KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASINDA BAĞLAYICI ŞİRKET KURALLARI

Melisa TELSAÇ

EYLÜL 2022

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASINDA BAĞLAYICI ŞİRKET KURALLARI

BAHÇEŞEHİR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÜKSEK LİSANS TEZİ

MELİSA TELSAÇ

SERMAYE PİYASALARI VE TİCARET HUKUKU YÜKSEK LİSANS DERECESİ İÇİN GEREKLİ ÇALIŞMALAR YERİNE GETİRİLMİŞTİR

EYLÜL 2022

BAHÇEŞEHİR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ONAY FORMU

Program Adı:	Sermaye Piyasaları ve Ticaret Hukuku
Öğrencinin Adı Soyadı:	Melisa Telsaç
Tezin Adı:	Kişisel Verilerin Yurt Dışına Aktarılmasında Bağlayıcı Şirket Kuralları
Tez Savunma Tarihi:	15.09.2022

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Lisansüstü Eğitim Enstitüsü tarafından onaylanmıştır.

Prof. Dr. Fatma ÖZKUL

Enstitü Müdürü

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

	Ünvanı, Adı Soyadı	**İmza**
Tez Danışmanı:	Dr. Ayşe Çiğdem Ayözger Öngün	
2. Üye :	Doç. Dr. Zafer Kahraman	
3. Üye :	Dr. Çiçek Ersoy Kekevi	

Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim.

Ad, Soyad :

İmza :

ÖZET

KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASINDA BAĞLAYICI ŞİRKET KURALLARI

Melisa TELSAÇ
Sermaye Piyasaları ve Ticaret Hukuku Yüksek Lisans Programı
Tez Danışmanı: Dr. Ayşe Çiğdem Ayözger ÖNGÜN

Eylül 2022, 141 sayfa

Kişisel veriler, kişilerin özel hayatlarının gizliliği kapsamında korunmakla birlikte, teknolojik gelişmeler sonucu büyük çapta olabilen bu verilere ekonomik değer biçildiği ve küresel şirketlerin bundan fayda sağladığı görülmektedir. Özellikle bu durum, kişisel verilerin bir şirketten başka bir gerçek veya tüzel kişiye aktarımına ilişkin kurallar getirilmesini zorunlu kılmıştır. Ancak şirketlerin ve özellikle grup şirketlerin birbirlerine kişisel verileri aktarırken her seferinde veri koruma otoritesinden izin almaları sorun oluşturduğundan, ilk olarak Avrupa Birliği hukukunda, bu izin alma süreçlerini bertaraf eden ve veri aktarımına alternatif kurallar getiren bağlayıcı şirket kuralları kabul edilmiştir.

Bağlayıcı şirket kuralları taahhüdünü veren grup şirketler ya da ekonomik anlamda iş birliğine sahip girişimler, değişik ülkelerde bulunan üyeleri arasında serbest veri akışı temin edebilmektedirler. Bu kurallar, işletmelerin hesap verebilirliği ve şeffaflığını desteklerken, kişilerin özel hayatlarının gizliliğini korumayı da taahhüt etmektedir. Bağlayıcı şirket kuralları aracılığıyla grup şirketin değişik ülkelerde bulunan bütün üyeleri aynı veri koruma kurallarını kabul etmekte ve uygulamaktadırlar. Bu nedenle bağlayıcı şirket kurallarına sahip olan şirketler, Türkiye bakımından da önem arz etmektedir. Bir grup şirketin Türkiye'de bulunan üyesi, kendisine iletilen bağlayıcı şirket kurallarını taahhüt edecektir.

Çalışmada Avrupa Birliği (AB) Genel Veri Koruma Regülasyonu'nda (Regülasyon-GDPR) düzenlenen bağlayıcı şirket kurallarının temel ilkeleri incelenmiş ve Regülasyon'un AB dışına veri aktarımları için öngördüğü yöntemler ele alınmıştır. Türk hukukunda Kişisel Verilerin Korunması Kanunu'nda bağlayıcı şirket kurallarına ilişkin hüküm bulunmasa da, Kişisel Verileri Koruma Kurumu'nun (Kurum) 10.04.2020 tarihli duyurusu ile Türk yasaları kapsamında bağlayıcı şirket kuralları çalışmada incelenmiştir. Ayrıca Avrupa Birliği Komisyonu Çalışma Grupları, Avrupa Adalet Divanı (AAD) ve Kişisel Verileri Koruma Kurulu'nun (Kurul) kararları da değerlendirilmiştir.

