşivleme, bilimsel veya tarihsel araştırma veya istatistiksel maksatlar bakımından gerekli ise hassas veriler işlenebilir.

k) Yasa'da ise hassas veriler ile ilgili son olarak, derlenip işlenen hassas verilerin veri sahibinin onayı ile üçüncü taraflara iletilebileceğini düzenlemiştir. Yasa'da aktarılma şartları olarak ayrı bir düzenleme olmamakla birlikte hassas verilerin aktarılması için onay şartının aranmasına yönelik kural koyulması yerinde bir düzenlemedir.

GDPR'da hassas verilerin işlenmesi ile ilgili olarak ayrıca, genetik, biyometrik veya sağlığa ilişkin verilerin işlenmesi ile ilgili olarak Üye Devletlerin sınırlamalar dahil diğer koşulları ileri sürebileceklerini düzenlemiştir.

4.4.3. Rızanın Şartları

Günümüzde rızanın alınma yöntemlerinin değişmiş olduğu, özellikle teknoloji vasıtasıyla akıllı telefonlardan, internetten ve benzeri kanallardan çeşitli onaylar alınabilmektedir. Diğer yandan çocukların teknoloji dünyasında doğup büyümeleri ve tüm hayatlarının içerisinde teknolojinin olmasından dolayı onların kişisel verileri ayrıca tehdit altındadır. Bu nedenlerle kontrolörlerin verinin işlenmesinde hukuka

uygunluk sebeplerinden olan veri sahibinin rızasını alırken hangi şartlara uymaları gerektiği, çocuğun rızası için nelere dikkat edilmesi gerektiği gibi hususların ayrıca düzenlenmesi önemlidir. Bu gerçekler karşısında GDPR'ın 7. maddesinde "rızanın şartları" ve 8. maddesinde "bilgi toplumu hizmetlerine ilişkin olarak çocukların rızasına ilişkin koşullar"ın belirlenmesinin çok önemli düzenlemeler olduğu ve Yasa'nın da ülke şartlarını göz önünde bulundurarak rızanın alınmasına ilişkin düzenleme eklemesinin faydalı olacağı değerlendirilmektedir. Bu noktada konu faydalı olması açısından GDPR'ın bu düzenlemelerine yer verilecektir.

Verinin işlenmesinin rızaya dayalı olduğu durumlarda kontrolör veri sahibinin rızası olduğunu ortaya koyabilmelidir, yani GDPR 7. maddenin 1. bendi altında ispat yükümlülüğünü kontrolöre yüklemiştir. 7. maddenin 2. bendi uyarınca, ilgili kişinin rızası başka hususların da yer verildiği yazılı bir beyanda verilmekteyse, rıza verilmesi talebi, diğer konulardan ayrıştırılabilir ve anlaşılır olmalı, açık ve basit bir dil ile yazılmalıdır, aksi halde aykırılık teşkil eden kısımlar geçersiz olacaktır. Bununla beraber, 7. maddenin 3. bendine göre veri sahibinin rızasını geri alınabilmesine, rızanın verilmesi kadar kolay olacak şekilde imkan tanınmalıdır ve veri sahibi rıza vermeden önce bu hakkın varlığı hakkında bilgilendirilmelidir. Bir diğer önemli şart ise rızanın serbest iradeye dayanılarak verilip verilmediği hususudur. 7. maddenin 4. bendine göre de bir sözleşmenin ifası hususunda, bir hizmetin sunulması için rızanın talep edilmesi dahil olmak üzere sözleşmenin ifası için gerekli olmayan bir işlemenin gerçekleştirilmesi şartına bağlanıp bağlanmadığı rızanın verilmesindeki özgür iradenin değerlendirilmesinde önem arz etmektedir.

Rızanın serbest verilmesi konusu kontrolör ile veri sahibi arasında önemli ekonomik dengesizlik veya itaat gibi durumlarda şüpheli olmaktadır. Bu dengesizliğin en tipik örneği iş ilişkisi kapsamında işçinin verilerinin işlenmesidir. Madde 29 Çalışma Grubuna göre, işçi/işveren ilişkisinin sonucu olarak çalışanlar neredeyse hiçbir zaman rızalarını serbestçe verme, reddetme veya iptal etme

konumunda değildirler.[230] Teoride bu hakları olmasına rağmen işçinin bir iş olanağını kaybetmesi gibi bir sonuçla karşı karşıya kalabileceğinden, üzerinde baskı olabileceği dikkate alınmalı ve işçiler için bazı ek güvenceler sağlanmalıdır. İşçi ile işverenin arasında bulunan ilişkinin niteliği gereği, işverenin işçinin rızasına dayanması yanıltıcı olabilmektedir. Bu sebeple, işlemenin hukuka uygunluğu konusunda rızaya dayanılması bu noktada sınırlandırılabilir.[231] Bu noktada işçinin özgür seçimine dayanılması ve çıkarlarına zarar gelmeksizin rızasını geri alabilmesi önemlidir.[232]

GDPR'ın çocuğun rızası ile ilgili düzenlemesine gelince, kişisel verinin işlenmesinde veri sahibinin rızası şartının uygulandığı hallerde, bir çocuğa bilgi toplumu hizmeti sunulmasıyla ilgili olarak çocuğun kişisel verisinin işlenmesi, çocuk en az 16 yaşında ise hukuka uygun olmaktadır. Çocuğun 16 yaşından küçük olması halinde işleme, yalnızca çocuğun ebeveyni veya vasisi tarafından onay veya yetki vermesi halinde hukuka uygun sayılacaktır. GDPR, Üye Devletlere 13 yaşından daha az olmamak kaydıyla, yasa ile belirtilen yaşı daha düşük olarak belirleme yetkisi vermektedir. [233]

4.5. Kişisel Verilerin Yurtdışına Aktarılması

Yasa, işlenmiş veya işlenmesi amaçlanmış verinin yurtdışına transferinin Kurul'un ücret karşılığında vereceği "transfer ruhsatı" ile mümkün olabileceğini ve bu ruhsatın ilgili ülkenin yeterli koruma seviyesine sahip olması durumunda verileceğini düzenlemiştir.

Transfer ruhsatı verilirken, Kurul tarafından verinin niteliği, işleme amacı, işlemenin süresi, hukukun genel ve özel ilkeleri, davranış ilkeleri ve verinin

---

[230] Giakoumopoulos, s.144; Küzeci, s. 240.
[231] Örneğin İngiltere'de denetleme makamı, işverenlerin işçilerin kişisel verilerini işlerken hukuka uygunluk şartı olarak nadiren rıza beyanına dayanabileceklerine işaret etmiştir. Bkz. Küzeci, s. 240.
[232] Küzeci, s. 240.
[233] Güney Kıbrıs bu yaşı LAW 125(I) of 2018 Kanununun 8. maddesi altında 14 olarak belirlemiştir.

korunması için güvenlik tedbirleri ile nihai hedefin göz önünde bulundurulması kuralı yer almaktadır. Transfer ruhsatı hususu 95/46/EC Sayılı Direktif'te yer almayıp Yasa koyucunun eklemiş olduğu bir düzenleme olarak karşımıza çıkmaktadır.

Yeterli koruma düzeyine sahip olmayan bir ülkeye aktarım söz konusu olacağında ise bazı şartların bir veya daha fazlasının yerine getirilmesi halinde izin verileceği belirtilmiştir. Bu şartlar;

- bilgiye konu kişinin herhangi bir kuşkuya yer bırakmayacak şekilde ve hukuka veya kabul edilmiş ahlak değerlerine aykırı olmayacak şekilde onayının alınması

- Aşağıdaki hallerde transferin gerekli olduğu belirtilmiştir.
a) bilgiye konu kişinin hayati çıkarlarının korunması veya
b) bilgiye konu kişi ile kontrolör veya kontrolörle üçüncü taraf arasında, bilgiye konu kişinin çıkarı için yapılmış olan bir sözleşmenin tamamlanması veya kurallarının yerine getirilmesi için veya
c) bilgiye konu kişinin talebi üzerine alınan, bilgiye konu kişi ile kontrolör arasında yapılacak sözleşme öncesi önlemlerin uygulanması için.

- transferin önemli kamu çıkarı, özellikle diğer ülkenin kamu makamlarıyla işbirliğine dair ilişkin sözleşme kurallarının yerine getirilmesi nedeniyle gerekli olması veya bu nedenlerle transfere hukuken ihtiyaç duyulması

- transferin bir mahkemeye yöneltilecek hukuki iddiaların oluşturulması, öne sürülmesi ve savunulması için gerekli olması

- transferin ilgili yasa uyarınca kamuya bilgi veren ve kamuya veya meşru çıkarı olan herkese açık olan bir kamu kayıt merkezinden, kayıt merkezine erişimin yasal olarak mümkün olması halinde yapılması durumlarının birinin varlığı halinde transfere izin verileceği belirtilmiştir.

Ayrıca Yasa, Kurula yeterli düzeyde koruma sağlamayan bir ülkeye, kontrolörün özel ve temel hakların korunmasına ilişkin yeterli teminat vermesi ve bu hakların ve teminatın uygun sözleşme kurallarından kaynaklanması halinde, veri transferine izin verme yetkisi vermektedir.

GDPR, verilerin yurtdışına transferin uygunluk hallerini 2 ayrı başlıkta düzenlemiştir. Bunlardan biri Avrupa Birliği Komisyonu'nun verdiği yeterlilik kararı[234] ile transferin gerçekleşmesi, diğeri ise 46. ve 49. maddeler altında düzenlenen komisyonun yeterlilik kararı olmamasına rağmen transferin yapılabileceğini belirleyen şartların varlığı halleridir.

Komisyon'un verdiği yeterlilik kararı hususu KKTC özelinde değerlendirildiğinde uygulanabilirliği tartışmalı bir konu olacaktır.[235] Bu nedenle yeterlilik kararı konusunun detayından bahsedilmeyecektir. Ancak kısaca belirtilebilir ki, AB'ye Üye Devletler GDPR'ı uygulamak zorundadır, bu nedenle Üye Devletlerarasında veri akışı serbestçe yapılabilmektedir. Yeterlilik kararı ile güvenli ülke seçilmesi, AB'ye Üye Devletler haricinde kalan ülkelere ayrıca izin şartı aranmaksızın verilerin transferi mümkün olacaktır. Bugüne kadar Komisyonun yeterlilik kararı verdiği ülkeler; Amerika Birleşik Devletleri, Andora, Arjantin, Faroe Adaları, Guernsey, İsviçre, İsrail, Japonya, Jersey Adası, Kanada, Man Adası, Uruguay, Yeni Zelanda'dır. Güney Kore ile yeterlilik kararı görüşmeleri devam etmektedir.[236] Türkiye için verilmiş bir karar bulunmamaktadır.

---

[234] GDPR madde 45'e göre Komisyon ilgili ülke, ülke içindeki bir bölge ya da belirli sektörlerin veya uluslararası kuruluşun yeterli koruma sağladığına yönelik karar verir.

[235] Daha önce belirtilen KKTC'nin siyasi konumundan dolayı Türkiye dışında bir ülke tarafından resmi olarak tanınmadığından, Komisyonun resmi şekilde güvenli ülke olarak belirleyip yeterlilik kararı vermesi mevcut durumda pek mümkün görünmemektedir.

[236] European Commision (2019) Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> son erişim 08.04.2019.

GDPR'ın 46. maddesinin 1. bendine göre Komisyon'un yeterlilik kararının olmadığı durumlarda yurtdışına veya uluslararası bir kuruluşa transfer, kontrolörün veya işlemcinin uygun tedbirleri almış olması ve veri sahiplerinin haklarının icra edilebilir nitelikte olması ve veri sahipleri için etkin yasal çarelerin bulunması koşuluyla yapılabilir.

Bu kapsamda 46. maddenin 2. bendi uyarınca kamu makamları veya diğer kamu kuruluşları arasında hukuken bağlayıcı ve icra edilebilir anlaşmalar, bağlayıcı kurumsal kurallar, standart veri koruması hükümleri, onaylanmış davranış kodları ve onaylanmış sertifikasyon mekanizması belirtilen uygun tedbirler olarak kabul edilmektedir. Bunların varlığı halinde bir denetim makamının özel iznine tabi olmadan transfer mümkündür.

GDPR'ın 47. maddesine göre bağlayıcı kurumsal kurallar kısaca; uluslararası grup şirketlerin farklı ülkelerde bulunan birimleri arasında yapılacak transferler için kabul edilmiş veri politikalarıdır. Bağlayıcı kurumsal kurallar ayrıca GDPR'ın 4. maddesinde de tanımlanmıştır. Bu tanıma göre; "bir Üye Devlet sınırları için işletmesi bulunan bir kontrolörün veya işlemcinin ortak bir ekonomik faaliyet içinde bir teşebbüsler birliği veya girişimler birliği kapsamında bir veya daha fazla üçüncü ülkede bulunan bir kontrolör veya işlemciye kişisel veri transferleri veya transfer setleri için uydukları kişisel verilerin korunması politikaları anlamına gelmektedir."

Standart veri koruması hükümleri ise Komisyon tarafından hazırlanan veya bir denetim makamı tarafından hazırlanıp Komisyon tarafından kabul edilen onaylanmış olan örnek sözleşme metinleridir. Üye Devletlerde veya üçüncü ülkelerde bulunan kontrolörler veya işlemciler, aralarında bu sözleşmeleri imzalayarak, yurtdışına gerçekleştirilen transferlerde GDPR'da aranan korumanın sağlanacağını sözleşmesel olarak taahhüt edebilirler.[237]

[237] Develioğlu, s.76.

Davranış kodlarında ise kısaca, Üye Devletler, denetim makamları, Kurul ve Komisyon, farklı işleme sektörlerinin spesifik özelliklerini ve mikro ve küçük-orta ölçekli işletmelerin ihtiyaçlarını da dikkate alarak GDPR'ın doğru uygulanmasına katkıda bulunma amacı güden davranış kuralları yazılmasını teşvik eder. GDPR madde 41'in 1. bendine göre davranış kurallarına uyulduğunun denetimi, yetkili denetim makamı tarafından akredite edilmiş, alanında uzman bir kurum tarafından yapılabilir.

Sertifikalar, kontrolörlerin ve işlemcilerin işleme faaliyetlerinin GDPR'a uygunluğunu göstermek maksadıyla, sertifikasyon kuruluşları ile yetkili denetim makamları tarafından verilir. 42. madde uyarınca alınan sertifika GDPR'a uyum yükümlülüğünü azaltmaz ve gönüllü olarak alınmalıdır.

Bağlayıcı kurumsal kurallar veya standart veri koruması hükümleri, kontrolörün sözleşmesel olarak GDPR'ın öngördüğü yükümlülükleri yerine getireceklerini taahhüt etmesine imkan verdiğinden ilgili üçüncü ülkeye yönelik yeterlilik kararı olmasa da kişisel verilerin transferi mümkün olmaktadır.[238] Davranış kodları ve sertifikasyonlara dayanılarak yapılan transferlerde, üçüncü ülkedeki kontrolörler veya işlemcinin uygun önlemleri uygulayacağını ayrıca taahhüt etmesi şartı da aranır.[239]

Yetkili denetim makamının izninin alınmış olması şartıyla 46. maddenin 1. fıkrasında belirtilen uygun önlemler kontrolör veya işlemci ve üçüncü ülke veya uluslararası kuruluştaki kontrolör, işlemci veya alıcı arasındaki sözleşme hükümleri ile sağlanabilir. 46. maddenin 3. bendinde belirtilen diğer bir yöntem ise kamu makamı veya kuruluşları arasındaki idari sözleşmelere uygulanabilir ve etkili veri sahibi haklarını içeren hükümler eklemektir.

---

[238] Develioğlu, s.77.
[239] Develioğlu, s.78.

GDPR'ın 48. maddesine göre bir üçüncü ülkede verilen ve bir kontrolörün ya da işlemcinin kişisel verileri aktarmasına veya ifşa etmesine yönelik herhangi bir mahkeme kararı veya kurul veya idari makam kararı, ancak talepte bulunan üçüncü ülke ile Birlik veya Üye Devlet arasında imzalanmış olan adli yardımlaşma anlaşmasına dayandığı takdirde tanıma veya tenfiz yapılabilir.

GDPR'ın 49. maddesinde belirtildiği üzere Komisyon'un verdiği yeterlilik kararının veya bağlayıcı kurumsal kurallar dahil uygun önlemlerin bulunmadığı hallerde verinin üçüncü ülkeye ya da uluslararası kuruluşlara transferi veya transfer setleri aşağıdaki şartlardan birinin varlığı halinde gerçekleşebilir;

a) veri sahibinin verilerinin transferinde yeterlilik kararı veya uygun önlemlerin bulunmaması nedeniyle transferin muhtemel riskleri konusunda bilgilendirildikten sonra vereceği açık rızası;

b) transferin veri sahibi ile kontrolör arasındaki bir sözleşmenin ifası veya veri sahibinin talebi üzerine veri sahibi ile kontrolör arasındaki bir sözleşme öncesi tedbirlerin uygulanması için gerekli olması;

c) transferin kontrolör ve diğer bir gerçek veya tüzel kişi arasında, veri sahibinin yararına olacak bir sözleşme ifası veya sonuçlandırılması için gerekli olması;

d) transferin önemli bir kamu yararı için gerekli olması;

e) transferin hukuki iddiaların tesisi, uygulanması veya savunması için gerekli olması;

f) transferin veri sahibinin fiziksel veya hukuki olarak rıza veremediği durumlarda veri sahibinin veya diğer bir kişinin hayati çıkarlarının korunması için gerekli olması;

g) transferin Birlik veya Üye Devlet tarafından kamuyu bilgilendirmek için tutulan, genel olarak kamunun ya da meşru ilgisi olan kişilerce incelemeye fırsat veren bir sicilden, Birliğin veya Üye Devletin incelemeye yönelik şartların yerine getirildiğinin ortaya konulabildiği ölçüde yapılıyor olması.

Bununla beraber, tekrarlanmaması kaydıyla ve sadece sınırlı sayıda veri sahibine ilişkin olduğu sürece, kontrolör tarafından ulaşılmak istenen meşru menfaatler için transfer gerçekleştirilebilir. Bunun için veri sahibinin menfaatleri veya hak ve özgürlükleri, kontrolörün menfaatlerinden ağır basmamalıdır. Ayrıca kontrolörün transfere ilişkin tüm şartları değerlendirmiş olması ve bu değerlendirmeye uygun olarak kişisel verilerin korunmasına yönelik bütün uygun tedbirleri alması gerekir. Kontrolör gerçekleştirdiği değerlendirmeyi ve aldığı tedbirleri belgelendirmek zorundadır ve transfer konusunda denetim makamına ve veri sahibine bildirimde bulunmalıdır.

Yasa'nın verilerin yurtdışına transferiyle ilgili düzenlemesine bakıldığında her şeyden önce "Transfer Ruhsatı" konusunun değerlendirilmesi gerekmektedir. Belirtildiği üzere böyle bir ruhsatın verilmesi 95/46/EC Sayılı Direktif'te yer almayıp Yasa'mızın getirmiş olduğu bir düzenlemedir. Bu düzenlemeye göre transferin yapılacağı ülkenin yeterli korumayı sağlaması halinde bir ücret karşılığı transfer ruhsatı verilecektir.

Öncelikle, aşağıdaki bölümde "Kurulun Gelirleri" başlığı altında da değinileceği üzere, böyle bir ruhsat verilmesi öngörülecekse dahi bu ruhsat için ücret talep edilmesi son derece anlamsızdır ve doğru değildir. Kurul'un hizmeti olmayan bir husus için ücret talep etmesi için makul bir açıklama gerekmektedir.

Öte yandan transfer ruhsatı verilmesi ile amaçlananın ne olduğu, takibinin denetiminin nasıl olacağı belirtilmemiştir. Yalnızca ilgili ülkenin yeterli koruma sağlaması, verinin niteliği, işleme amaç ve süresi, hukukun genel ve özel ilkeleri, davranış ilkeleri, güvenlik önlemleri, menşe ülkenin koruma seviyesi, verinin

iletilme şekli ve nihai hedefin göz önünde bulundurulacağı belirtilmiştir. Ancak bu kuralların hiçbiri net olmayıp tamamen genel yoruma açık kurallar olarak karşımıza çıkmaktadır. Bu kurallar ancak yeterli koruma sağlayan ülke belirlenmesi için değerlendirilebilecek kurallar olabilecektir ki yine de daha net ve anlaşılır hale getirilmelidir. Ayrıca transferi yapılacak verinin bir hassas veri olması halinde, bu kuralın öngördüğü transfer şekli ile hassas veri için koyduğu kural çelişecektir. Şöyle ki, hassas verinin işlenme şartı başlığı altındaki maddede derlenip işlenen hassas verilerin, veri sahibinin onayı ile üçüncü taraflara iletilebileceğini düzenlenmiş olmasına rağmen transfer ruhsatında yeterli koruma sağlanıyorsa ve Kurul uygun görüp bu ruhsatı verirse, kişinin hassas verisi de transfer edilecektir. Eğer üçüncü taraftan kastedilen taraf yalnızca ülke içerisindeki kişiler ise de bu rıza şartı yeniden gözden geçirilmesi gereklidir, zira üçüncü tarafın tanımı açık uçlu bırakıldığından, KKTC sınırları dahilinde olabileceği anlamı çıkmayabilecektir.

Yasa, yeterli koruma bulunmayan ülkeye yapılacak veri transferinde öncelikle bilgiye konu kişinin transfere vereceği rızanın bulunması şartını koymuş ardından da yasal işleme şartlarına paralel olan durumların bulunması halinde transferin gerekli olduğunu belirtmiştir. Ancak bu şartlar olsa da gönderimin yapılacağı ülkenin güvenli olmayan ülke olduğu ve Yasa'da güvenli ülke kriterlerinin belirlenmemiş olduğu göz önünde bulundurulmalıdır. Bu kuralda bu durumlardan birinin varlığı halinde transfer gereklidir denilerek bir zorunluluk olduğu izlenimi uyandırılmaktadır. Ayrıca bu şartlara yönelik de herhangi bir ek kural belirlenmediğinden, tek başına bu şartlardan birinin olması durumunda veri transferi izni verilmemelidir.

Çalışmamızın çıkış noktası, GDPR kuralları ışığında Yasa'mızın yeniden şekillendirilmesi hususudur. GDPR'ın tamamının verilerin korunması açısından sıkı şartları öngördüğü değerlendirildiğinde, KKTC'nin durumu, mevzuat eksiklikleri, teknik gelişiminde kat etmesi gereken yollar göz önünde bulundurularak veri transferinin istisnaları konusunda GDPR kurallarının tamamen aynı şekliyle örnek alınmasının uygun olmayacağı değerlendirilmektedir. Bu

noktada Yasa'nın transfer ruhsatı ile ilgili 11. maddenin 1. fıkrasında yer alan kuralı kaldırılmalı, 2. fıkrada yer alan (A) fıkrası, (B) fıkrasında yer alan bentler, (C), (Ç) ve (D) fıkraları ve Yasa'nın revizyonunda gündeme gelebilecek ek istisnalar olması halinde ilgili istisnaların tek bir fıkra altında birleştirilerek, bunlardan birinin varlığı dışında transferin gerçekleşeceği ülkede yeterli korumanın bulunması şartının eklenmesi, yeterli koruma bulunmayan ülke olmaması halinde ise (3). fıkrada belirtilen kuralda yer alan şartların yerine getirilmesi haline Kurul'un transfere onay verebileceği düzenlenmelidir.

Verilerin yeterli koruma sağlamayan bir ülkeye transferi ile ilgili kuralların yer almasına rağmen belirtildiği gibi, Kurul'un yeterli düzeyde koruma sağlayan ülkeleri belirlemesinin hangi kriterlere dayanacağı hususunun Yasa'da düzenlenmemiş olması bir eksiklik olarak göze çarpmaktadır. Transferin düzenlendiği 11. maddenin sonunda Kurul'un görevlerinden de olan yeterli koruma sağlayan ülkelerin belirlenmesinde göz önünde tutulacak kriterler spesifik olarak Yasa ile belirlenmelidir.

Belirtilmelidir ki, verilerin Kurul tarafından verilecek "transfer ruhsatı" olmaksızın yurtdışına çıkamayacağı düzenlemesinin varlığı ve Kurul'un uzun süre kurulmamasından dolayı verileri yurtdışına çıkarılması konusunda uzun zaman sorun yaşanmıştır ve halen yaşanmaktadır. KKTC'de özellikle iş ortakları ya da grup şirketleri Türkiye'de bulunan birçok tüzel kişi, yürürlükte olan bir Yasa olmasına rağmen transfer ruhsatı ön şartına bağlanmış olduğundan verilerini yurtdışına kendi inisiyatiflerine göre çıkarmışlardır. Zira yeterli koruma sağlama şartından dolayı KKTC'deki hiçbir kurum, kuruluş veya kişi Türkiye'yi güvenli olmayan bir ülke olarak değerlendirmediğinden, yeterli koruma sağlamayan ülkeye transfer için öngörülen şartlara da itibar edilememiştir. Bu sebeple bu transferler yapılırken birçok kurum, verileri yurtdışına çıkarırken kendi güvenlik politikalarına, etik kurallarına uyumlu olacak şekilde transferi yapmıştır ancak her kurumun bu etik kurallara uymadığı da bir gerçektir.

Transferin düzenlendiği 11. maddenin (C) fıkrasında transferin önemli kamu çıkarı olması halinde transfere ihtiyaç duyulması ile ilgili koyulmuş olan kuralda, kamu çıkarının ne olduğu KKTC hukukuna göre belirlenmiş olmasına dair ek kural konulması faydalı olabilir. Bu hususta GDPR'ın istisnaları düzenlediği 49. maddede kamu yararının Birlik veya kontrolörün tabi olduğu Üye Devlet hukuku tarafından belirleneceği düzenlenmiştir. Kamu yararı ifadesinin yoruma açık bir ifade olduğu göz önünde bulundurulduğunda, kamu yararı için başka bir ülkeye veri transferinin KKTC hukuku nezdinde belirlenmesi yerinde bir düzenleme olabilir.

Yine 11. maddenin (C) fıkrasında fıkrada "özellikle diğer ülkenin kamu makamlarıyla işbirliğine ilişkin sözleşme kurallarının yerine getirilmesi nedeniyle gerekli olması" kuralının özellikle Türkiye ile olan sıkı ilişkileri ve iki ülke arasında yapılan ve yapılmaya devam eden işbirliği protokollerinin uygulanabilirliği, Türkiye'ye nazaran daha az olsa da Güney Kıbrıs ile yapılan işbirliklerinin uygulanabilirliği açısından avantajlı olduğu görülmektedir. Bu maddeye dayanarak yapılacak olan veri transferlerinde, işbirliği protokollerinin detayı, veri alıcılarının sorumlulukları gibi konularda dikkatli olunmalı, Yasa ile belirlenen ilkelere, özellikle verilerin gizliliği ve bütünlüğü ilkesine (ilke olarak revize edilmesi halinde) aykırı olmamasına özen gösterilmelidir.

4.6. Veri Sahibinin Hakları

GDPR veri sahiplerinin sahip olduğu hakları ayrı ayrı başlıklar halinde düzenlemiştir. Yasa'nın 4. Bölümünde sayılan hakların hepsi GDPR'da yer almakla birlikte bazı haklar yalnızca GDPR'da bulunmaktadır. Çalışmamızın bu bölümünde GDPR ve Yasa'da yer alan veri sahibinin haklarına kısaca değinilecektir.

4.6.1. Bilgilendirilme Hakkı

Yasa'nın 13. maddesinde ve GDPR'da 13 ve 14. maddeler altında kişisel verinin veri sahibinden elde edildiği ve bilginin üçüncü taraftan alınması ile ilgili bilgiye konu kişinin bilgilendirilmesi konusunda ayrım yapılmıştır.

Yasa'ya göre kontrolör, veri sahibinden kişisel verilerin toplanması aşamasında, bilgiye konu kişi halihazırda bilgi sahibi değilse, kendisine uygun ve açık bir şekilde en azından kendisinin ve varsa temsilcisinin kimliği ve işlemenin amacıyla ilgili bilgi vermekle yükümlüdür. Kontrolör bilgiye konu kişiyi ayrıca, verinin alıcıları veya alıcı kategorileri, veriye erişim ve verinin düzeltilmesi hakkının varlığı ve bu verinin gerekli olması halinde, verinin güvenlik içerisinde işlenmesinin sağlanması koşuluyla, bilgiye konu kişinin yasal olarak yardım etmek mecburiyetinde olup olmadığını ve mecbursa bunu reddetmesinin sonuçları hakkında da bilgilendirmekle yükümlüdür.

Bilginin üçüncü kişilerden elde edilmesi durumunda ise veri sahibi, bu bilgiler gereğince bilginin kaydı sırasında veya bilginin üçüncü taraflara iletilmesinin beklendiği aşamada henüz bilgilendirilmemişse kendisine bilgi verileceği düzenlenmiştir.

Yine bilginin üçüncü kişilerden elde edilmesi durumu ile ilgili olarak, işlemenin özellikle istatistiki ve tarihi amaçlarla veya bilimsel araştırma amacıyla yapılması halinde, bilgiye konu kişiyi haberdar etmek imkansız ise veya onu haberdar etmek için orantısız bir çaba gerekliyse veya bilginin iletilmesi başka bir yasayla mümkünse, her koşulda Başkan'ın iznini almak suretiyle bu bilgilendirmenin yapılmayacağı düzenlenmiştir.

Yasa, 95/46/EC Sayılı Direktif'in 13. maddesinin "Muafiyetler ve Sınırlamaları" düzenleyen kısmında yer alan bazı istisnalara bilgilendirme yükümlülüğü altında yer vererek, Devletin savunması, ulusal ihtiyaçları veya ulusal güvenliği veya cezai suçların önlenmesi, tespiti, soruşturulması ve kovuşturulması amacıyla kısmen veya tamamen göz ardı edilebileceğini düzenlemiştir. Ancak belirtilmelidir ki

95/46/EC Sayılı Direktif'te bu hakkın kapsamının yasal önlemlerle sınırlanabileceği düzenlenmişken, Yasa hakkın kısmen veya tamamen uygulanmamasına olanak tanımaktadır.

Yasa yine 95/46/EC sayılı Direktif'in 9. maddesinin "kişisel verilerin işlenmesi ve ifade özgürlüğü"nü düzenleyen kısmında belirtilen istisnaya benzer bir istisnaya yer vererek, bilgiye konu kişinin erişim ve itiraz haklarına zarar gelmemesi, aile yaşamının ihlal edilmemesi koşuluyla ve derlemenin yalnızca gazetecilik amacıyla yapılması halinde bilgiye konu kişiyi bilgilendirme yükümlülüğü bulunmamaktadır.

GDPR'ın bilgilendirme yükümlülüğü ile ilgili düzenlemesi Yasa'dan daha geniş tutulmuştur. 12. maddeye göre kişisel verinin veri sahibinden elde edildiği durumlarda bilgiye konu kişi halihazırda bilgi sahibi değilse, kendisinin ve ilgili hallerde temsilcisinin kimliği ve iletişim bilgileri, ilgili hallerde bilgi güvenliği yetkilisinin iletişim bilgilerinin iletilmesi gerekir. Bu bilgiler özellikle bilgiye konu kişinin haklarını kullanmak üzere kontrolöre ulaşımında önem teşkil eder.

Yine, veri işlenmesinde hedeflenen amaç ve işlemenin hukuki dayanağı, verilerin meşru menfaate dayanarak işlenmesi halinde kontrolör veya üçüncü kişi tarafından hedeflenen meşru menfaatler ve eğer varsa alıcı veya alıcı kategorileri hakkında da bilgi verilmelidir.

Ayrıca, kişisel verinin üçüncü ülkeye veya uluslararası kuruluşa transferi niyetinde olduğu ve Komisyonun yeterlilik kararı olup olmadığı, olmaması durumunda transfer için alınan tedbirlerin neler olduğu ve bunlara ne şekilde erişebileceğine dair bilginin de bilgiye konu kişiye bildirilmesi gerekmektedir.

Kontrolör belirtilen bilgilere ek olarak işlemenin adil ve şeffaf olmasını sağlamak maksadıyla, kişisel verilerin elde edildiği sırada bilgiye konu kişiye, verilerin saklama süresi veya süre belli değilse sürenin belirlenmesinde kullanılacak

kriterleri; bilgiye konu kişinin haklarının varlığı; kişisel verinin bilgiye konu kişinin rızasıyla işlendiği durumlarda rızayı geri alma hakkının bulunduğu; denetim makamına şikayet etme hakkı; verinin elde edilmesinin sözleşmesel bir zorunluluktan kaynaklanıp kaynaklanmadığı ya da sözleşmenin tesisi için gerekli olup olmadığı, bilgiye konu kişinin kişisel verilerini sağlamak zorunda olup olmadığı ve verinin sağlanamamasının muhtemel sonuçları; otomatikleştirilmiş karar vermenin uygulandığı ve buna dair anlamlı bilgi, işlemenin önemi ve sonuçları hakkında bilgiye konu kişiyi bilgilendirmelidir. Kontrolörün kişisel verileri elde ettiği amaç dışında başka bir amaçla işleme niyeti olduğu durumda, işlemeden önce bu fıkrada belirtilen bilgileri bilgiye konu kişiye aktarmalıdır.

Yasa'nın 13. maddesine göre kişisel verinin bilgiye konu kişiden elde edilmediği durumlar için belirlenen bilgilendirme yükümlülüğü altında verilecek bilgiler bilgiye konu kişiden alınan bilgilerle paraleldir. Ancak bilgiye konu kişiye sağlanması gerektiği belirtilen bilgiler arasında alıcı veya alıcı kategorilerine yer verilmemiş, bunun yerine kişisel veri kategorilerinin açıklanması düzenlenmiştir. İşlemenin kontrolörün veya üçüncü bir kişinin meşru menfaatleri için gerçekleştirildiği hallerde kontrolör veya üçüncü kişi tarafından hedeflenen meşru menfaatler hakkında verilecek bilgi ise, işlemenin adil ve şeffaf olmasını sağlamak için bilgiye konu kişiye sağlanması gereken bilgiler arasında sayılmıştır. Ayrıca sözleşmesel zorunluluklar ve bunun sonuçları hakkında bilgi verilmesi aranmamış, kişisel verilerin kaynağı ve kamuya açık bir kaynaktan gelip gelmediği bilgilerinin bilgiye konu kişiye sağlanması öngörülmüştür.