Anahtar Kelimeler: Bağlayıcı Şirket Kuralları, Yurtdışı Veri Aktarımı, Veri Koruması, Hesap Verebilirlik.

ABSTRACT

BİNDİNG CORPORATE RULES İN CROSS BORDER DATA TRANSFER

Telsaç, Melisa
Capital Markets and Commercial Law Master's Program
Supervisor: Dr. Ayşe Çiğdem Ayözger ÖNGÜN

September 2021, 141 pages

Although personal data is protected within the scope of the privacy of individuals' private lives, it is seen that this data, which can be on a large scale as a result of technological developments, is valued economically and global companies benefit from it. This situation necessitated the introduction of rules regarding the transfer of personal data from one company to another natural or legal person. However, since it poses a problem for companies and especially group companies to obtain permission from the data protection authority every time they transfer personal data to each other, first of all, binding company rules have been adopted in European Union law, which eliminates these permission processes and sets rules for data transfer.

Group companies or undertakings in economic cooperation that issue and undertake binding corporate rules can provide free data flow among their members located in different countries. The binding corporate rules are committed to protecting the privacy of individuals, while increasing transparency and accountability of companies. Through binding corporate rules, all members of the group company in different countries accept and apply the same data protection rules. For this reason, companies having the binding corporate rules are also important for Turkey. A member of a group company in Turkey will commit to the binding corporate rules communicated to him.

In the study, the basic principles of the binding corporate rules regulated in the EU General Data Protection Regulation were examined and the methods stipulated by the Regulation for data transfers outside the European Union were discussed. Although there is no provision regarding the binding company rules in the Personal Data Protection Law in Turkish law, the binding corporate rules regulated within the framework of Turkish laws with the announcement of the Personal Data Protection Authority on 10.04.2020 are evaluated in the study. In addition, the decisions of the European Union Commission Working Groups, the European Court of Justice and the Personal Data Protection Board were also examined.

Key Words: Binding Corporate Rules, Data Transfer to Third Parties, Data Protection, Accountability.

TEŞEKKÜR

Bu tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın Dr. Ayşe Çiğdem Ayözger Öngün'e sonsuz teşekkürlerimi sunarım.

Sevgili aileme manevi hiçbir yardımı esirgemeden yanımda oldukları için tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR

AAD : Avrupa Adalet Divanı

AB : Avrupa Birliği

ABA : Avrupa Birliği Antlaşması

ABAD : Avrupa Birliği Adalet Divanı

ABTHB : Avrupa Birliği Temel Haklar Bildirgesi

AEA : Avrupa Ekonomik Alanı

APEC : Asya-Pasifik Ekonomik İş Birliği

ASTB : Avrupa Serbest Ticaret Birliği

BCR : Bağlayıcı Şirket Kuralları (Binding Corporate Rules)

Bkz. : Bakınız

BM : Birleşmiş Milletler

C. : Cilt

BŞK : Bağlayıcı Şirket Kuralları

DYYK : 4875 sayılı Doğrudan Yabancı Yatırımlar Kanunu

DİREKTİF : 95/46/EC sayılı Avrupa Parlamentosu Direktifi

E. : Esas

EC : European Comission

E.T. : Erişim tarihi

ETK : 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

FSEK : Fikir Ve Sanat Eserleri Kanunu

GDPR : General Data Protection Regulation (Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımında Gerçek Kişilerin Korunmasına Dair Avrupa Birliği Genel Veri Koruma Regülasyonu)

GVKR : 2016/679 sayılı Avrupa Parlamentosu Genel Veri Koruma Regülasyonu

İK : 4857 sayılı İş Kanunu

İÜHFM :İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

K. : Karar

Kurul : Kişisel Verilerin Korunması Kurulu

Kurum : Kişisel Verilerin Korunması Kurumu

KVKK **:** 6698 sayılı Kişisel Verilerin Korunması Kanunu

Md-m. **:** Madde

OECD **:** Ekonomik İşbirliği ve Kalkınma Örgütü/Organisation for Economic Co-Operation and Development