Yasa'nın, bilgilendirme hakkı altındaki kurallara 95/46/EC Sayılı Direktif'le paralel şekilde yer verildiği görülmektedir. GDPR'ın, 95/46/EC Sayılı Direktiften ayrıldığı nokta ise, 95/46/EC Sayılı Direktif'in uygulamada olduğu dönemde Üye Devletler, veri sahiplerine sağlanması gereken bilgilere ilişkin farklı düzenlemeler benimsemişken, GDPR'ın bu konuda yeknesak bir uygulama sağlamasıdır.[240]

[240] Korff, D. (2002) EC Study on Implementation of a Data Protection Directive: Comperative Summary of National Laws, Londra, Human Rights Centre University of Essex, s.98.

Ayrıca GDPR, veri sahibinin kişisel verileri hakkında bilgilendirilmesi ile ilgili olarak 95/46/EC Sayılı Direktif'e göre geniş kapsamlı düzenleme yapmıştır. Yasa'nın, bilgiye konu kişinin bilgilendirilme hakkı ile ilgili kurallarını, GDPR'ın öngördüğü kurallar ve güncel ihtiyaçlar ışığında yeniden düzenlenmesi faydalı olacaktır.

4.6.2. Erişim Hakkı

Bilgiye konu kişilerin diğer bir hakkı ise kendilerine ait işlenmiş olan verilere erişim hakkıdır. Yasa, 95/46/EC Sayılı Direktif'te belirtilen veri sahibi haklarına ilişkin kurallardan birçoğunu alarak bilgiye konu kişinin "erişim hakkı" (madde 14), "itiraz hakkı" (madde 15), "erişim ve itiraz haklarını kullanılması" (madde 16), "doğrudan veya dolaylı pazarlama için işleme" (madde 17) başlıklarıyla ayrı ayrı maddeler halinde kurallara tabi tutmuştur.

GDPR ise veri sahibinin haklarını detaylı olarak incelemiştir. Yasa'da ve 95/46/EC Sayılı Direktif'te ayrı ayrı yer verilmiş erişim ve itiraz hakkında belirtilen hükümleri tek başlık altında birleştirerek doğru bir düzenleme yapmıştır. Zira erişim ve itiraz haklarının içerisinde belirtilen kurallar ve haklar birbirleri ile ilişkili, bazı noktalarda aynı olduğundan, her iki maddenin yeknesak şekilde düzenlenmesi anlam karmaşasına yol açmaması bakımından faydalıdır.

Yasa ve GDPR'ın belirlemiş olduğu haklar bazı farklılıklar haricinde temelde aynı kurallara dayanmakta olduğundan, her iki mevzuat hükümlerine birlikte değinilecektir.

A. Bu kurallara göre bilgiye konu kişinin sahip olduğu haklar;

1. kişisel verilerinin işlenip işlenmediğini öğrenme, işlenmiş verisi varsa bu verilere ulaşma hakkı.

2. İşlemenin amacı, kişisel veri kategorileri hakkında bilgi edinme hakkı.

3. Kişisel verilerin açıklandığı veya açıklanacağı, özellikle üçüncü ülke veya uluslararası kuruluşlardaki alıcı veya alıcı kategorileri hakkında bilgi edinme hakkı;

Yasa'da "bu bilgiyi alanlar veya alan kategoriler" ifadesine yer verilmiştir. Ancak, GDPR'da olduğu gibi yalnızca alanlar değil, verinin açıklanmasının planlandığı alıcılar hakkında da bilgi verilmesi kişinin haklarını kullanabilmesi açısından önemlidir. Bununla birlikte alıcı tanımına Yasa'da yer verilmediğinden, alıcıların içerisinde yurtdışında bulunan bir alıcının da dahil olabileceğinin Yasa'da açık şekilde ifade edilmesi faydalı olacaktır.

4. Mümkün olan hallerde kişisel verinin öngörülen saklama süresi, mümkün değilse bu sürenin belirlenmesi için kullanılacak kriterler hakkında bilgi edinme hakkı;

Yasa'da yer almayan bu kuralın, verilerin işlenmesinde uyulacak ilkelerde belirtilen sınırlı süre ilkesinin bir yansıması olduğu görülmektedir. Bu çalışmanın "genel ilkeler" başlığı altındaki değerlendirmelerimizde de belirtildiği gibi, Yasa'nın verilerin saklanma süresi ile ilgili daha belirgin kurallar yer almalı, Başkan'ın inisiyatifi olmaksızın her bir verinin kendine özgü gereklilikleri ve mevzuatların öngördüğü kurallar ışığında saklanma sürelerinin belirlenmesi gerekmektedir. Belirtilenler doğrultusunda, bilgiye konu kişinin erişim hakkını kullanarak verilerin saklama süresi ile ilgili bilgi sahibi olması sağlanmalıdır.

5. Bir önceki bilgilendirmeden beri işlemede kaydedilen ilerleme hakkında bilgi edinme hakkı;

GDPR'da olmayıp Yasa'da bulunan bu kurala göre veri sahibinin erişim hakkını kullanması ve kontrolörün verdiği cevap sürecinde veri sahibine iletilen tüm bilgilerin detaylı şekilde kaydının tutulması ve o bilgiyle ilgili olarak, bir sonraki erişim hakkının kullanımında doğru bilgileri verebilmesi maksadıyla kontrolör tarafından teknik geliştirmelerin yapılması gerekmektedir.

6. Kontrolörden kişisel verilerin düzeltilmesini veya silinmesini, bilgiye konu kişiyle alakalı işlemenin sınırlandırılmasını talep etme veya işlemeye itiraz etme hakkının varlığı hakkında bilgilendirilme hakkı;

Bilgiye konu kişinin bu hakkıyla ilgili olarak Yasa hem erişim hakkı hem itiraz hakkı altında düzenlenmeler yapmıştır. Erişim hakkının düzenlendiği 14. maddenin 2. fıkrasında veri sahibinin belirtilen hususlarda, kontrolöre, soru sorma ve yanıt alma hakkına sahip olduğu belirtilerek (B) bendinde "verinin düzeltilmesi, silinmesi veya bloke edilmesi, özellikle yanlışlıklar ve eksiklikler nedeniyle bu Yasa uyarınca icra edilmemiş olan işleme" denilmiştir. Bu kuralın ifadesinin tam olarak anlatılmak istenileni ifade etmediği görülmektedir. Fıkranın başlangıç cümlesi ile bendin gelişine bakıldığında ifade bozukluğu olduğu, bu bent için veri sahibinin bu hakka sahip olduğuna dair bir ibarenin eklenmesi uygun olacaktır. Diğer yandan "yanlışlıklar ve eksiklikler nedeniyle bu Yasa'nın kuralları uyarınca icra edilmemiş işleme" ifadesiyle neyin kastedildiğinin net olmadığı, Yasa kurallarına göre işlenmesi gerekip de işleme konulmayan bir verinin tespitinin yapılıp veri sahibine bildirilmesi ise de, pratikte bu hakkın uygulanmasının zorluğunun aşikar olduğu görülmektedir. 95/46/EC Sayılı Direktif'teki maddenin çevirisinde yapılan bir hatadan kaynaklı da net olmayan bir ibare koyulmuş olabileceği göz önünde tutulmalıdır.[241]

Diğer yandan itiraz hakkının yer aldığı 15. maddenin 1. fıkrasında, bilgiye konu kişinin içinde bulunduğu özel duruma ilişkin meşru nedenlerle kendisi hakkında işlenmiş ya da işlenecek veri hakkında kontrolöre yapağı itirazda; düzeltme, kullanımdan geçici olarak imtina, bloke etme, iletilmesinden veya silinmeden imtina, işlenmeme ve silinme gibi belirli bir işlemin yapılması veya yapılmaması hususlarına yer verilmesi gerektiği belirtilmiştir. Öncelikle bu fıkrada belirtilen

[241] 95/46/EC Sayılı Direktifin 12 (b) maddesi "as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive in particular because of the incomplete or inaccurate nature of the data" denilmektedir. Bu cümlede esasında "verinin eksik veya yanlış niteliği sebebiyle bu Direktif hükümlerine uygun işlenmeyen verilerin düzeltilmesi, silinmesi veya engellenmesi" hakkı kastedilmektedir. Yasa, bu kuralı farklı şekilde almakla birlikte böyle bir zorunluluğu olmadığının da belirtilmesi gerekmektedir. Ancak koyulan hükmün anlaşılır ifadeleri içermesi gerektiği açıktır.

"özel duruma ilişkin meşru nedenler" ifadesinin kaldırılması gerekmektedir. Bireyin haklarını kullanması kısıtlanmamalı, bu haklarını kullanması için meşru nedenlerin olması beklenmemelidir.[242]

Öte yandan, 14. ve 15 maddelerde iki ayrı şekilde benzer hakların belirtilmekte olduğu düşünüldüğünde, her iki hakkın aynı madde altında düzenlenmesi faydalı olacaktır.

7. İmkansız olmadığı ve orantısız çaba gerektirmediği sürece, yapılan her türlü düzeltme, silme ve bloke etme hakkında verinin iletildiği üçüncü taraflara bildirim yapılması hakkı;

Bu talep hakkı 95/46/EC Sayılı Direktif'te yer alan Yasa'ya da eklenmiş olan bir kural olarak karşımıza çıkmakta olup, veri üzerinde yapılan herhangi bir işlem olduğunda, özellikle verilerin silinmesi ile ilgili bir işlem yapıldığı takdirde bu işlem hakkında alıcıların da bilgi edinmeleri önemlidir, dolayısıyla bu hakkın Yasa'da korunması gerektiği değerlendirilmektedir.

8. Denetim makamına şikayette bulunma hakkı.

9. Kişisel verilerin bilgiye konu kişiden elde edilmediği hallerde verilerin kaynağına ilişkin tüm mevcut bilgiler hakkında bilgi edinme hakkı.

---

[242] GDPR'ın 21. maddesinde itiraz hakkı başlığı altında yapmış olduğu düzenlemeye göre, md 6(1) (e) ve (f) bentlerinde veri sahibi kamu yararı nedeniyle kontrol veya üçüncü kişinin menfaatlerine dayanarak yapılan işlemede, bu düzenlemelere dayanan profiller olmak üzere, kendi somut durumuna dayanarak her zaman itiraz edebilir. Kontrolör, işlemenin veri sahibinin menfaatleri, hak ve özgürlüklerine baskın çıkan yasal dayanakları olduğunu veya yasal hakların tesisi, kullanılması ya da korunması için gerekli olduğunu ortaya koymadıkça kişisel verilerin işlemeye devam edilemeyeceğini düzenlemiştir. Görüldüğü üzere kişinin kendi somut durumuna dayanarak itiraz edilmesi hakkı kamu yararı ve veri sahibi dışındaki kişilerin menfaati için olan işlemede söz konusu olmaktadır. Bunun haricinde kişi her zaman verisinin işlenmesine itiraz edebilir, buna ek gerekçe göstermesine gerek yoktur.

10. GDPR'ın 22(1) ve (4). maddelerde anıldığı şekilde, profilleme dahil olmak üzere, otomatikleştirilmiş karar vermenin uygulandığı[243] ve bu hallerde asgari olarak uygulamanın mantığına dair anlamlı bilgiler ve işlemenin önemi ve bu işlemenin ilgili kişi bakımından sonuçları hakkında bilgi edinme hakkı;

Otomatik kararlar, herhangi bir insan müdahalesi olmadan yalnızca otomatik yollarla işlenen kişisel verileri kullanarak alınan kararlardır. Veri sahipleri yasal etkiler üreten veya benzer şekilde önemli etkileri olan otomatik kararlara tabi olmamalıdır. Bu tür kararların önemli bir etkiye sahip olması muhtemel ise örneğin, kredibilite, elektronik ortamda işe alım prosedürü, işteki performans veya davranış ya da güvenilirliğin analizi ile ilgili olarak bireyin yaşamında olumsuz sonuçlardan kaçınmak için özel koruma gereklidir. Bu karar konusunu bir örnekle izah etmek gerekirse; bir finans şirketinin bir müşterisinin kredibilitesini hızlıca değerlendirmek için müşterinin kredi ve diğer hesaplarını nasıl devam ettirmeyi sağladığını, müşterinin önceki adreslerini, kamuya açık kaynaklardan müşterinin yargı geçmişi gibi sicil kaydını, iflası gibi belirli verileri toplar ve bu veriler bir puanlama algoritması ile potansiyel müşterinin kredibilitesinin değerlendirilmesi konusu otomatik kararlara bir örnektir.[244]

Bu hak, 95/46/EC Sayılı Direktif'te olup Yasa'da yer verilmeyen bir haktır. Özellikle kurumsal şirketlerin çalışanlarının performansını değerlendirmesi, bankaların veya finans şirketlerinin kredi verirken yaptıkları araştırmalar vesair prosedürler ülkemizde yaygın şekilde kullanılmakta, bu işlemlerle veri sahipleri otomatik kararlara konu haline gelmektedir. Bu nedenle, 95/46/EC Sayılı Direktif ışığında Yasa hazırlanırken bu hakka ilişkin kural Yasa'ya eklenmemişse de gelişen

[243] GDPR'da veri sahibinin hakları arasında düzenlenen ve 22(1) maddesine göre "veri sahibi, profilleme dahil olmak üzere sadece otomatik işlemeye dayanan ve kendisi hakkında hukuki sonuçlar doğuran veya onu benzer surette önemli ölçüde etkileyen bir karara konu olmama hakkında sahiptir" 22(4) maddesinde ise veri sahibinin hak ve özgürlükleri ile meşru menfaatlerinin korunması için uygun güvencelerin alınmadıkça bu kararın hassas veriler için uygulanamayacağı belirtilmiştir.

[244] Giakoumopoulos, s.233.

teknik imkanlar doğrultusunda ülkenin mevcut durumunun göz önünde tutulması ve bu hakkın da Yasa'ya eklenmesi faydalı olacaktır.

11. Kişisel verilerin, Komisyonun yeterlilik kararının bulunmadığı üçüncü bir ülkeye veya uluslararası kuruluşa uygun tedbirler alınarak aktarıldığı durumlarda bu tedbirler hakkında bilgi edinme hakkı;

Bu kural da GDPR'da yer verilen bir kural olup, verileri yurtdışına transferi ile ilgili Yasa metinlerinin yeniden düzenlenmesinde, verilerin uygun tedbirler alınarak transferi ile ilgili bir kural konulması halinde, belirtilen bilgilendirilme hakkı bu tedbirler için de düzenlenmelidir.

4.6.3. Bilgiye Konu Kişinin Haklarının Sınırlandırılması

Bilgiye konu kişinin haklarının sınırlandırılması şartlarında ise Yasa ve GDPR kurallarının benzediği görülmektedir. Yasa'nın düzenlemesine göre, Kontrolör, Kurul kararı ile bilgiye konu kişiye bilgi verilmesini, özel bir yasada açıkça öngörülmüş olması, üstün nitelikte bir kamu yararı, Devletin iç ve dış güvenliğinin korunması açısından gerekli olması, bilgi verilmesinin idari veya cezai bir soruşturmanın amacının gerçekleşmesini güçleştirmesi durumlarında sınırlayabilir, erteleyebilir veya reddedebilir; ayrıca bunların sebebini ilgili kişiye yazılı olarak bildirebilir.

GDPR'da ise bu sınırlandırma daha geniş kapsamlı tutulmakla birlikte önemli sınırlamalardan birkaçına değinilecektir. GDPR'a göre, sınırlandırmanın temel hak ve özgürlüklerin özüne saygı gösterdiği ve demokratik bir toplumda gerekli ve orantılı bir tedbir olduğu durumlarda, ulusal güvenlik, savunma, kamu güvenliği, kamu güvenliğine yönelik tehditlere karşı koruma ve önleme dahil suçların önlenmesi, soruşturulması, tespiti ve kovuşturulması veya cezaların uygulanması,

yargı bağımsızlığının ve adil yargılamanın korunması sebepleriyle sınırlandırılabilir.

Yasa'da yer alan sınırlamanın yeniden gözden geçirilmesi aşamasında, GDPR'ın özellikle temel hak ve özgürlüklerin özüne saygı gösterilmesi ve ülke demokrasisinin gerekliliği durumlarında sınırlamanın yapılması kurallarının göz önünde bulundurulması önemli olacaktır.

4.6.4. Bilgiye Konu Kişinin Erişim ve İtiraz Haklarının Kullanılması

Yasa, bilgiye konu kişinin verilerine erişimi ve itiraz haklarını kullanabilmesi yöntemini 16. maddede düzenleyerek, kişinin erişim hakkını, Kurul'un çıkaracağı Tüzük'te belirtilen bir ücret karşılığında kontrolöre başvurunun sunulması ile kullanabileceği belirtilmiştir. Kontrolörün veya Kurul'un düzeltme veya silinme talebini yerinde bulunması halinde, kontrolörün başvuru sahibine gecikmeksizin ve hiçbir ücret almaksızın anlaşılabilir bir ille kendisini ilgilendiren işlemenin düzeltilmiş halini vermekle yükümlü olduğu düzenlenmiştir. Bu başvurunun bir ücret karşılığında yapılabilmesi hususunun değerlendirilmesi gerekmektedir. 95/46/EC Sayılı Direktif'in erişim hakkının kullanılmasını düzenleyen 12. maddesine bakıldığında, "aşırı gecikme veya masraf olmaksızın" veriye erişim hakkı tanınmıştır. Verilere erişim ve itiraz hakkının kullanılmasında kontrolöre bir ücret ödenmesi, tekrarlayan veya amacını aşan kişi taleplerinin önüne geçilmesi ya da kontrolörlerin gereğinden fazla şekilde insan gücü ve zaman harcamasına yol açılmaması bakımından makul görülebilir. Ancak ücretler için çıkarılacak Tüzük'te belirlenecek ücretin bilgiye konu kişilerin haklarını kullanmalarını zorlayacak ölçüde yüksek olmaması, toplumun her kesiminden insanın haklarından yararlanmasına zemin hazırlayacak makul bir ücret olmasına dikkat ve özen

gösterilmelidir. Bu nedenle Yasa ile bu ücretin belirlenmesinde uygulanacak kriterlerin özel olarak belirlenmesi faydalı olacaktır.[245]

4.6.5. Doğrudan veya Dolaylı Pazarlama

Kişisel verilerin pazarlama maksadıyla kullanılması yaygındır. Özellikle son yıllarda teknolojinin gelişimiyle birlikte kişisel verilerin yer aldığı veri tabanlarının ticari olarak kullanılması durumu oldukça yaygın ve tehlikeli boyutlara dahi ulaşmıştır. Bu nedenle bilgiye konu kişilerin verilerinin pazarlama maksadıyla kullanılması konusunda verileri üzerinde söz sahibi olmaları önemlidir.

Yasa'nın 17. maddesine göre, kontrolör bilgiye konu kişiden yazılı onay almadıkça, bilgiye konu kişinin kişisel verisini doğrudan veya dolaylı pazarlama maksadıyla kullanamayacaktır. Bu amaç için izin almak üzere bilgiye konu kişiye ulaşmasında ise, kamuya açık kaynaklardan temin etmek suretiyle, bilgiye konu kişinin adını ve adresini kullanabileceği düzenlenmiştir.

GDPR'ın doğrudan pazarlama ile ilgili hükmünü düzenleyen 21. maddesinin 2. fıkrasına göre, kişisel verilerin doğrudan pazarlama amacıyla işlendiği hallerde bilgiye konu kişi kendisine ait kişisel verilerin, söz konusu doğrudan pazarlama ile ilgili olduğu ölçüde, profilleme de dahil olmak üzere bu pazarlama için işlenmesine her zaman itiraz etme hakkına sahiptir.

Yasa'nın konuyla ilgili düzenlemesinin GDPR'ın düzenlemesinden daha sıkı tutulduğu görülmektedir. GDPR bilgiye konu kişiye sahibine ek olarak, pazarlama alanında profilleme yapmak suretiyle verinin işlenmesine itiraz hakkı tanımıştır.

---

[245] Yasa'nın Kurula ücret belirleme yetkisini veren 37. maddesinde, belirlenecek ücretin aylık asgari ücretin binde beşinden az ve aylık asgari ücret miktarından fazla olamayacağı düzenlenmiştir. Ancak önerimizde belirtilen kriter, kişilerin haklarını kullanmasını teşvik etmeyi sağlayacak, diğer taraftan kontrolörler açısından amacını aşan taleplerle zayi olabilecek insan gücü ve zamanının da önüne geçilmesini sağlayacak ölçüde belirlenmesinin kriter olarak eklenmesidir.

Ancak Yasa'da yer alan "dolaylı pazarlama" ile kastedilen pazarlama yöntemi açık olmadığından, GDPR'ın kapsamına aldığı profilleme yönteminin de dolaylı pazarlama içerisinde sayılabileceği düşünülebilir. Yasa'nın koyduğu sıkı şartlar yerinde olmakla birlikte doğrudan ve dolaylı pazarlama ile kastedilenin daha açık olması sağlanabilir.

4.6.6. Silinmeyi Talep Hakkı

Yasa'da veri sahibinin talepleri arasında verilerin silinmesi hakkını talep etme hakkı bulunmaktadır. Ancak, bu çalışmada AB Mevzuatı altında işlenen GDPR (1.2.4.g.) bölümünde belirtildiği üzere GDPR'ın getirdiği bir yenilik olan unutulma hakkı düzenlemesi mevcuttur. GDPR "Silinmeyi Talep Hakkı (Unutulma Hakkı)"nı 17. maddesinde detaylı şekilde düzenlemiştir. Bu kurala göre bilgiye konu kişinin silinme hakkına sahip olduğu ve aşağıdaki hallerden birinin varlığı halinde bu hakkını kullanması halinde, kişisel verilerin gecikmeksizin silinmesinin kontrolör açısından da bir yükümlülük olacağı düzenlenmiştir. Bu haller;

- kişisel verilerin elde edildikleri veya başka surette işlendikleri amaçla ilgili olarak artık gerekli olmaması

- işlemenin rızaya dayanarak yapıldığı hallerde veri sahibinin rızasını geri çekmesi ve işleme için başka bir yasal dayanak olmaması

- bilgiye konu kişinin işlemeye itiraz hakkını kullanması ve işleme için baskın çıkan meşru menfaatlerin bulunmaması

- kişisel verilerin hukuka aykırı şekilde işlenmiş olması

- kişisel verilerin Birlik veya kontrolörün tabi olduğu Üye Devlet hukukundan kaynaklanan hukuki bir yükümlülüğe uymak için silinmesinin gerekmesi

- kişisel verilerin bir çocuğa bilgi toplumu hizmetlerinin sunulması ile bağlantılı olarak elde edilmesi.

Kontrolörün, silinmesi talep edilen kişisel veriyi kamuya açıklamış olduğu hallerde, bu veriyi işleyen diğer kontrolörleri de veri sahibinin silinme hakkını kullandığı yönünde bilgilendirmesi gerekmektedir. Bu yükümlülük, kontrolörün mevcut teknoloji ve uygulama masrafları göz önünde bulundurularak, alınabilecek teknik tedbirler dahil kendisinden beklenebilecek makul adımları atması yeterli olacaktır, zira ilgili veri birçok kontrolör tarafından kullanılmış olabilir. Bu kuralı 95/46/EC Sayılı Direktif'te ve dolayısıyla Yasa'da yer alan silinme hakkından ayıran en önemli özellik de budur. Bu kural ile yalnızca kontrolörün kişisel veriyi silmesi değil, verinin yayıldığı diğer kontrolörlerin de aynı şekilde davranmalarını sağlaması için harekete geçmesi aranmaktadır ve bilgiye konu kişiye gerçek anlamda bir "unutulma hakkı" tanınmaktadır.

Özellikle dijital dünyadaki gelişmeler, kişisel verilerin yaygın şekilde kullanılması durumları göz önünde tutulduğunda, bilgiye konu kişiye böyle bir hakkın tanınması ülkemiz için de faydalı olacak, kişi hak ve menfaatlerinin korunmasına katkı sağlayacaktır. Dolayısıyla bu hakkın da Yasa kapsamına alınması gerekmektedir.

Tüm bunların dışında Yasa'nın bir eksikliği olarak belirtilmesi gerekir ki, bilgiye konu kişinin kişisel verilerinin silinmesini talep etmesi ya da öngörülen saklama süresi dolan verilerin silinmesi, yok edilmesi ya da diğer bir yöntem olan anonim hale getirilmesine dair bir kural bulunmamaktadır. Veriler üzerinde bu işlemleri yapacak olan kontrolör veya hale göre işlemcinin tabi olacağı kurallara ayrıca yer verilmesi gerekmektedir.

4.7. Kontrolör ve İşlemcinin Sorumlulukları

4.7.1. Tazmin Etme Yükümlülüğü

Bilgiye konu kişinin kişisel verilerinin mevzuata aykırı şekilde kullanılmasından dolayı uğradığı zararların tazminini isteme hakkı bulunmaktadır.

Yasa'nın 18. maddesine göre Kontrolör, zararı doğuran olaydan dolayı sorumlu olmadığını kanıtlamadıkça, bu Yasa'nın herhangi bir kuralının ihlalinden dolayı zarar gören bilgiye konu kişinin zararını tazmin edeceği düzenlenmiştir.

GDPR'da ise 82. maddede tazminat hakkı ve sorumluluk daha kapsamlı olarak düzenlenmiştir. Kısaca değinmek gerekirse, GDPR'ın öngördüğü kuralların ihlali nedeniyle maddi veya manevi zarara uğrayan kimse, bu zarar için kontrolör veya işlemci tarafından tazmin edilme hakkına sahiptir. İşlemeye katılan her kontrolör, bu Direktif'in ihlalinden dolayı oluşan zarardan sorumludur. İşlemci ise Direktif'in özel olarak işlemciye yönelttiği yükümlülüklere uymadığı ya da kontrolörün talimatları dışında veya talimatlara aykırı davrandığı hallerde, işlemenin neden olduğu zarardan sorumlu olacaktır. Kontrolör veya işlemci bu ihlalin neden olduğu zarardan hiçbir şekilde sorumlu olmadığını kanıtlarsa, bu sorumluluktan kurtulabilecektir.

Yasa'nın düzenlemesine bakıldığında, kontrolörün sorumlu tutulması kaçınılmaz bir hükümdür ancak bir ihlale sebebiyet veren davranış yalnızca kontrolör tarafından yapılmayabilir. Bir sonraki bölümde inceleyeceğimiz işlemenin güvenliğine ilişkin düzenlemelerde de görüleceği üzere, işlemci veya işlemcinin yetkisinde görev yapan kişiler, kontrolörün talimatına göre işlemlerini yürütmelidirler. Bu kişilerin yapabilecekleri ihlalden sorumlu tutulmaları verinin güvenliğinin sağlanmasına önemli ölçüde katkı sağlayacaktır. Bu nedenle müşterek sorumluluğun düzenlenmesi faydalı olacaktır.

4.7.2. İşlemenin Güvenliği

Kişisel verinin işlenmesi konusunda hem gizliliğin hem güvenliğin temin edilmesi önemlidir. Veriyi işleme alan herkes, bu gizlilik ve güvenlikten sorumlu olacaktır. Bu konuda Yasa da GDPR da çeşitli düzenlemeler yapmıştır. Her iki mevzuatın öngördüğü kuralların önemli noktalarına kısaca değinilecektir.

4.7.2.a. Veri Koruma Görevlisi

Yasa'nın, 10. maddesinde kişisel verileri işleyen her kurum ve kuruluşun, işlediği veriyi korumakla görevli en az bir personel görevlendirmekle yükümlü olduğunu, bu görevlinin Yasa çerçevesinde kontrolörün isteyebileceği bilgiler doğrultusunda kurumdaki kişisel verilerin işlenmesini ve korunmasını izleyeceği ve gözeteceği düzenlenmiştir.

GDPR ise, 37. maddesinde işlemenin yargısal faaliyette bulunan mahkemeler hariç, bir kamu kurumu veya kuruluşu tarafından gerçekleştirilmesi halinde ya da kontrolörün veya işlemcinin esas faaliyetleri, tabiatı, kapsamı ve/veya amaçları gereği bilgiye konu kişilerin düzenli ve sistematik şekilde gözlemlenmeleri gerektiği hallerde ya da hassas verilerin geniş çaplı işlenmesine ilişkin ise bilgi güvenliği yetkilisi atanmasını öngörmüştür. Ayrıca Birlik veya Üye Devlet hukuku, sayılan haller dışında kontrolör veya işlemcilerin bilgi güvenliği yetkilisi atamasını zorunlu kılabilir.

Yasa'nın 10. maddesiyle GDPR'ın öngördüğü kuralı, kontrolör veya işlemci ayrımı yapmaksızın görevli atanması yönündeki düzenlemesi ile karşılamakta olduğu görülmektedir. Ancak, veri koruma görevlisinin "kontrolörün isteyebileceği bilgiler doğrultusunda kurumdaki kişisel verilerin..." ifadesiyle amaçlananın ne olduğunun net olmadığı görülebilmektedir. Veri koruma görevlisinin asli görevi verinin

korunmasını bağımsız şekilde gözetmektir bu nedenle kontrolör tarafından gelebilecek bir talebin karşılanması maksadıyla görevli atanamaz.[246]

Yasa'nın bu ifadesinin yeniden gözden geçirilmesi ve denetçinin görevlerinin, hangi konumda olacağının Yasa ile düzenlenmesi gerekmektedir.

4.7.2.b. İşlemenin Gizliliği ve Güvenliği

Yasa bu yükümlülüğü 12. maddesi altında düzenlemiştir. Bu kurala göre;

- verinin işlenmesi gizlidir. Bu işlem yalnızca kontrolör, işlemci veya işlemcinin yetkisi altında görev yapan kişilerce ve yalnızca kontrolörden alınan talimat uyarınca yapılır.

- işlemenin yapılması içini kontrolörün uygun nitelikleri taşıyan teknik bilgi açısından yeterli teminatı sağlayan ve gizliliğe riayet açısından şahsi güvenilirliği olan kişileri seçmesi gerekir.

- kontrolör, verinin istem dışı veya yasadışı zarara uğraması, istem dışı kaybı, değiştirilmesi, yetkisiz kişilere iletilmesi veya erişim imkanı sağlaması ve her türlü diğer yasadışı işleme tabi tutulmasına karşı gizliliğin ve korunmasının sağlanması için uygun kurumsal ve teknik önlemleri almalıdır. Bu önlemler, işleme sürecindeki ve veri işlemenin doğasına uygun düşecek riskleri karşılamada güvenliği temin etmelidir.

- Başkan, teknolojik gelişmeleri de göz önünde bulundurarak, verinin güvenliğine ve her kategoride veri için gerekli koruma önlemlerine ilişkin olarak zaman zaman talimat verebilir.

---

[246] GDPR'ın 38. maddesinin 3. fıkrasında da denetçinin bağımsızlığının sağlanması için ayrı bir düzenleme getirilmiştir. Bu kurala göre kontrolör veya işlemcinin, denetçinin görevlerinin ifasına dair hiçbir talimat alamayacağını temin etmelerini, denetçinin görevlerini ifa ettiği için kontrolör veya işlemci tarafından görevden alınamayacağını veya cezalandırılamayacağını düzenlemiştir.

- işleme, kontrolör adına kendi denetimi altında olmayan bir işlemci tarafından icra edilmekteyse, işleme görevinin verilmesinin yazılı olarak yapılması gerekmektedir. Görevlendirme işlemcinin işlemeyi yalnızca kontrolörden aldığı talimat üzerine yapmasını ve bu kısımda yer alan diğer yükümlülükleri de üstlenmesini sağlamalıdır.

Bu kuralla beraber Yasa gizlilik yükümlülüğünü ayrı bir maddede ele alarak 19. maddede, kontrolör ve işlemcilerin bu Yasa kuralları çerçevesinde öğrendikleri kişilere ait verileri, yasal olarak iletebilecekleri kişi veya mercilerden başkasına iletemeyecekleri veya açıklayamayacakları, ayrıca bu yükümlülüğün görevden ayrıldıktan sonra da devam edeceğini düzenlemiştir.

Yasa'nın gizlilik ve güvenlik ile ilgili düzenlemeleri ana hatlar açısından yerindedir. Bununla beraber bazı ek düzenlemelerle güncellendiği takdirde kuralın uygulanabilirliği daha kolay hale gelebilir.

Konuyla ilgili GDPR'ın 32. maddesinde örnek alınabilecek önemli düzenlemeleri bulunmaktadır. Şöyle ki, alınacak tedbirlerle uygun düştüğü ölçüde, kişisel verilerin psödonimleştirilmesi ve şifrelenmesi, işleme sistemleri ve hizmetlerinin gizliliğini, bütünlüğünü, ulaşılabilirliğini ve dayanıklılığını sürekli olarak temin etme yetisi, fiziksel veya teknik bir kaza olduğunda kişisel verilerin kurtarılması ve bu verilere erişimin yeniden sağlanması yetisi, işlemenin güvenliğini temin eden teknik ve organizasyonel tedbirlerin etkinliğini düzenli olarak kontrol etmek, ölçmek ve değerlendirmek için bir prosedür hazırlanması öngörülmektedir. Yasa'nın da böyle bir prosedürün hazırlanmasını içeren hükümleri içermesi, hem güvenlik için uygulanabilecek yöntemler açısından yol göstermesi hem de verileri işleyenlerin denetlenmesinin kolaylaştırılması açısından bir prosedürün hazırlanması ve bu prosedürün takibinin sağlanması açısından faydalı olacaktır.

Bununla beraber Yasa, gizlilik ve güvenliğe bir halel gelmesi halinde ne yapılacağı ile ilgili de yol gösterici olmalıdır. Örneğin bir ihlal durumunda bu ihlalin Kurul'a veya bilgiye konu kişiye bildiriminin nasıl, ne zaman, hangi usulle yapılacağı, nelerin bilgilendirmeyi gerektiren kriterde ihlal sayılacağı hususlarının kurala bağlanmış olması gerekmektedir.