RG **:** Resmi Gazete

s. **:** sayfa

S. **:** Sayı

TBK **:** 6098 sayılı Türk Borçlar Kanunu

TBMM **:** Türkiye Büyük Millet Meclisi

TCK **:** 5237 sayılı Türk Ceza Kanunu

TMK **:** 4721 sayılı Türk Medeni Kanunu

TTK **:** 6102 sayılı Türk Ticaret Kanunu

vd. **:** ve devamı

VERBİS **:** Veri Sorumluları Sicili için Geliştirilen Veri Sorumluları Sicil Bilgi Sistemi

WP **:** Avrupa Komisyonu Çalışma Grubu (Working Party)

GİRİŞ

Kişisel verilerin korunması kavramı, özel hayatın gizliliği hakkı çerçevesinde düzenlenmiş olup, kişisel veri kavramının tarihsel gelişimi de özel hayatın gizliliği hakkıyla birlikte ele alınmıştır. Kişisel verilerin korunmasının temelini oluşturan sır saklama yükümlülüğü, tarihte yaklaşık iki bin beş yüz yıl önce Hipokrat yemini kapsamında ortaya çıkmıştır. Doktor ve hasta arasında oluşan gizlilik ilişkisi başka meslek grupları için de kabul edilmiş olup, taraflar arasında sır saklama yükümlülüğü ve dolayısıyla kişisel verilerin korunması kavramı; avukatın sır saklama yükümlülüğü, banka sırrı ve meslek sırrı çerçevesinde uygulanmaya başlanmıştır[1].

Dünyada 1960'lı yıllarda gelişmeye başlayan bilgi teknolojileri ve kişilerin verilerinin toplanarak otomatik olarak işlenmesi ve aktarımı olanağı, kişisel verilerin korunması kavramının temellerini atmıştır. Bu süreçte ele geçirilmesi ve aktarılması kolaylaştığından kişisel verilerin korunmasına dair gereksinim gün geçtikçe artmıştır[2]. Devletlerin farklı yetki ve görevleri sonucu elde ettiği verilerle, toplumu oluşturan bireyler karşısında çok fazla güçlendiğinin fark edilmesi, devletlerin bu verilere ilişkin yaptıklarının denetlenmesi ihtiyacını doğurmaya başlamıştır[3]. Bilgisayar sistemlerinin gelişimiyle beraber kişisel verilerin bilgisayarlar aracılığıyla toplanması, işlenmesi, raporlanması ve aktarımı işlemlerinin yaygın hale gelmesiyle 1970'li yıllarda kişisel veriler, yasal düzenlemelerle korunmaya çalışılmıştır[4].

İlk veri koruma kanununun 1970 yılında Almanya'da çıkarıldığı görülmüş olup bu hususta ilk ilke kanun da 1973 yılında İsveç'te yayımlanmıştır[5]. 1974 yılında ABD'de özel alanların korunmasına dair bir yasa yürürlüğe konulmuştur. Daha sonra 1977'de Kanada ve 1978'de Fransa'da Elektronik Veri İşlenmesi Veriler ve Özgürlük Haklarına Dair Kanun ile kişisel verilerin korunmasına ilişkin çeşitli yasal düzenlemeler gerçekleştirilmiştir.

---

[1]Akgül, Aydın, Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Kocaeli Üniversitesi Doktora Tezi, Kocaeli, 2013, s.109.

[2] Yılmaz, Sabire Sanem, Kişisel Verilerin Korunması Regülasyonu ve Unutulma Hakkı, Terazi Hukuk Dergisi, Cilt:13, Sayı: 142, Haziran 2018, s.116-121.

[3] Mendos Kuşkonmaz, Elif, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, İstanbul Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2013, s.33.

[4] Yılmaz, S., s.116-121.

[5] Turan, Metin, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, Güncellenmiş 2. Baskı, Seçkin Yayıncılık, Ankara, 2019, s. 26-27.