4.8. Kişisel Verileri Koruma Kurulu

Kişisel verilerin korunmasına yönelik mevzuata sahip her ülke, ulusal düzeyde kişisel verilerin korunmasını denetlemekten ve izlemekten sorumlu denetim makamı oluşturmalıdır. Ülkemizde yürürlükte olan Yasa kapsamında da kişisel verilerin korunması konusunda denetim makamı sıfatıyla oluşturulması öngörülen kurul Kişisel Verileri Koruma Kurulu'dur.

Yasa'nın örnek alınmış olduğu 95/46/EC Sayılı Direktif'te oluşturulması öngörülen denetim makamı (supervisory authority) ve makamın sahip olması gereken temel özellikler, yasamızda da yer almış ve Kurul'un görevleri bu çerçeve baz alınarak hazırlanmıştır.

Kurul, kişisel verilerin korunması ve işlenmesi çerçevesinde kişilerin korunmasına dair kuralların uygulanmasını denetlemekten ve izlemekten sorumlu olacaktır. Kurul, tüzel kişiliğe sahip, idari ve mali özerkliğe sahip olacaktır. Bunun anlamı, oluşturulması öngörülen kurul, kendilerine özgü gelir kaynaklarına, ayrı bir bütçeye sahip olacak ve kendi kararlarına dayanarak harcama yapabilir durumda olacaktır. Bunun yanı sıra; dış müdahale ve denetimler noktasında bağımsız olacaktır.

GDPR, her bir Üye Devlet tarafından bağımsız denetim makamlarının oluşturulmasını öngörmektedir. Buna göre her Üye Devlet, gerçek kişilerin verilerini işlemeyle ilişkili temel hak ve özgürlüklerini korumak ve kişisel verilerin birlik dahilinde serbest dolaşımını kolaylaştırmak için bu Direktif'in uygulanmasını

gözetmekten sorumlu olmak üzere bağımsız kamu kurumu tesis edecektir. GDPR, madde 51'de de belirtildiği üzere, denetim makamı, Direktif kurallarıyla uyumlu olacak şekilde, diğer denetim makamlarıyla ve Komisyon'la işbirliği yapar.

Bu bağımsızlık GDPR'ın 52. maddesinde aşağıdaki şekilde yer almaktadır.

- Denetim makamı, görevlerini yerine getirirken ve yetkilerini kullanırken tam bağımsız olacaktır.

- Üye veya Üyeler, görevlerini yerine getirirken ve yetkilerini kullanırken dış etkilerden uzak kalır ve hiç kimseden emir ve talimat almaz.

- Üye veya Üyeler, görevleri ile bağdaşmayacak her türlü davranıştan uzak duracak ve görevleri süresince ücret karşılığı olsun ya da olmasın bu nitelikte bir işte çalışmaktan kaçınacaktır.

- Her bir Üye Devlet, denetim makamının Kurul'la ilişkilerinde yerine getirecekleri olmak üzere görevlerini etkin şekilde yerine getirmeleri ya da yetkilerini kullanmaları için gereksinim duyulan insan kaynağı, teknik ve finansal kaynakları, mekanı ve altyapıyı sağlayacaktır.

- Her bir Üye Devlet, denetim makamlarının münhasıran ilgili denetim makam üyesi ya da üyelerinin talimatına tabi olacak kadrosunu kurması ve bu kadroyu seçmesini temin edecektir.

- Her bir Üye Devlet, denetim makamının bağımsızlığını etkilemeyecek şekilde finansal denetime tabi olmasını ve kendi yıllık kamusal bütçesine sahip olmasını temin edecektir. Bütçe, genel devlet bütçesi ya da ulusal bütçeye de dahil olabilir.

Kişisel Verileri Koruma Kurulu'nun yapısının özerk ve bağımsız olması, en başta en yakın komşularımız olan Güney Kıbrıs ve Türkiye ile yapılabilecek veri aktarımları bakımından güvenli ülke sayılmamız için sahip olmamız gereken

kriterlerin başına gelmektedir. Bir ülkenin güvenli ülke sayılması içi etkin ve çalışır durumda bağımsız bir otorite olması aranmaktadır. GDPR'ın 45. maddesine göre Devlet, Kurul'un görevlerini etkin şekilde yerine getirmek üzere gerekli insan kaynağını, teknik ve finansal kaynakları, mekan ve altyapıyı sağlamalıdır. Ayrıca 42. maddede belirtildiği üzere, Kurul'un mali durumu ile ilgili olarak, Kurul'un bağımsızlığını etkilemeyecek şekilde finansal denetimin yapılması ve kendi yıllık kamusal bütçesinin olmasını temin etmelidir.

Kurul'un devletin işleyişinden, hükümetlerden, siyasi erklerden tamamen bağımsız şekilde oluşturulup, işlemlerini yürütebilmesi önemlidir. Bu Kurul'un güvenilirliği, ülkenin güvenli ülke sayılmasının başında gelecektir. Direktif'in 52. maddesi, Kurul'un görevlerini yerine getirmesinde tam bağımsız olması kuralını koymuştur. 45. maddede ise kişisel verilerin yurtdışına aktarımları için koruma seviyesinde yeterliliğinin değerlendirilmesinde, verinin aktarılacağı ülkede bağımsız bir denetim makamının olması şart koşulmuştur.

4.8.1. Kurulun oluşumu ve Üyelerin Nitelikleri

Kurul, Cumhurbaşkanı tarafından atanıp Cumhuriyet Meclisi'nin onayıyla atanan bir başkandan ve çeşitli kurumlardan atanmış olan on üyeden oluşacaktır. Üyelerden iki tanesi Cumhuriyet Meclisi tarafından, biri Bakanlar Kurulu kararı ile oluşturulan Kamu Net Üst Kurulunda görev yapan üyeler arasından olmak üzere Başbakan'ın önerisi ile Bakanlar Kurulu tarafından, Barolar Birliği, Kıbrıs Türk Ticaret Odası, Kıbrıs Türk Sanayi Odası, Kıbrıs Türk Mühendis ve Mimar Odaları Birliği ve Kıbrıs Türk Tabipler Birliği'nin kendi üyelerinden olmak üzere bu Birlikler tarafından atanacak birer üye ve Yükseköğretim Planlama, Denetleme ve Akreditasyon ve Koordinasyon Kurulunun akademisyenler arasından atayacağı bir üye olacaktır.

GDPR'a göre ise denetim makamının her bir üyesi, parlamento, hükümet, devlet başkanı veya Üye Devlet hukukunca tayin edilen bağımsız bir kuruluş tarafından şeffaf bir usul uygulanarak seçilecektir.

Yasa'ya göre Kurul üyeleri çeşitli meslek gruplarından oluşmaktadır. Bu çeşitlilik Kurul'un işleyişinde farklı fikirlerin olmasını ve farklı bakış açıları ortaya koyularak karara varılmasını sağlayacağı gibi, fikir birliğine varılmasını da zorlaştırabilir. Kanaatimizce üyelerin atanmasını düzenleyen maddenin bu çeşitliliğe hükmeden kısmının muhafaza edilmesi gerekmektedir.

Kurul Başkan ve Üyelerinde aranan nitelikleri düzenleyen 22. madde; "Kuzey Kıbrıs Türk Cumhuriyeti vatandaşı olmak, üniversite veya dengi bir yüksekokuldan mezun olmak, kamu haklarından yasaklı bulunmamak, bir yıldan fazla hapis cezasına çarptırılmamış olmak veya affa uğramış olsalar dahi, rüşvet, hırsızlık, dolandırıcılık, sahtekarlık, irtikap, ırza geçme, hileli iflas ve benzeri yüz kızartıcı suçlardan dolayı mahkum olmamış olmak, disiplin suçundan ötürü Kamu hizmetinden azledilmemiş olmak" şartlarını aramaktadır. Kurul Başkanı olarak atanacak kişinin bu maddede belirtilen özellikler yanında ayrıca "kamu görevinde veya kamu görevi dışında sorumluluk taşıyan bir görevde en az on yıl çalışmış olmak "veya" doktora seviyesinde lisansüstü eğitim yapmış ve kamu görevinde veya kamu görevi dışında sorumluluk taşıyan bir görevde en az beş yıl çalışmış olmak" şartları aranmaktadır.

GDPR'a göre Üyelerin, görevlerini yerine getirmeleri ya da yetkilerini kullanmaları için gereken, özellikle kişisel verilerin korunması alanında vasıf, deneyim ve yetilere sahip olmaları gerekmektedir.

Bize göre Yasa'nın en önemli eksikliklerinden bir tanesi de göreve atanacak Başkan ve üyelerin atandıkları Kurul'un görev ve sorumlulukları konusunda asgari bilgi ve tecrübeye sahip kişiler olmaları şartı aranmamasıdır. Nitekim GDPR'da denetim makamının üyeleri hakkındaki genel şartlar arasında üyelerin özellikle kişisel

verilerin korunması konusunda tecrübeli olması aranmaktadır. Uygulamada Kurul üyelerinin atanmasında bu niteliklere dikkat edilmiş ya da ileride dikkat edilecek olsa da herhangi bir merciinin inisiyatifinde olmaması açısından bu hususun Yasa ile belirlenmiş olmasının Yasa'nın iyileştirilmesi ve Direktif'e uyumu açısından olumlu bir değişiklik olacağı değerlendirilmektedir..

Ayrıca, oluşturulması öngörülen kurumsal yapıya bakıldığında, bir Başkan, tam zamanlı olmayan 10 üye ve verilen görevlerin yürütülmesini sağlamak üzere en fazla 10 kişiden oluşacak bir bürodan ibaret olacak olan kurumsal yapının Kurul değil Kurum olması ve bu Kurumun Başkan ve Üyelerden oluşacak Kurul ve işlerin yürütülmesine yetecek istihdama sahip bir bürodan oluşması gerekecektir. Kavram karmaşası olmaması açısından ilk etapta bu kurumsal yapının adlandırılmasının Kişisel Verileri Koruma Kurulu yerine Kişisel Verileri Koruma Kurumu olması ve Kurul Başkanı'nın aynı zamanda Kurum Başkanı da olması doğru olacaktır. Bununla beraber, Kurul Başkanı'nın yardımcısı makamının da Yasa'da yer almadığı görülmektedir. Gerek Başkan'ın görevlerinin yerine getirilmesinde yardımcı olacak gerekse Başkan'ın yokluğunda görevlerin idamesini sağlayacak bir yardımcının da oluşturulması gereken Kurum yapısına dahil edilmesi gerektiği açıktır.

4.8.2. Kurul Başkan ve Üyelerinin Görev Süresi ve Görevin Sonlanması

Kurul Başkan ve Üyelerinin görev süresi dört yıldır. Atayan makam tarafından görevden alınmadıkları sürece, süresi dolmadan görevi sona eren Başkan ve üyenin, yerine yeni kişiler atanana kadar görevleri devam eder. Görev süresi dolan Başkan veya Üye, yeniden atanabilmektedir. Kurul Başkanı veya Üyesi olarak atanmış olan kişiler, atandıkları tarihten başlamak suretiyle, siyasi partilerin organlarında görev alamazlar.

Kurul Başkanı veya Üyesinin ölümü veya istifa etmesi halinde, atamada aranan niteliklerden birini veya daha fazlasını kaybetmesi halinde, özürsüz olarak üst üste üç toplantıya katılmaması halinde, atayan makam veya kurumca görevde alınması halinde Kurul Başkan ve üyelik boşalmaktadır.

GDPR'a göre Üye Devletler, yürürlüğe koyacakları Yasa ile her bir denetim makamının kuruluşunu, üye olarak atanmak için sahip olunması gerekli vasıfları ve atama koşullarını, üyelerin atama kural ve usullerini, dört yıldan az olmamak şartıyla, ancak denetim makamının bağımsızlığını korumak üzere kademeli bir atama usulü uyarınca bir kısmı daha az belirlenebilecek şekilde görev sürelerini, üyelerin yeniden atanıp atanmayacaklarını, atanacaksa kaç dönem atanabileceğini, üyelerin yükümlülüklerini belirleyen şartları, görev süresi boyunca ve sonrasındaki yasak faaliyetleri, meslekleri ve menfaatleri, görevlerinin sona erdirilmesine ilişkin kuralları belirler.

Üyelerin ilgili Üye Devletin hukukuna uygun olarak görev sürelerinin bitimi, istifası ya da zorunlu emeklilik hallerinde görevi sona erebilir. Bununla beraber, GDPR, madde 53'de de belirtildiği üzere Üyeler, ancak görevlerini ciddi surette suiistimal eder ya da görevlerinin ifası için gerekli şartlara artık sahip olmazlarsa görevden alınabilirler.

Yasa'da oluşturulacak Kurul'un şeffaflığı, güvenirliği açısından sakıncalı görülen bazı kurallar bulunmaktadır. Şöyle ki, Kurul Başkanı Cumhurbaşkanı tarafından atanacak, üyelerinin dört tanesi ise siyasi partiler tarafından atanacaktır. Başkan ve üyenin siyasal parti organlarında yer almaması kuralından anlaşılan odur ki, siyasi partiler ile organik bir bağ olmaması beklenmektedir. Fakat gerek Cumhurbaşkanı tarafından atanan Başkan'ın gerekse siyasi partilerin aday göstermesi ve Cumhuriyet Meclisi'nin bu adayları oylaması yöntemi, inorganik bir bağ yaratmaktadır. Bu yöntemle siyasi partiler, kendi adaylarını ya da parti ideolojisin en yakın kişiyi destekleyecektir. Aynı şekilde, Cumhurbaşkanı da ister istemez iç politikadaki ideolojisinden dolayı kendine en yakın kişiler arasından Başkan'ı

atayabilir. Bununla beraber, Kurul Başkan ve üyeliğinin boşalmasına yönelik kurallara bakıldığında, atayan makamın veya kurumun atadığı Üye'yi görevden alabilmesi hakkı bulunmaktadır ve görevden alma şartları da belirtilmemiştir. Yani siyasi partilerin ya da Cumhurbaşkanı'nın ideolojisine ters bir davranışta bulunabilecek her Başkan ve Üye, görevden alınma tehlikesi ile karşı karşıya kalabilir. Tüm bunların olma ihtimali, Kurul'un üzerinde bir gölge oluşturabilir, Kurul'un işleyişini, verdiği kararları ya da uygulamalarını kamu veya veri sahibi açısından şaibeli hale getirebilir. Kurul Başkan ve Üyeleri'nin atanmaları, atandıkları kurum veya makamca görevden alınabilmesi kurallarının gözden geçirilmesi gerekliliği yanında, bu kişilerin siyasi parti organlarında görev almaları değil, üye bile olmamaları gerektiğine yönelik kural getirilmelidir. Aksi halde, kişisel verilerin korunması gibi hassas bir konu için görev alacak olan Kurul, daha başından kamu tarafından güvensiz ilan edilebilir. Görevden alma ya da göreve son verme kararı ancak görevde işlediği suçlardan dolayı mahkumiyeti halinde verilmelidir.

Kurul Başkan ve üyelerinin görevlerine son verilmesi şartlarının sıkı tutulması, atanma şartlarından birini yitirmesi, istifa, sağlık nedeniyle zorunlu emeklilik, görevinde işlediği suçlardan dolayı yargılanıp mahkum edilmesi gibi durumların varlığı dışında görevlerine son verilememesi şartı koşulmalıdır. Bu sayede; özellikle siyasi partilerle veya Birliklerle organik ya da inorganik bağı olan Başkan ve Üyelerin görevlerinde bağımsızlığının sağlanabilmesi mümkün olacaktır.

Kurul Başkan ve Üyeleri'nin görevleri ile ilgili olarak görev süreleri ve yeniden atanabilmeleri hususu ile ilgili olarak eksikliği görülen nokta, Başkan ve Üyeler'in kaç dönem tekrar seçilebilecekleridir. Bu belirleme, Direktif'in 54. maddesinde de yer almaktadır. Kurul'un kendisini yenilemesi, belirli insanların tabiri caizse tekeline dönüşmemesi açısından tekrar eden dönemlere bir kısıtlama getirilmesi gerekmektedir. Bize göre Kurul Başkan ve Üyelerinin 2. dönem seçilme hakları da olmamalıdır. 2. dönem tekrar seçilmek isteyen Başkan ve Üyeler kendilerini o

makama atayacak veya seçecek kişi veya kuruma karşı görevlerini suiistimal edebilirler ve kurumun bağımsızlığına gölge düşürebilirler.

4.8.3. Kurulun Toplantıları

Sürekli çalışan Kurul, olağanüstü bir durum olmadıkça ayda en bir kez toplanacaktır. Toplantı yeter sayısı üye tam sayısının salt çoğunluğu, karar yeter sayısı ise toplantıya katılanların salt çoğunluğudur. Kabul ve ret oylarının eşit olması durumunda oylamaya konulan husus reddedilmiş olur. Çekimser oylar, toplantı yeter sayısına dahil olup, karar yeter sayısı açısından dikkate alınmaz. Oylamalar, açık oyla yapılır. Kurul üyeleri, kendileri veya temsil ettikleri kurumların taraf olduğu şikayet konularına ilişkin kararlara katılamaz.

Kurul'un toplantı usulüne bakıldığında Başkan dahil 11 kişiden oluşan Kurul'un salt çoğunluğu ile toplanılabileceği, katılan üyelerin salt çoğunluğuyla da karar alınabileceği düzenlenmiş ve çekimser oylar ile ilgili olarak ise bu oyların toplantı yeter sayısında dikkate alınacağı ancak karar alırken yeter sayısına dahil edilemeyecekleri şekilde bir düzenleme yapılmıştır. Kişisel Verileri Koruma Kurulu'nun alacağı kararlarda yapılacak en basit hesaplamayla 11 kişiden oluşan Kurul'un 3 üyesiyle bir karar verebileceği gibi bir durum ortaya çıkmaktadır. İlk etapta bu usulün değişmesi yani özellikle karar yeter sayısının yükseltilmesi gerektiği açıktır. Özellikle; çeşitli mesleki gruplardan oluşan Kurul Üyeleri'nin çoğunluğunun toplantıya katılımı karar konusu meseleye yaklaşımın doğruluğunun gerektiği gibi tartışılabilmesi, kişisel verileri koruma hukuku kapsamına giren herhangi bir konunun değerlendirilip karar alınma aşamasında Kurul Üyeleri'nin çoğunluğunun katılımı önemlidir. Diğer yandan çekimser oyun kabul edilmekte olduğunun da ayrıca tartışılması gerekmektedir. Her Üye'nin olumlu ya da olumsuz karara katılıp görüşlerini hiçbir etki altında kalmadan sunabilmesi gerekmektedir. Özellikle bireylerin temel hak ve özgürlüklerini etkileyebilecek boyutta önemli konuları görüşüp karara bağlayacağı durumlarla karşılaşacak olan Kurul'un

çoğunluğunun tam katılımıyla karar vermesi gerektiği bilincinin yerleşmesi gerekmektedir.

Kurul toplantılarının düzenlendiği maddeyi incelemeye devam ettiğimizde, Kurul Üyeleri'nin kendilerini veya temsil ettikleri kurumların taraf olduğu şikayet konularına ilişkin karara katılamayacağı düzenlenmiştir. Bu nitelikteki bir üyenin karara katılımının olamayacağının düzenlenmesi yerinde olmakla birlikte, bu konunun görüşüldüğü bir toplantıya katılımından da men edilmesi gerekir. Hatta yalnızca kendisi veya temsil ettiği kurum değil, birinci derece akrabalar gibi Kurul Üyesi'nin verdiği oyun üzerine şüphe düşürebilecek yakınlıktaki hısımlarını ilgilendiren konularda ne kararlara ne de toplantılara katılmaması gerekmektedir.

4.8.4. Kurulun Başkanının ve Kurulun Görevleri

Kurul Başkanının görev ve yetkileri, yurt içinde ve yurtdışında Kurulu temsil etmek, Kurulun toplantılarını yönetmek, Yasa ile verilen yetkilerin kullanılmasını ve görevleri gerektirdiği hizmetlerin yürütülmesini sağlamak, Kurum personelinin çalışmalarını gözetmek, denetlemek ve onların verimliliklerini artırma yönünde gerekli önlemleri almak, Kurul bütçesinin ve kesin hesaplarının hazırlanmasını ve uygulanmasını sağlamak ve Kurulun ita amirliğini yapmak, hizmet için gerekli araç, gereç ve aygıtların Kurul kararlarına uygun olarak satın alınmasını sağlamak ve Yasa ile kendisine verilen görevleri yerine getirmek ve yetkileri kullanmak şeklinde düzenlenmiştir.

Yasa'da Kurul'un görevlerine aşağıdaki şekilde yer verilmiştir:

1. Kişisel verilerin işleme tabi tutulmasına ilişkin konularda tavsiye ve önerilerde bulunmak ve bunları kendi takdirine bağlı olarak kamuoyunun dikkatine getirmek, gerekmesi halinde bu konularda tüzük taslakları

hazırlayıp Bakanlar Kurulu'nun onayına sunmak, standartları belirlemek ve bunlara ilişkin bildirim yayımlamak.

2. Kişisel veri işlenmesiyle bağlantılı olarak kişileri koruyucu kuralların uygulanmasına yönelik talimatlar vermek.

3. Bu Yasa'da öngörülen ruhsatları vermek.

4. Kişisel verilerin kontrolörler tarafından işlenmesi dolayısıyla kişilik haklarının ihlal edildiğini iddia edenlerin şikayetleri hakkında karar vermek, bunu yaparken de bu tür veri işlenmesinin yasallığını soruşturmak, denetlemek, tüm bunlarla ilgili işlemlerden başvuru sahiplerini haberdar etmek.

5. Diğer ülkelere veri aktarımı konusunda diğer ülkede yasal bakımdan eşdeğer korunmanın bulunduğu hususunda onay vermek.

6. Kendi yetkisine veya bir şikayete dayanarak herhangi bir dosyayı denetlemek. Bu bağlamda avukat ile müvekkili arasındaki mahremiyete tabi verinin dışındaki her türlü mahrem de dahil olmak üzere, kişisel verilere ulaşma ve her türlü veriyi toplama hakkına sahiptir. İstisnai olarak, ulusal güvenlik veya özellikle ciddi suçların ortaya çıkarılması gerekçesiyle tutulan dosyalarda isimleri kayıtlı olanlara ilişkin ayrıntılara erişemez. Denetleme, Kurul tarafından bu amaçla görevlendirilmiş çalışanlar tarafından yürütülür. Kurul Başkanı, ulusal güvenlik nedeniyle tutulmuş bir dosyaya bağlı bir denetlemede şahsen hazır bulunur. Denetlemeye ilişkin usul, Kurul tarafından hazırlanıp, Başbakanlıkça önerilecek ve Bakanlar Kurulunca onaylanacak bir tüzükle belirlenir.

7. Bir önceki takvim yılına ait yıllık görev raporunu hazırlamak. Söz konusu rapor, gerekli olması halinde ilgili mevzuatta yapılması gerekli değişiklik önerilerini de kapsar.

8. Bu Yasa kurallarına aykırılık taşıyan herhangi bir hususu yetkili makamların dikkatine getirmek.

9. Bu Yasa uyarınca verilen yetki ve görevlerin gerektirdiği hizmetlerin yürütülmesi için gerekli personeli bu Yasa kuralları çerçevesinde istihdam etmek.

10. Görevlerini yerine getirmesi bağlamında diğer ülkelerde kurulmuş olan muadil kurul veya kurumlarla işbirliği içinde olmak.

GDPR'da ise, sürekli çalışması öngörülen denetim makamının görev ve yetkileri geniş tutulmuş ve çok detaylı şekilde yer verilmiştir.

Denetim makamının, Direktif'in uygulanmasını gözetme; veri işleme konusundaki riskler ve kişi hakları konusunda kamu bilincini artırma; devlet, kamu kurumları, diğer kuruluşlara gerçek kişilerin verilerinin işlenmesindeki hak ve yükümlülükleri konusunda danışmanlık yapmak; şikayetleri araştırmak ve sonuca vardırmak; diğer denetim makamları ile işbirliği yapmak; işleme faaliyetleri hakkında bilinçlendirme ve tavsiyede bulunmak; işleme faaliyetlerinin Direktif'e uyumluluğunun denetlenmesi maksadıyla alınan sertifikanın değerlendirmesini yapmak ve karar vermek gibi görevleri vardır.

Denetim makamları, şikayet prosedürünü kolaylaştırmak üzere elektronik ortamda doldurulabilen şikayet başvuru formu veya başka iletişim vasıtaları ile ilgilinin şikayette bulunabilmesini sağlamalıdır. Denetim makamı, kendisine verilen bu görevi yerine getirirken, bilgiye konu kişiden, bilgi güvenliği yetkilisinden ücret talep etmemelidir. Ancak, Direktif'in 57. maddesinde de belirtildiği üzere, denetim

makamının tekrarlayan şikayet durumlarında ya da açıkça dayanıksız veya aşırı olması durumunda idari masraflar için makul bir ücret öngörülmesi hakkı bulunmaktadır.

Madde 58'e göre de denetim makamı, görevlerinin ifası için gerekli bilgilerin verilmesi için talimat vermek, gerekli tüm kişisel verilere ve bilgilere erişmek; kişisel veri denetimi şeklinde inceleme yapmak; ihlallerin bildirimlerini yapmak; Direktif'i ihlal eden kontrolör veya işlemciye yaptırım uygulamak gibi geniş yetkilere sahiptir.

Kurul Başkan ve Üyeleri'nin görev ve yetkileri açısından bakıldığında, bu düzenlemelerin mehaz 95/46/EC Sayılı Direktif doğrultusunda hazırlanmış olduğu görülmektedir. Dolayısıyla genel anlamıyla yeterli görülebilecek görev ve yetkiler öngörülmüştür ancak bazı net olmayan görevlerin, Yasa'nın yürürlük yılı göz önünde bulundurulduğunda günümüz koşullarında eksik olabilecek ve 95/46/EC Sayılı Direktif'te öngörülen bazı görevler bulunmaktadır.

Bunlardan kısaca bahsetmek gerekirse ilk olarak; "Kişisel veri işlenmesiyle bağlantılı olarak kişileri koruyucu kuralların uygulanmasına yönelik talimatlar vermek" görevinde daha spesifik yetkiler yer alması ileride yaşanabilecek bazı ihtilafların önüne geçebilir. Örneğin, bu talimatların yanında, kontrolöre ihtarda bulunma, uyarma, kişisel verilerin işlenmesi üzerinde geçici veya kalıcı yasak koyma, verileri silme direktifi verme yetkisi gibi kararların verilebilmesi de eklenmelidir.

Yasa'nın Suç ve Cezalar Bölümü'nde yer alan idari para cezalarındaki yaptırımlara yönelik olarak Kurul'un karar verme hak ve yetkisi bulunmaktadır ancak bu yetki Kurul'un görevleri arasında sayılmamıştır. Bu eksikliğin giderilmesi, Kurul'un kararlarını almasında bu yönde ileri sürülebilecek olası bir ihtilafı engelleyebilecektir.

Kurul'un bir önceki yıla ait yıllık görev raporunun hazırlanması görevi gerek Kurul'un şeffaflığı açısından gerekse GDPR'ın 59. maddesine uyum açısından gereklilik olmakla birlikte, devamında belirtilmiş olan "gerekli olması halinde ilgili mevzuatta yapılması gerekli değişiklik önerileri"nin bu rapor kapsamına girebileceği konusunda bir karmaşa olduğu görülmektedir. Zira önceki yılın görev raporu ile ileriye dönük olacak bir önerinin aynı raporda yer alması yerine bu önerinin yıllık iş planında yer alması daha doğru olacaktır. Bununla beraber Kurul'un stratejik planı görevinin de ayrıca Kurul'un görevleri arasında yer almasının günümüz Kurum faaliyetleri açısından önemli olacağı değerlendirilmektedir.

Kurul, Yasa kurallarına aykırılık taşıyan hususları yetkili makamların dikkatine getirirken, gerektiğinde yasal işlem başlatma yetkisine de sahip olması gerektiğinden hukuki işlerin yürütülmesinde Kurul'un temsil edilmesi ya da Kurul aleyhine açılabilecek bir davada Kurul'u temsil etme ve bunlar için Kurul bünyesinde görevlendirilecek ya da dış danışmanlık şeklinde avukat yetkilendirme görevinin de eklenmesinin önemli bir tamamlama olacağı değerlendirilmektedir.

Kurul'un görevleri arasında standartların belirlenmesinin ve bunlara ilişkin bildirimlerin yapılmasının yer aldığı görülmektedir. Bu standartları belirleme hususunun netleşmesi yine önemli düzeltmelerden olacaktır. Örneğin hassas veriler için kriter belirlenmesi, veri güvenliği için sağlanması gereken kriterlerin belirlenmesi gibi ilaveler yapılması daha net ve günümüz şartlarına uyumlu düzenleme olacaktır.

Kurul'un sahip olması gereken diğer bir görev ve yetkisi düzenleyici işlemleri yapma yetkisidir. Ayrıca gerek günümüz dünyasının bu alandaki gelişmelerinin yakalanabilmesi gerekse GDPR'ın 20. maddesine uyum açısından uygulama ve mevzuattaki gelişmelerin ve uluslararası gelişmelerin takip edilmesi de Kurul'un görevlerine dahil edilmesi gerekli sorumluluklardandır.

Bununla beraber, Yasa'nın 8. maddesinde "Dosyalama Sistemleri ve İşlemler Sicili"nin Başkan tarafından tutulacağı düzenlenmiştir. Bu madde gereği bu sicil üzerinde kullanılacak karar mekanizmasının Başkan'ın görevlerini düzenleyen maddede ayrıca yer verilmesi olası ihtilaf oluşumu açısından daha netlik kazandıracağı, Yasa'nın Başkan'a yüklediği görevler mahiyetinde genel bir ifadeyle, öngörülebilir görevlerin yazılmasından imtina edilmesinin anlamlı olmayacağı açıktır.

Kurul'un görevleri arasında sayılan "kişisel verilerin işleme tabi tutulmasına ilişkin konularda tavsiye ve önerilerde bulunmak" görevi aynı zamanda diğer kurum veya kuruluşlarca hazırlanacak ve kişisel verilere ilişin herhangi bir hüküm içeren mevzuat tasarıları hakkında görüş bildirme, bu kurum ve kuruluşlara gerektiğinde danışmanlık vermeyi de kapsamaktadır. Bu nedenle Kurul'un bu görevinin bu anlamda netleştirilmesi daha uygun olacaktır.

4.8.5. Kurulun Gelirleri

Kurul'un gelirleri, "Birleştirme Ruhsatı" ve "Transfer Ruhsatı" karşılığında ödenecek ücret, Genel Bütçeye konulacak ödenek, Kurul'a yapılacak her türlü yardım ve bağışlar ve diğer gelirler olarak belirlenmiştir. Bununla beraber, mali yıl bütçe yasası yürürlüğe girdiği takdirde, Cumhuriyet Meclisi'nce onaylanıp yürürlüğe girmedikçe Kurul bütçesinden harcama yapılamayacağı, yasanın yürürlüğe girmemesi halinde gireceği tarihe kadar geçmiş yıl bütçe yasasına bağlı gider cetvellerinde öngörülen ödeneklerin 1/12'sinin aylık olarak uygulanmasına ve gelirlerin tahsiline devam edilebileceği düzenlenmiştir. Ayrıca, Kurul'un bütçesinin Sayıştay denetimine bağlı olup, Kurul'un gelir ve giderleri Kurul bütçesinde gösterilir.

Yasa'ya bağlı Cetvel'in olması ve o Cetvel ile belirlenecek alt ve üst limitler olmadan Kurul'un olası bir idari yaptırım için ücret talep edemeyeceğinden, bununla ilgili bir ekleme yapılması gerekmektedir. Ücretlerin nasıl belirleneceği Kurumca hazırlanıp Başbakanlıkça Bakanlar Kurulu'nun onayına sunulacak Tüzük ile hazırlanacaktır. Kurul'un tüzükleri tamamlanıp gelir elde edilene kadar Kurul'un oluşumuyla tam zamanlı çalışmaya başlayacak olan Başkan'ın aylık ödeneğinin nasıl karşılanacağı sıkıntısı ile karşılaşılması kaçınılmazdır. Yasa'ya eklenmiş bir geçici madde ile bütçenin tahsisine değin Kurul Başkanı'nın ödeneğinin ne şekilde karşılanacağı düzenlenmemiş olduğundan, şimdilerde oluşturulan Kurul için atanan Başkan'ın, geçecek olan bu sürede ödeneğinin nasıl, hangi bütçeden karşılanacağı gibi sorunlarla karşılaşılmıştır.

Kurul'un gelirlerini düzenleyen maddeye bakıldığında, Kurul'un vereceği "Transfer Ruhsatı" ve "Birleştirme Ruhsatı" için ücret talep edileceği görülmektedir. Kişisel Verileri Koruma Kurulu'nun asli görevinin kişisel verilerin işlenmesinin mevzuata uygunluğu ve yine bu kapsamda kişilerin temel hak ve hürriyetlerini korumak olduğu gerçeği karşısında kontrolörlerin verileri yurtdışına çıkarmaları ya da verilerin tutulduğu dosyaların birleştirilmesi hususunda verilecek ruhsat için ücretten ziyade bu işlemlerin mevzuata uygunluğunun takip edilip denetlenmesi gerekmektedir. Kurul'un görevini yerine getirirken kontrolörleri ek mali külfet altına sokulmasındaki maksat anlaşılmış değildir.

Bununla birlikte, veri sahiplerinin de Kurul'a yapacakları herhangi bir başvurudan ücret talep edilmeyeceğinin de açıkça Yasa'da yer alması gerekmektedir. GDPR'ın 57. maddesi de bu yönde bir düzenleme getirerek, denetim makamlarının görevlerini ifasında veri sahipleri ve ilgili hallerde bilgi güvenliği yetkilisinden ücret alınmayacağını belirtmiştir. Ancak, bu taleplerin özellikle tekrarlanan talepler olması, taleplerin açıkça dayanaksız ve aşırı olması durumunda, denetim makamının idari masraflarına dayanan makul bir ücret talep edebilecekleri de ayrıca düzenleme altına alınmıştır. Direktif'in bu istisnai düzenlemesiyle denetim

makamlarını aşırılaşmış talepler ya da bunu alışkanlık haline getirecek vatandaşların getireceği iş yükünden de korumayı amaçladığı görülmektedir.