Uluslararası kuruluşlara bakıldığında; Avrupa Konseyi, Avrupa Birliği, Birleşmiş Milletler (BM) gibi kuruluşlar; rehber ilkeler ve hukuki metinler yürürlüğe koymaya başlamıştır. Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından 1980'de yayınlanan *"Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler"* belgesiyle kişisel veriler, ayrı bir hak şeklinde düzenlenmişti. Fakat bu ilkelerin hukuki bir bağlayıcılığı bulunmamaktaydı. OECD Rehber İlkeleri veri koruma kanunu bulunan ülkeler açısından kanunlarına bu ilkeleriyerleştirmeleri için, veri koruma kanunu bulunmayan ülkeler açısından ise temel oluşturması amacıyla yayımlanmıştır[6]. Kişisel verileri koruyan en önemli uluslararası düzenleme Avrupa Konseyi'nin 28 Ocak 1981 tarih ve 108 sayılı *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Gerçek Kişilerin Korunmasına Dair Sözleşme"* olmuştur. Sözleşmeyi imzalayan devletlere, bu sözleşme hükümlerini iç hukuklarına aktarma yükümlülüğü getirilmiştir. Bu Sözleşme, ülkelerin kişisel verilerin korunmasına dair hazırladıkları yasal düzenlemelerinin temelini meydana getirmiştir. Sözleşme, Türkiye tarafından 18 Şubat 2016 tarihinde[7] yürürlüğe girmiştir.

Avrupa Birliği'nin de kişisel verilerin korunması alanına yönelik önemli düzenlemeleri olmuştur. AB, 24 Ekim 1995 tarihinde *"Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Verilerin Serbest Dolaşımı Yönergesi"ni*, 15 Aralık 1997 tarihinde*"Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi*"ni ve 12 Temmuz 2002 tarihinde ise *"Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Yönergesi"*ni kabul etmiştir. Son olarak, 14 Nisan 2016 tarihinde 2016/679 sayılı "Kişisel Verilerin İşlenmesi ve Verilerin Serbest Dolaşımında Gerçek Kişilerin Korunmasına Dair Avrupa Birliği Genel Veri Koruma Regülasyonu" (Regülasyon-GDPR) kabul edilmiştir. Regülasyon AB'de kişisel veriler alanında geçerli tek bir metin olacaktır. GDPR'ın (General Data Protection Regulation) hazırlanmasında, kişilerin veri koruma haklarının geliştirilmesi ve veri aktarımında AB üyeleri arasındaki düzenleme farklılıkların ortadan kaldırılması hedeflenmiştir. GDPR, AB üyeleri arasındaki kişisel veri akışının yanı sıra, AB sınırları dışına gerçekleştirilecek veri aktarımlarının tabi olduğu koşulları da düzenlenmektedir. Regülasyon m.94/2 gereğince, Direktif

[6]Aksoy, Hüseyin Can, Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara, Çakmak Yayınevi, 2010, s.4.
[7] RG Tarih: 18.02.2016, Sayı: 29628.

çerçevesinde kurulan 29. Madde Çalışma Grubu'nun (WP) yerini Avrupa Veri Koruma Otoritesi almıştır. Regülasyon ile, kişilerin temel hak ve özgürlükleri ile veriler üstünde denetim imkanı sağlanırken teknolojik, sosyal ve ekonomik değişikliklerle bir orta yol bulunmaya çalışılmıştır.[8]

Türk Hukukuna kişisel verilerin korunması kavramı, ilk kez 2010 yılında 5981 sayılı yasayla gerçekleştirilen Anayasa değişikliğiyle Anayasa'nın 20/3. maddesine girmiştir. Daha sonra kişisel verilerin korunması amacıyla yürürlüğe giren ilk kanun, AB düzenlemeleri göz önüne alınarak meydana getirilmiş olan 6698 sayılı '*Kişisel Verilerin Korunması Kanunu*'dur (KVKK). Bununla birlikte, kişisel veriler konusunda Türk hukukunda yapılan ilk düzenleme ise 2012 tarihli '*Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik*'tir[9]. KVKK Tasarısı, 24 Mart 2016'da TBMM'de kanunlaştırılmış ve 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir[10]. 6698 sayılı Kanun ile beraber kanunun uygulanmasını denetleyecek olan Kişisel Verileri Koruma Kurulu da bazı yönetmelikler yayınlamıştır.

Teknolojik gelişmeler ve dijitalleşme beraberinde pek çok yarar getirmiş ve bu teknolojiler ile kişisel verilerin iletimi çok kolay hale gelmiştir. Bu durum, kişisel verilerin aktarımından meydana gelen bir ekonomi de oluşturmuştur. Artık kişisel verilerinde ekonomik bir değeri bulunmakta ve büyük küresel işletmeler bundan yarar sağlamaktadır. Veri alışverişinin işlerliği sağlanırken, kişisel verilerin dayandığı temel hak ve özgürlükler de küresel ölçekte korunmalıdır. Tam da bu nedenle, kanaatimizce veri koruma hukukunun aslında ulusal olamayacak global olmayı gerekli kılan bir hukuk dalı olduğu açıktır.