4.8.6. Kurul Başkanının Tam Zamanlı Çalışması ve Ödenekler

Kurul Başkanı, tam zamanlı olarak görev yapar ve görevi boyunca başka hiçbir işle iştigal edemez. Başkana Bakanlar Kurulu'nun 18A bareminin en üst basamağından az olmayacak şartıyla belirleyeceği aylık ödenir.

Bunun yanında Üyelerin, görev yaptıkları her toplantı günü için Bakanlar Kurulu'nun saptayacağı miktarda huzur hakkı ödeneceği düzenlenmiştir.

Yasa, yalnızca Kurul Başkanı'nın tam zamanlı çalışmasını ve Başkan'ın başka hiçbir işle iştigal edemeyeceğini öngörmüştür. Bunun yanında Üyeler, Yasa'da öngörülen bu kadar görev ve yükümlülüklere ve Kurul'un sürekli çalışmasını öngörmesine rağmen tam zamanlı olmadan ayda en az bir defa toplanmaları öngörülmüştür. Ayrıca Kurul Başkanı'nın aylık ödenek alacağı, Üyelerin ise görev yaptıkları her toplantı günü için Bakanlar Kurulunun saptayacağı miktarda huzur hakkı ödeneği verileceği öngörülmüştür.

Üyelerin görevlerini layıkıyla yapabilmeleri için gerekli zamanı ve eforu kullanabilmeleri için tam zamanlı çalışmaları gerekmektedir. Bununla beraber Üyelerin bağımsızlığının sağlanması için tatmin edecek aylık ödeneklerinin olması elzemdir.

Bu noktada ise Başkan'ın ve Üyelerin ödeneklerinin dayanak noktasının Bakanlar Kurulu olması durumu dikkat çekmektedir. Kurul Üyeleri'nin tam zamanlı olması durumunda Üyelerin ve Başkanın kaçıncı baremden ödeneceklerinin Yasa'da belirlenmesi gerekmektedir. Bununla birlikte Kurul Üyeleri'nin mevcut haliyle katıldıkları toplantı başına ücret alacakları durumda da, yine Bakanlar Kurulunun belirleyeceği huzur ödeneği değil, Yasa ile saptanmış bir ödenek almaları daha

uygun olacaktır. Zira sık değişen hükümete dayanarak her dönemin Bakanlar Kurulu'nun karar mekanizmasına göre değişecek bir ücret ile Kurul Üyeleri'nin aylık ücret alması doğru bulunmamaktadır. Yukarıda da belirtildiği üzere, Kurul Üyeleri'nin bağımsızlığının sağlanması için gerekli düzenlemelerin yapılması Kişisel Verileri Koruma Kurulu'nun amacı ve hedefleri bakımından önemlidir.

4.8.7. Kurul Personeli

Yasa, Başkan ve Kurul'a vermiş olduğu görev ve yetkilerin gerektirdiği hizmetleri yürümek üzere bir büro kurulmasını öngörmektedir. Büro için 10 kişiyi aşmamak kaydıyla 1 Koordinatör, 1 Hukukçu, 3 Bilgi/Belge Yöneticisi, 2 Denetleme Memuru, 1 Mali İşler Memuru, 1 Sekreter, 1 Odacı/Şoför istihdam edilecektir. Personeller, KKTC İş Yasası kuralları çerçevesinde istihdam edilecek ve sözleşmeli olacaktır.

Yasa, Kurul personelinin Kurul tarafından istihdam edileceğine ve hizmet koşullarının sözleşmede belirtileceğine yer vermiştir. Ayrıca, personele verilecek ücretlerin, Bakanlar Kurulunca saptanmış olan kademe ve derecelere göre verileceğini ve her yıl Kurul Bütçesinde de bu ödemelere yer verileceğini belirtmektedir.

Kurul'a atanması planlanan personel sayısının az olduğu ve Yasa ile daha fazla personel istihdamının engellendiği görülmektedir. Yasa'nın özellikle tam zamanlı çalışmayacak olan Kurul Üyeleri'nin atanmasını ve Başkan Yardımcısı olmamasını içerdiği göz önüne alındığında, Kurul'un işleyişini sürdürecek yeterli sayıda personelin olamayacağı gerçektir. Ayrıca Üyeler tam zamanlı çalışsa dahi, 10 kişilik personelin yeterli olmayacağı açıktır. Bununla beraber, personellerin statülerine bakıldığında, araştırma, soruşturma yapacak kişilerin Denetleme Memuru olarak atanmalarında herhangi bir koşula yer verilmemiştir. Alanında uzman kişilerin Kurul'a "uzman" statüsüyle istihdamı ve özellikle yetkin kişilerin

Denetleme Memuru olarak atanmaları gerekmektedir. Bununla birlikte, atama konusu yanında özellikle Denetleme Memuru'nun denetim yapma yetkisinin verilmesine ilişkin bir kuralın da Yasa'da yer alması gerekmektedir. Kurul personelinin hangi işi yapacağı, görevleri kimden alabileceği gibi hususların Yasa içerisinde yer alması gerekmektedir. Zira İş Yasası kuralları çerçevesinde istihdam edilecekleri dışında işlerini yürütürlerken sahip olmaları gereken yetkinin Yasa'dan gelmesi önem arz etmektedir.

Personel atamalarının Kurul tarafından yapılması kuralı yerinde olmakla birlikte, ödeneklerinin dayanağının yetersiz olduğu, hukuken bu personellerin kamu tüzel kişi personeli oldukları gerçeği karşısında görevlerinin derecelerinin, derecelere göre de ödeneklerinin alt sınırının Yasa ile belirlenmesi doğru olacaktır.

4.8.8. Sır Saklama Yükümlülüğü

Kurul Başkanı, Üyeleri ve personelinin görevleri sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları, bu konuda yasal olarak yetkili kılınan mercilerden başkasına açıklama ve kendi yararlarına kullanmaları yasaklanmıştır. Bu sır saklama yükümlülüğü, görevlerinden ayrılmalarından sonra da süresiz olarak devam eder.

GDPR'a göre denetim makamının üyeleri ve kadrosu, Birlik ve Üye Devlet hukukuna uygun olarak, görevleri sırasında ve sonrasında görevlerini ifa ederken ya da yetkilerini kullanırken öğrendikleri gizli bilgilere ilişkin sır saklama yükümlülüğüne tabidir. GDPR, madde 54'e göre bu yükümlülük, görev süresi boyunca, özellikle gerçek kişilerin Direktif'in ihlallerine dair bildirimleri için geçerlidir.

Yasa'da bireylere ait en hassas bilgilerin, bunun yanında verileri işleme tabi tutan kontrolörlerin gerektiğinde ticari sırlarını inceleyip bilgi sahibi olacak olan Kurul Başkanı, Üyeleri ve personelinin, uluslararası mevzuatlara uyumlu olarak, sır

saklama yükümlülüğü ve bu yükümlülüğü ihlal edenlerin ise Yasa'nın "Suç ve Cezalar" bölümü tahtında suç işlemiş olacakları ve mahkumiyeti halinde para cezasına çarptırılacağına dair hükmün düzenlenmiş olması olumlu görülmektedir. Zira özellikle KKTC gibi küçük bir ada ülkesinde, her halükarda dijital dünyanın bu kadar büyüdüğü bir ortamda, gerek ilgililer gerekse üçüncü kişiler hakkında elde edilen çok özel bilgilerin bir şekilde yetkisiz kişilere aktarıldığı durumlarda oluşabilecek zararın boyutu büyüktür. Bu sebeple sır saklama yükümlülüğünün ihlali halinde yaptırımın öngörülmesi yerindedir.

4.8.9. Kurul Kararlarına Karşı Yargı Yolu

Kurul'un kararlarına karşı yargı yoluna "idari para cezaları" maddesi altında yer verilerek Kurul'un bu madde altında vermiş olduğu cezalarla sınırlı tutulmuştur. Ancak Kişisel Verileri Koruma Kurulu'nun icraatlarının geniş boyutu nedeniyle verebileceği kararlardan herhangi bir kişinin etkilenmesi mümkündür. Bu nedenle, Kurul'un vermiş olduğu kararlardan etkilenen gerçek veya tüzel kişilerin bu kararlara karşı yargı yolunun açık olması ile ilgili de düzenlemenin Yasa'nın revizyonuna eklenmesi gerekmektedir.

4.9. KKTC'de Görev Yapan Diğer Kurumlar

4.9.1. Bilgi Teknolojileri ve Haberleşme Kurumu

KKTC'de 2012 yılında yürürlüğe giren 6/2012 Sayılı Elektronik Haberleşme Yasası, elektronik haberleşme sektörünün düzenlenmesi ve denetlenmesi amacıyla Bilgi Teknolojileri ve Haberleşme Kurumu'nun kurulmasını öngörmüştür. Kurul, mali ve idari özerkliğe sahip bir tüzel kişi olup işlevlerinde bağımsızdır.

Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK) Başkan ve Başkan Yardımcısı dahil olmak üzere 7 üyeden oluşan Kurul tarafından yönetilmektedir. Kurul'un 1 üyesi Cumhurbaşkanı tarafından, 3 üyesi haberleşmeden sorumlu Bakanın önerisi ile Bakanlar Kurulu tarafından, 2 üyesi Cumhuriyet Meclisinde grubu bulunan ve en fazla üyeye sahip iki siyasal parti tarafından sunulup Cumhuriyet Meclisi tarafından ve bir üyesi Kıbrıs Türk Mühendis ve Mimar Odaları Birliği, Ticaret Odası ve Sanayi Odasının birlikte belirleyecekleri ve Bakanlar Kurulu tarafından aranacak toplam 7 üyeden oluşur. Bakan Bakanlar Kuruluna 3 adayı önerirken Başkan ve Başkan Yardımcısını da belirler.

Bilgi Teknolojileri ve Haberleşme Kurul üyelerinin atanması, Kişisel Verileri Koruma Kurulu üyelerinin atanması usulüyle benzerlik göstermektedir. Ancak, oluşturulacak olan makamın Kurum olması ve Kurul tarafından yönetilmesi, Kişisel Verileri Koruma Kurulu için idealde olmasını önerdiğimiz Kurum yapısına benzerdir. Ancak, BTHK'da Başkan ve Başkan Yardımcısı dışındaki Kurul üyeleri daimi üye sayılmamaktadır. Elektronik Haberleşme Yasası'nın kapsamı KKTC'de elektronik haberleşme çerçevesinde olduğundan, Kişisel Verileri Koruma Kurulu için önerdiğimizden farklı olarak Kurul üyelerinin tam zamanlı çalışması zorunluluğu doğmayabilir.

Kurul üyeleri toplantı başına asgari ücretin 1.5 katının 1/4 oranında ödenek alır. Ancak Kurul üyelerine verilecek aylık toplam ödenek her halükarda aylık asgari ücretin 1.5 katını aşamaz.

Kurul'a atanacak üyelerde aranan nitelikler arasında üyelerin bir üniversite veya dengi bir yükseköğrenim kurumunun, bilgi teknolojileri ve haberleşme veya ilgili mühendislik, hukuk, ekonomi, ticaret, uluslararası ilişkiler veya ilgili dallarında en az lisans seviyesinde mezunu olma ve en az 5 yıllık mesleki tecrübeye sahip olma şartı yer almaktadır. Bu şart, Kurumun faaliyetlerinin yetkin üyelerle yürütmesinin beklendiğini ortaya koymaktadır. Kişisel Verileri Koruma Kurulu'na atanacak üyenin nitelikleri arasında tecrübe vasfının Yasa'da yer alması önemlidir.

Kurul üyelerinin görev süreleri 5 yıl olup her üye en fazla iki dönem görev yapabilir. Kurul üyelerinin görevlerinin sona erme koşullarına bakıldığında ise üyenin ölümü veya yazılı istifası, özürsüz ve izinsiz olarak 1 yıl içinde 3 Kurul toplantısına katılmaması, Sağlık Kurulu raporuyla görevini yapamayacağının belgelenmesi veya üyelerin atanmasında aranan şartlara aykırılık oluşması ve/veya tespit edilmesi halleri dışında üyelerin görev sürelerinin dolmadan görevlerine son verilemeyeceği yer almaktadır. Kurul üyelerinin atanmasındaki siyasi kanatın varlığı, görev sürelerinin 2 dönem olabilmesi kuralları olsa da, atayan kurum tarafından Kurul üyelerinin görevlerine son verilememesinin, üyelerin bağımsızlığını önemli ölçüde sağlayan nokta olduğu söylenebilir. Kişisel Verileri Koruma Kurulu üyelerinin atayan makam tarafından görevden alınabilmesi ile ilgili yapmış olduğumuz eleştiriler ve önerilerimiz doğrultusunda, Yasa'nın iyileştirilmesi aşamasında Elektronik Haberleşme Yasası'nın 7 (2). maddesinin direk örnek alınabileceği değerlendirilmektedir.

Bilgi Teknolojileri ve Haberleşme Kurumu'nun Hizmet Birimi, Kurulun yönetiminde, toplamda 35 kişiyi geçmeyecek şekilde 3 hukukçu, 3 sekreter, 3 katip, 2 arşiv memuru ve 2 odacı/şoför ve ihtiyaç duyulan alana göre konularında uzman 22 uzman personelden oluşmaktadır. Belirtilmiş olduğu gibi BTHK'nın Kurum yapısı Kişisel Verileri Koruma Kurulu için önermekte olduğumuz yapıya örnek oluşturabilir. Denetleme, düzenleme yetkisi anlamında kapsamı daha dar olan BTHK'nın Kurum personeli sayısı ile yetkisi daha geniş olan Kişisel Verileri Koruma Kurulu'nun Yasa ile sınırlandırılan büro personeli sayısı arasındaki fark, çalışmamızda eleştirilen Kurum yapısının yeniden gözden geçirilmesi için bir göstergedir.

4.9.2. Rekabet Kurulu

KKTC'de 2009 yılında yürürlüğe giren 36/2009 Sayılı Rekabet Yasası, etkili rekabet ortamının sağlanması ve korunması amacıyla kamu tüzel kişiliğini haiz, bağımsız ve tarafsız bir Kurul oluşturulmasını öngörmüştür.

Kurul 5 üyeden oluşmaktadır. Üyelerden biri Bakanlar Kurulu tarafından Kurul Başkanı olarak görevlendirilmekte olup bir üye de Kurul tarafından Başkan Yardımcısı olarak görevlendirilir. Kurul üyeleri, Ekonomi ve Enerji Bakanlığı, Maliye Bakanlığı, Kıbrıs Türk Barolar Birliği, Kıbrıs Türk Ticaret Odası ve Kıbrıs Türk Sanayi Odası tarafından gösterilen ikişer aday arasından Bakanlar Kurulu tarafından seçilerek atanmıştır. Her halükarda atanan üyelerden birinin hukuk, birinin ekonomi, birinin de maliye veya muhasebe dallarında lisans eğitimi almış olması zorunlu kılınmıştır. Kurul üyelerinde aranan nitelikler arasında mezun oldukları dallarda mesleki tecrübeye sahip olmak da yer almaktadır. Bu kuraldan da anlaşılacağı üzere Rekabet Kurulu'nun faaliyetlerini BTHK'da da olduğu gibi, yetkin üyelerle yürütmesi beklenmektedir.

Tam zamanlı görev yapacak olan Rekabet Kurulu üyelerinin başka bir iş yapamayacağı, resmi veya özel hiçbir görev alamayacağı, herhangi bir teşebbüste veya teşebbüs birliğinde yönetici, direktör, yönetim kurulu üyesi veya hissedar olamayacağı veya danışmanlık hizmeti veremeyeceği, siyasi partilerin kurullarında görev alamayacağı Kurul üyelerinin yasaklarını içeren 14. madde ile düzenlenmiştir. Kurul Başkan ve üyelerinin ödenekleri için Kamu Görevlileri Yasası'na atıf yapılmış, maaşlar baremlerle belirlenmektedir. Rekabet Kurulu üyelerinin tam zamanlılığı hususu, Kişisel Verileri Koruma Kurulu ile ilgili yapmış olduğumuz öneri ile benzerlik göstermektedir.

Kurul üyelerinin görev süresi 6 yıl olup en fazla 2 dönem görev yapabilmektedirler. Kurul üyeliği, üyenin ölümü veya yazılı istifası, yukarıda yer verilen 14. maddedeki kuralların herhangi birinin ihlal edildiğinin Mahkeme kararıyla kesinleşmesi, Rekabet Yasası kurallarına aykırı hareket edildiğinin Mahkeme kararıyla kesinleşmesi halinde kendiliğinden sona erer. Ayrıca Kurul üyelerinin atanmasında öngörülen niteliklerin yitirilmesi veya var olmadığının sonradan tespit edilmesi, üyenin özürsüz ve izinsiz olarak üst üste 2 veya 1 yıl içinde 5 Kurul toplantısına katılmaması ya da Kurul kararıyla verilen görev ve sorumlulukların yerine

getirilmemesi, Sağlık Kurulu raporuyla görevini yapamayacağının belgelenmesi halinde Kurulun önerisi ile Bakanlar Kurulu tarafından sona erdirilir. Belirtilen nedenler dışında üyelerin görev süreleri dolmadan görevlerine son verilemez. Kurul üyelerinin görev sürelerinin sona ermesi sebeplerine bakıldığında, özellikle üyenin bağımsızlığına önem verilmiş olduğu görülmektedir. BTHK'da da olduğu gibi Kurul üyeleri atandıkları makam tarafından görevden alınamamaktadır.

Görülebileceği üzere KKTC'de aktif olarak çalışan 2 önemli Kurul'un üyelerinin görevlerinin sona ermesine dair kuralları arasında atanan makam tarafından görevine son verilmesi imkanı tanınmamıştır ve bu özellikleri üyelerin bağımsızlığının sağlanması açısından önem teşkil etmektedir.

Rekabet Kurulu'na bağlı hizmet biriminin ayrı bir yasa ile düzenleneceği yer almaktadır. Henüz gerekli yasal çalışma tamamlanmadığından Kurul çalışmalarına Bakanlık tarafından Kurul'a görevlendirilen 2 idari personel yardımcı olmaktadır. 2011 yılından beri aktif bir şekilde faaliyetlerini yürüten Rekabet Kurulu'nun faaliyet alanı ve işleme usulü nedeniyle hizmet birimi hakkındaki yasal çalışma için ivedilik gösterilmediği, tam zamanlı çalışan üyeler ve 2 personel ile çalışmalarını yürütebildikleri görülmektedir.

4.10. Diğer Bulgular

Yasa'nın yürürlüğe girişi, Resmi Gazete'de yayımlandığı tarihtir ancak Yasa'nın hükümlerinin uygulanmaya başlaması ayrıca düzenlenmek durumundadır. Zira bir denetlemenin, ihlal durumunun ele alınması gibi hususlar ya da verilerin yurtdışına çıkarılması gibi konularda Kurul'un faaliyetlerine aktif olarak başlamış olması gerekmektedir. Hatta bu sebeple, Yasa'nın yürürlüğe girdiği yıldan beri Kurulun oluşturulmamış olmasından dolayı Yasa maddeleri uygulanmamış veya etik nedenlerle uygulansa dahi ihlal halleri yaptırımsız kalmıştır. Yasa, kontrolörlerin yani kişisel verileri işleme tabi tutan tüm Kurum veya Kuruluşların, gerçek ve tüzel

kişilerin durumlarını Kurul'un ilan edeceği tarihten itibaren altı ay içerisinde bu Yasa kurallarına uyumlu hale getirmelerini öngörmüştür. Yasa'nın yürürlüğe girdiği tarihin akabinde Kurul oluşmuş olsa bile kontrolörlerin durumlarını öngörülen kurallara uyabilecek hale getirebilmeleri mümkün olmayacaktır. Teknoloji ile hızla gelişen bilişim dünyasında her gün teknik gelişmeler yaşanmaktadır. Bu nedenle, örneğin bir firmanın veri tabanını kişisel verilerin korunması hukukuna tamamen uyumlu hale getirmesinin beklenmesi için, bu firmanın birçok teknik geliştirme yapması, bu geliştirmeler için belirli yatırımların yapılması, çalışanlarını bu konuyla ilgili bilinçlendirmek üzere eğitimler vermesi, hukuki prosedürlerin, politikaların belirlenmesi ve daha birçok çalışma yapması gerekmektedir. Tüm bunların altı ay gibi kısa bir sürede yapılmasını beklemek gerçek dışıdır. Bununla beraber Yasa'nın ardından takriben 12 yıl geçmiş olduğundan yasa içeriği çağ dışı kalmaya yüz tutmuştur. Bu haliyle kontrolörlerin durumlarını uyumlu hale bir şekilde getirdiği farz edilse dahi, kısa sürede Yasanın yenilenmesi zorunluluğu oluşacağından, kontrolörlerin tüm çalışmalarını gözden geçirmesi ve birçok geliştirmeyi, yatırımları yeniden yapmaları gerekecektir. Dolayısıyla uyum süresinin daha uzun tutulması, geliştirilmesi gereken kısımların maddeler halinde ayrıca belirtilmesi ve bu uyum beklentisinden önce Yasa'nın revizyonu gerekmektedir.

Kurul'un Başkan ve Üyeleri hakkında getirilebilecek bir şikayetin değerlendirilmesi veya bir disiplin soruşturmasının hangi Yasa'ya dayanarak yürütüleceği veya görevlerinin kötüye kullanılması gibi işlemiş oldukları suçların yargılama usullerinin Yasa'da yer almadığı görülmektedir.

Kurul Üyeleri'nin yalnızca siyasi parti organlarına üye olamamaları dışında yapabileceği ya da yapamayacağı işlerle ilgili herhangi düzenlemeye yer verilmediği görülmektedir. Özellikle tam zamanlı çalışan olarak görevlendirilmeleri gereken Üyelerin, yapabileceği işlerle ilgili düzenleme yapılması gerekmektedir. Bu konuda GDPR'ın "Denetim makamının kurulmasına ilişkin kuralları" düzenleyen 54. maddesinde devletin, kurul üyelerinin

yükümlülüklerini belirleyen şartları, görev süreleri ve sonrasında yasak faaliyetleri, meslekleri ve menfaatlerini Yasa ile belirleyeceği belirtilmiştir. Bu maddeden de görülebilir ki Direktif, üyelerin tam zamanlı görevlendirildikleri süre boyunca men edildikleri faaliyetleri ve menfaatlerinin Yasa'da yer almasını öngörmektedir. TC'nin 6698 sayılı Yasası'nın 21. maddesinin 10. fıkrasında yer alan düzenleme konuyla ilgili kapsamlı olması bakımından güzel bir örnek oluşturmaktadır. Bu maddeye göre; "*Kurul Üyeleri özel bir kanuna dayanmadıkça, Kurul'daki resmi görevlerinin yürütülmesi dışında resmi veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetlerinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak, Kurul Üyeleri, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler*" denilmektedir. Bununla birlikte Direktif'in Denetim Makamı'nın bağımsızlığını düzenleyen 52. maddesine göre "*Üyeler, görevleri ile bağdaşmayacak her türlü davranıştan uzak durur ve görevleri süresince ücret karşılığı olsun olmasın, bu nitelikte işlerde çalışmaktan kaçınır*" denilmiştir. Üyelerin görevleri esnasında bağımsız olabilmeleri Yasa koyucunun önceliklerinden olmalıdır. Bu nedenle tüm bu maddelerden ve çalışmamızda belirtilen sebeplerle, Kurul Üyeleri'nin başka işle iştigal etmemeleri, dolayısıyla da tam zamanlı görev almaları gerekmektedir.

Yine Üyelerin tam zamanlı olması gerekliliği ile birlikte düzenlenme ihtiyacı duyulacak diğer bir madde ise Kurul Başkanı için düzenlenmiş olduğu gibi üyelerin de önceki görevleri ile ilgili kurallardır. Kurul Üyesi kamudan atandığı takdirde, üyeliğinde geçirilecek sürenin emeklilik süresinden sayılması, görevi sona erdiğinde kamudaki görevine devam etmesi, barem içi artışındaki düzenlemeler gibi konuların Yasa'da yer alması gerekmektedir.

SONUÇ

Bu çalışmamızın ilk bölümünde kişisel verilerin korunmasının önemine değindik. Özellikle elektronik ortamda verilerin sürekli paylaşılmakta olduğu, akıllı telefon, sosyal medya kullanımlarının artmasından dolayı verilerin üçüncü kişiler tarafından kolaylıkla elde edilebildiği, bu verilerle ticari fayda sağlanmakta olduğu konularına dikkat çektik.

Sonraki bölümlerde Kuzey Kıbrıs Türk Cumhuriyeti'nin hukuk sistemini inceledik ve 2007 yılında yürürlüğe giren Kişisel Verilerin Korunması Yasası'nı derinlemesine ele alarak Avrupa Birliği'nin bu konuda rehber edindiği GDPR ile mukayesesini yaptık.

Netice itibarıyla çalışmamızdan şu sonucu çıkarmış bulunmaktayız;
KKTC, yasal açıdan çağdaş normlara uygun bir takım düzenlemeler yaparken, çıkarılan yasaların uygulamaya konulmasında bürokrasinin hantallığı sebebi ile çok da aktif davranamamaktadır. 89/2007 sayılı Kişisel Verilerin Korunması ile ilgili Yasa'nın Meclisten geçmesinin üzerinden 12 yıl gibi bir zaman geçmesine rağmen yasada geçen "Kişisel Verileri Koruma Kurulu" yeni oluşturulmuştur. Bu sebeple Yasa'da öngörülen tüzükler çıkarılamamış ve çalışma esasları belirlenememiştir. Dolayısıyla ilgili Yasa tam anlamıyla uygulama sahası bulamamaktadır.

Gerek gelişen teknolojiler dolayısıyla kişisel verilerin her alanda işlem görüyor olması, gerekse uluslararası veri akışının kolaylıkla yapılabilecek durumda olması, tüm devletlerin veri korunmasına ilişkin mevzuatlarını gözden geçirmesine neden olmuştur. Bu bağlamda yukarıda detayı verilen veri korumaya ilişkin düzenlenen Tüzükler güncel ihtiyaçlara göre sürekli değişime uğramakta, iç hukuklar ise bu değişime ayak uydurmaya çalışmaktadır. KKTC'nin en yakını Türkiye ve Güney Kıbrıs da bu ülkelerdendir. Hal böyleyken 89/2007 Sayılı Yasa'nın çağdaş dünyaya

ve özellikle de AB'de yürürlükten kaldırılan 95/46/EC Sayılı Direktif'in yerine uygulamaya konulan GDPR'a uyumlu hale getirilmesi şarttır.

KAYNAKÇA

Kitap ve Makaleler

Arıklı, E. (2011) Günümüzdeki Türk Halkları ve Tarihleri, Ankara: Nüans Kitabevi

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

Başalp, N. (2015) Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, *Mühf-Had*, 21(1), 77-105

Başalp, N. (2004) *Kişisel Verilerin Korunması ve Saklanması*, Ankara, Yetkin Yayınları.

Berber, L. K., vd. (2009) *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*, İstanbul, Karakter Color AŞ.

Beytar, E. (2017) *İşçinin Kişiliğini ve Kişisel Verilerinin Korunması*, İstanbul, On İki Levha Yayıncılık.

Çalık, T. (2015) Birleşmiş Milletler Organlarının İnsan Hakları ile İlişkisi, *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 2, 1091-1134

Çekin, M. S. (2018) *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, On iki Levha Yayıncılık, İstanbul

Develioğlu, H, M. (2017) 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul

Doğu, A. H. (2016) *Bilişim Hukuku*, Ekin Yayınevi, Bursa

Dutertre, G. (2003). *Avrupa İnsan Hakları Kararlarından Örnekler*, Avrupa Konseyi Yayınları, Ankara

Ekinci, B. E. (2016) Kuzey Kıbrıs Türk Cumhuriyeti Yüksek Mahkemesi Kararlarında Hukuk Devleti İlkesi, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 65(3), 723-770

Giakoumopoulos, C., vd. (2018) *Handbook on European Data Protection Law*, Luxembourg, Publications Office of the European Union.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği*, 27(3), 451-471.

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

Korff, D. (2002) EC Study on Implementation of a Data Protection Directive: Comperative Summary of National Laws, Londra, Human Rights Centre University of Essex

Korkmaz, İ. (2016) Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, *TBB Dergisi*, 81-152

Necatigil, Z. (1988) *Kuzey Kıbrıs Türk Cumhuriyetinde Anayasa ve Yönetim Hukuku*, İstanbul, Çavuşoğlu Basım ve Yayım A.S.

Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum. *Uyuşmazlık Mahkemesi Dergisi*, 0 (3), 1-38

Öztürk, B., Altınok, Ç, E. (2018) Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu, *Fasikül Hukuk Dergisi*, 10(100),

Pazarcı, H. (2018) *Uluslararası Hukuk*, 17. Baskı, Turhan Kitabevi, Ankara

Rıdvan, K. (2014) *Küreselleşen Dünyada Uluslararası Kuruluşlar*, İstanbul, Beta Basım Yayım.

Şimşek, O. (2008) *Anayasa Hukukunda Kişisel Verilerin Korunması*, İstanbul, Beta Basım

Tataroğlu, M. (2013) Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED), *Yönetim ve Ekonomi*, 20(1), s.263-289

Tekin, N. (2014). Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirmesi. *Uyuşmazlık Mahkemesi Dergisi*, 0 (4), 222-262

Turhan, T. (2008) Tarihsel Bakış Açısıyla Kıbrıs Türk Hukuk Sistemi, *Ankara Üniversitesi Hukuk Fakültesi Dergis*i, 57(2), 254-286

Uygun, M. (2010) Avrupa Birliği'nin 95/46 sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, TC. Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Ankara.

Raporlar

Akıncı, A. N. (2017) Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, T.C. Kalkınma

Bakanlığı İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, Yayın No: 2968, Çalışma Raporu No: 6

Ceran, A. (2014) IKV Değerlendirme Notu: Kişisel Verilerin Korunması: Avrupa ve Türkiye, İktisadi Kalkınma Vakfı, Rapor No: 104, s. 6

Devlet Planlama Teşkilatı (2000), Sekizinci Beş Yıllık Kalkınma Planı: Türkiye'nin Dış Ekonomik İlişkileri Özel İhtisas Raporu.

Akademik Tezler

Akgül, A. (2013) Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu Ve Yargısal Denetimi, Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, İzmit

Aksoy, H. C. (2008) Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara.

Aras, Ü. Y. (2010) İnsan Hakları Temelinde Özel Hayat Hakkinin Ulusal ve Uluslararası Alanda Uygulamaları, Yüksek Lisans Tezi, T.C. Bahçesehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yüksek Lisans Programı, İstanbul

Aydın, S. E. (2014) AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Sucu, Yüksek Lisans Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul.

Ayözger, A. C. (2016) Elektronik haberleşme Sektöründe Kişisel Verilerin Korunması, Doktora Tezi, T.C. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, İstanbul.

Boz, A. (2014) Kişisel Verilerin Korunması: Türkiye, ABD ve AB örnekleri, Yüksek Lisans Tezi, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Ankara.

Bük, A. (2015) Elektronik Ortamda Saklanan Kişisel Verilerin Elde Edilmesi / Değiştirilmesi Suretiyle İşlenen Suçların Ceza Hukuku Açısından Değerlendirilmesi, Doktora Tezi, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, Ankara.

Civelek, D. Y. (2011) Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, Uzmanlık Tezi, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Dinkci, F. (2014) Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye Örneği, Ondokuz Mayıs Üniversitesi, Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Samsun.

Güldüren, C. (2015) Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi, Doktora Tezi, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Ankara.

Hayrunnisa, Ö. (2009) Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Doktora Tezi, T.C Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara

Henkoğlu, T. (2015) Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler için Bilgi Güvenliği Politikasının Geliştirilmesi, Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, Ankara.

Gözüküçük, M. (2014) Veri İsleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı, İstanbul.

Küzeci, E. (2010) Kişisel Verilerin Korunması, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Genel Kamu Hukuku) Anabilim Dalı, Ankara.

Elektronik Kaynaklar

Avrupa Birliği Türkiye Delegasyonu (2019) Avrupa Birliği Temel Haklar Bildirgesi: <https://www.avrupa.info.tr/tr/avrupa-birligi-temel-haklar-bildirgesi-708>

Avrupa Birliği Türkiye Delegasyonu (2019) Katılım Müzakereleri: <https://www.avrupa.info.tr/tr/katilim-muzakereleri-720>

Birleşmiş Milletler, Birleşmiş Milletler Türkiye'nin refahı için Türkiye ile birlikte çalışıyor:
<http://www.un.org.tr/bm-turkiye-kuruluslari/>

Council of Europe (2018)- Details of Treaty No.223;
<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223>

Erginel, T. (2018) KKTC Yargısı, www.tanererginel.com: <http://www.tanererginel.com/>

European Commision (2019) Adequacy Decisions: How the EU determines if a non-EU country has an adequate level of data protection: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>

European Commision (2018) EU-US Privacy Shield: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-data-transfers_en>

Kişisel Verileri Koruma Kurumu (2018) Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler: <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler>

KKTC Cumhuriyet Meclisi (2018) Hükümetler: <http://www.cm.gov.nc.tr/Bilgi/H%DCK%DCMETLER.pdf>

Organisation for Economic Co-operation (2008) Closing Remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy: <Http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinterneteconomy.htm>

T.C Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü (2015) 31853594-101-30-3870 Sayılı Kanun Tasarısı: <https://www2.tbmm.gov.tr/d26/1/1-0320.pdf>

T.C Dışişleri Bakanlığı (2011) Avrupa Konseyi:

<http://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa>

T.C Dışişleri Bakanlığı (2011) Kıbrıs Meselesinin Tarihçesi, BM Müzakerelerinin Başlangıcı:
<http://www.mfa.gov.tr/kibris-meselesinin-tarihcesi_-bm-muzakerelerininbaslangici.tr.mfa>

Türk Dil Kurumu, Güncel Türkçe Sözlük:
<http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c55a657c7f7a7.51989574> son erişim 05.04.2019

Türkiye Ekonomi Politikaları Araştırma Vakfı (2010) KKTC'de Yasa Hazırlama ve Yasa
Yapma Süreci Kurumsal ve Fonksiyonel Analizi:
<https://www.tepav.org.tr/upload/files/14550067272.KKTC_Enerji_Sektorunun_Kurumsal_ve_Fonksiyonel_Analizi.pdf>