Günümüzde gerçekleşen büyük ve hızlı veri akışı, ekonomik gelişim ve toplumsal ilerleme bakımından yararlar sağlasa da, bu gelişmeler, kişisel verilerin korunması ve kişilerin mahremiyetine dair endişeler de oluşturmuştur. 1970'li

[8] Yeditepe Üniversitesi, Avrupa Ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Uluslararası Sempozyumu Bildiri Özeti;
bkz. https://law.yeditepe.edu.tr/sites/default/files/kvkk_-_kitapcik-v3.pdf, E.T:15.09.2021.
[9] Han, Işık Aslı, Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt:18, Sayı:1, Ocak 2019, s.421.
[10] Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, KVKK Yayınları, Ankara, 1. Baskı, 2018, s.8.

yıllardan itibaren oluşan endişelere dair kişisel verilerin korunması için yürürlüğe konulan ilk uluslararası düzenleme, 108 sayılı Avrupa Konseyi Sözleşmesi olmuştur.

Avrupa Birliği hukukuna bakıldığında 7 Aralık 2000 tarihinde imzaya açılan '*Avrupa Birliği Temel Haklar Bildirgesi*' (ABTHB) ile kişisel verilerin korunması, AB'de temel hak şeklinde kabul edilmiştir. Ayrıca kişisel veriler ve kişilerin mahremiyeti, hem mülga 95/46 sayılı Avrupa Parlamentosu Direktifi (Direktif), hem de 2016/679 sayılı Genel Veri Koruma Regülasyonu (Regülasyon-GDPR-GVKR) ile korunmuştur.

Veri ekonomisi, uluslararası ticaretin hız kazanması ve kişisel verilerin uluslararası aktarımlarının çoğalması ile birlikte 2016 yılında yürürlüğe giren Regülasyon, tüzel kişilerin ilgili kişilerin kişilik haklarına saygı duymasının sağlanması ile zarar görenler açısından işlerliği olan hukuki çözüm ve tazminat sistemi getirmiştir. Regülasyon ile birlikte, kişisel verilere ilişkin şirketlerin hesap verebilirliğinin bir yükümlülük şeklinde getirilmesi, kişisel verilerin ve kişilerin mahremiyetinin korunmasını temin eden önemli ilkeler arasında olmuştur. Hesap verebilirlik, yürürlükteki veri koruma mevzuatının yasa ve kurallarının şirket tarafından uygulanması ve bunların uygulandığının her zaman için kanıtlanabilir olması anlamına gelmektedir. Bu kapsamda hesap verebilirliği sağlamak adına Regülasyon'da idari ve teknik tedbirler, risk analizleri gibi birçok yükümlülük getirilmiştir. Bağlayıcı şirket kuralları, şirketlerin alacağı bu idari ve teknik tedbirleri açık şekilde düzenlemekte, taahhüt etmekte ve bu çerçevede şirketin hesap verebilirliği de artmaktadır.

Bağlayıcı şirket kurallarının getirilme amacı, bu kuralları düzenleyip taahhüt eden küresel grup şirket içinde serbest şekilde veri aktarımının yapılmasıdır. Bu nedenle, bağlayıcı şirket kuralları, Regülasyon içinde üçüncü ülkelere veri transferi amacıyla getirilen uygun güvenlik tedbirleri kapsamında yer almaktadır. Ayrıca, bağlayıcı şirket kuralları, veri koruma hukuku açısından uyumun temelini meydana getirebilecek yükümlülüklerin icra edilmesini ve kanıtlanmasını sağlayabilecektir.

Kişisel verilerin işlenmesi faaliyetleri, ülkemizin ve hatta kıtaların sınırlarını aşmaktadır. Bu kapsamda çok uluslu bir grup şirketin vereceği benzeri bir taahhüdün, Türk veri koruma hukukuna temin edebileceği faydaların da bulunduğu görülmüş ve Kurum'un 10.04.2020 tarihli duyurusunda, Türkiye'de mukim veri sorumluları

tarafından bağlayıcı şirket kuralları hazırlanabileceği belirtilmiştir. Kurum, kendi duyurusunda çok uluslu şirketlerin kendi aralarında gerçekleştirecekleri veri aktarımları bakımından yurt dışına veri aktarım yollarının uygulamada yetersiz kalabildiğini kabul ederek, aslında bu kuralları bir aktarım seçeneği olarak sunmuştur. İlk olarak Regülasyon'da düzenlenmiş olan bağlayıcı şirket kuralları, 6698 sayılı KVKK uyarınca Kurum'ca meydana getirilen alternatif uygun güvenlik tedbiri anlamına gelmektedir.

Çalışmamızın ilk bölümünde kişisel veri kavramı, bu verilerin işlenmesine dair ilkeler, kişisel verilerin aktarımı, yurt içinde ve yurt dışına aktarım ve yeterli korumanın bulunması kavramları incelenmiştir.

Çalışmamızın ikinci bölümünde ise, Türk hukukunda kişisel verilerin yurt dışına aktarılması kriterleri yer almıştır. KVKK m.3'e göre ilgili kişinin aydınlatmaya dayanan (m.10), belli bir konuda ve özgür iradeyle açıkladığı açık rızası ile yurt dışına veri aktarılması olanaklıdır. Açık rıza, sözlü veya yazılı olarak verilebilir ve istisnalar haricinde (KVKK m.5/2-d) ilgili kişi açık rıza beyanını istediği zaman geri alabilecektir. KVKK m.9 gereğince yeterli korumanın var olduğu ülkelere kişisel veri aktarımında, transfer edilecek kişisel verinin özelliğine göre yani özel nitelikli veri olup olmamasına göre KVKK'nın m.5/2 veya m.6/3'da yer alan işleme koşullarının bulunması gerekmektedir. Öte yandan, KVKK m.9/2-b ve 12/2 gereğince Türkiye'de yerleşik olan veri sorumlusunca yeterli veri koruması olmayan ülkelere veri aktarımı için hazırlanacak sözleşmelerde asgari olarak, veri aktarımı yapan veri sorumlusunun yükümlülükleri, veri alıcısı veya işleyenin yükümlülükleri ve ortak hükümlerin yer alması zorunludur. Anılan hükümler kapsamında veri aktarımı, veri sorumlularından veri sorumlularına veya veri sorumlularından veri işleyenlere yapılabilmektedir. KVKK'da açık şekilde düzenlenmese de yabancı ülkelere veri aktarımında kullanılabilecek diğer bir düzenleme, bağlayıcı şirket kurallarıdır.

Çalışmamızın üçüncü bölümünde Türk hukukunda bağlayıcı şirket kuralları ele alınmıştır. Bağlayıcı şirket kuralları, KVKK dahil Türk Hukukunda yasal bir düzenlemede yer almamış ve Kurum'un 10.04.2020 tarihinde yayınladığı "bağlayıcı şirket kuralları"na dair bir duyurusu ile Türk hukukuna girmiştir. Bağlayıcı şirket kurallarına ilişkin anılan duyuru, Regülasyon kapsamında hazırlanmıştır. Bu bölümde bağlayıcı şirket kurallarının aktörleri olan grup şirketler, ilgili kişi ve Kişisel Verileri

Koruma Kurulu ele alınmıştır. Ayrıca bu bölümde, bağlayıcı şirket kurallarında bulunması gereken hususlar olan; bağlayıcılık unsurunun sağlanması, bu kuralların etkili uygulanmasının sağlanması, kişisel verilerin işlenmesi ve aktarılması sürecinin açıklanması, Kurum ile koordinasyonun sağlanması, raporlama ve kayıt değişikliği mekanizmalarının belirlenmesi, veri güvenliğinin sağlanması, yapılacak tüm kişisel veri aktarımlarını kapsayacak biçimde veri koruma ilkelerine dair bir açıklama ile teknik ve idari önlemler yer yer Regülasyon ile ele alınarak açıklanmaya çalışılmıştır. Ayrıca KVKK m.12 ve m.15/3 kapsamında şirketlerin, veri işleme ve aktarımında hesap verebilirliği ve şeffaflığı açıklanmıştır. Veri aktarımında Kurul'a başvuru yetkisi, başvuru yöntemi, başvuruda verilecek bilgi ve belgeler ile başvurunun nasıl sonuçlandırılacağı ele alınmıştır. Bununla birlikte, bağlayıcı şirket kuralları kapsamında veri sorumluları ve veri işleyenlerin hukuki (tazminat), idari ve cezai sorumluluğu, Türkiye'de şube ya da irtibat bürosu olan grup şirket veya teşebbüslerin sorumluluk halleri ele alınmıştır. Son olarak bağlayıcıyı şirket kurallarının ihlalinde ispat yükü ve KVKK m.11 kapsamında veri sahibinin hakları ele alınmıştır.

Çalışmanın dördüncü bölümünde Regülasyon'da düzenlenen bağlayıcı şirket kurallarının temel ilkeleri değerlendirilmiştir. Öncelikle AB hukukunda uluslararası veri aktarım yöntemleri, AB hukukunda açık rıza kavramı (Regülasyon m.6-7), Avrupa Birliği Komisyonu'nun uygunluk/yeterlilik kararı çerçevesinde aktarım, yeterli korumaya tabi veri aktarımları (Regülasyon m. 46/2/c), bu kapsamda Schrems I ve Schrems II kararlarında getirilen ölçütler, davranış kuralları (Regülasyon m.40) ve sertifikasyon mekanizması hususları ele alınmıştır. Bununla birlikte, AB hukukunda bağlayıcı şirket kurallarının tanımı, tarihsel gelişimi, bu kuralların getiriliş amaçları, bu kuralların konu ve kişi bakımından uygulanması, m.29 Çalışma Grubu çalışmalarında bağlayıcı şirket kuralları kapsamında verilecek taahhütler, onay süreci ve AB içindeki ana şirketin sorumluluk halleri ve denetim mekanizmaları konuları incelenmiştir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMI, VERİLERİN İŞLENMESİNDEKİ GENEL İLKELER VE VERİ AKTARIMI

I.KİŞİSEL VERİ KAVRAMI

A.Genel Olarak Kişisel Veriler

Kişisel veri kavramı, KVKK'nun 3/1-d maddesinde, 95/46 sayılı Direktif'in 2/a maddesiyle uyumlu olarak gerçek bir kimseye ait olan, belirli veya belirlenebilir her türlü bilgi şeklinde tanımlanmaktadır[11]. Bir başka deyişle kişisel veri; bir kimsenin kişisel, ailevi, mesleki bilgilerine ait olan, bu kimseyi başka kişilerden ayırt edebilecek özellikleri gösteren tüm verilerdir[12]. Bu çerçevede kişinin kimliğini gösteren bilgiler, köken ve fiziksel özellikleri, sağlık, öğrenim bilgileri, özel hayatına dair bilgiler, arkadaşları ile haberleşmeleri, yerleşim adresi, banka şifreleri, kart bilgileri, sosyal medya hesapları, sevdiği renk, yemek, yakın arkadaşı, dini inancı, siyasi düşünceleri, alışveriş davranışları gibi bilgiler, kişisel veri şeklinde tanımlanmaktadır[13]. Elbette bu bilgiler kişiyi belli ya da belirlenebilir kıldığı durumda kişisel veri halini almaktadır. Verinin kişisel veri olarak tanımlanabilmesi için kimliği belli veya tespit edilebilir

[11] Aşıkoğlu, Şehriban İpek, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul, On İki Levha Yayınları, 1. Baskı, 2018, s.5; Başalp, Nilgün, Sırabaşı, Volkan, İlbaş, Çığır, Hanesson, Einar, Kişisel Verilerin Korunması, Ankara Barosu Uluslararası Hukuk Kurultayı 2008 Bilişim ve Hukuk, 2008, II, s.293; Şen, Ersan, Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, İBD, 83(3), 2009, s.1200; Aksoy, 2010, s.11; Akgül, Aydın, Danıştay Kararları Işığında Kişisel Sağlık Verilerin Korunması, Danıştay Dergisi, (133), 2013, s.23; Korkmaz, İbrahim, Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBB Dergisi, 2016, s.94.

[12] Ayözger Öngün, Çiğdem, Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, İstanbul, Beta Yayınları, Genişletilmiş 2. Baskı, İstanbul, 2019, s.6.

[13] Aksoy, 2010, s.1.

kişinin bulunması[14] ve verinin bu kişiye dair olması gerekir[15]. Bu koşulların bulunmaması halinde var olan veri, kişisel veri olmayacaktır[16]. Kişisel verinin gerçek kişiyle ilişkilendirilemez duruma getirilmesi, verinin anonim hale getirilmesi anlamına gelmektedir[17].

Kişisel veri kavramının Anglo–Amerikan hukuk ekolünde genelde ekonomik bir anlayışla mülkiyet ya da fikri mülkiyet çerçevesinde değerlendirildiği görülmektedir. Bu ekole göre kişisel veri, sadece veri sahibinin kendisinin bir uzantısı şeklinde değil, ürünü olarak kabul edilmelidir[18]. Anglo–Amerikan hukuk ekolündeki bu değerlendirme, kişisel verinin fikri mülkiyet hakkı kapsamında[19] ya da eşya hukukundaki "şey" kavramıyla özdeş olduğunu kabul eden[20] mülkiyet hakkı kapsamında nitelendirilmesi gerektiği yönünde 2 yaklaşımı ortaya çıkarmaktadır. İkinci yaklaşım çerçevesinde değerlendirildiğinde veri sahibi, hukuka aykırı bir ihlâl gerçekleşirse denetimini mülkiyet hakkından kaynaklanan yetkilerle yapacaktır. Aynı yaklaşım çerçevesinde veri sahibi kişi, verisinin üstündeki yetkilerini satım, kiralama şeklinde borç ilişkilerinde kullanabilir veya bunların kullanımlarını uygun bir bedelle veya bedelsiz şekilde devredebilir[21]. Bu yaklaşım çerçevesinde örneğin, veri işleme bir ivaz karşılığında gerçekleşeceğinden bu durum veri işleyen şirketleri daha az veri

[14] Dülger, Murat Volkan, Kişisel Verilerin Korunması Hukuku, İstanbul, Hukuk Akademisi Yayınları,1. Baskı, 2019, s.9.
[15]Üçüncü, Sümeyye Hilal, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, İstanbul, On İki Levha Yayınları, 1. Baskı, 2019, s.9.
[16] Dülger, 2019, s.10.
[17] Turan, s.81.
[18] Aksoy, Hüseyin Can, The Right to Personality and It's Different Manifestations as the Core of Personal Data, 2008, Ankara Law Review, s.215; Taştan, Furkan Güven, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, 2017, İstanbul, On İki Levha, s.54.
[19] Prins, Corien, When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter? Script – ed, 2006, s. 279; Samuelson, Pamela, Privacy as Intellectual Property? Stanford Law Review, Vol. 52, No. 5, May, 2000 Symposium: Cyberspace and Privacy: A New Legal Paradigm?, 2000, s.1134; Ayrıca bkz. Ayözger Öngün, s. 17; Aksoy, 2010, s. 60; Taştan, s.57-58; Akgül, Aydın, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul, Legal, 2014, s.74; Küzeci, Elif, Kişisel Verilerin Korunması, Ankara, 2010; Turhan, s.66.
[20] Genel olarak bkz. Ünal, Mehmet ve Başpınar, Veysel, Şeklî Eşya Hukuku, Ankara, Savaş, 2017; Ayan, Mehmet ve Ayan, Nurşen, Kişiler Hukuku, Ankara, Seçkin, 2016, s. 27; Antalya, Osman Gökhan ve Topuz, Murat, Eşya Hukuku Marmara Hukuk Yorumu, 4(1), Ankara, Seçkin, 2019, s.57; Oğuzman, Mustafa Kemal, Seliçi, Özer, ve Oktay Özdemir, Saibe, Eşya Hukuku, İstanbul, Filiz, 2014, s.8.
[21] Akgül, (Kararlar) s.74; Bartow, Ann, Our Date, Ourselves: Privacy, Propertization and Gender. USFL. Review, 1999, s.633; Kang, Jerry, Information Privacy in Cyberspace Transactions. Stanford Law Review, 1998, s.1193; Purtova, Nadezhda, Private Law Solutions in European Data Protection: Relationship to Privacy and Waiver of Data Protection Rights, Netherlands Quarterly of Human Rights Journal, 2010, s.179; Litman, Jessica, Information Privacy/Information Property, Stanford Law Review, 2000, s.1283.

işlemeye zorlayacaktır[22], ek olarak ekonomiyi olumsuz yönde etkileyebilecektir[23]. Çalışmamızda 'Kişisel Verilerin Aktarımında Menfaatler Dengesi' başlığı ele alınırken ilgili kişi ve veri işleyen veri sorumlusu arasında gelişen veri işleme süreci açısından nasıl bir dengenin göz önüne alınması gerektiği ele alınmaya çalışmıştır. İkinci yaklaşım kapsamında ele alınacak bir menfaat dengesinin sağlanması için bir ivaz ödenmesi gerekli olacaktır[24]. Kanaatimizce Anglo–Amerikan hukuk ekolündeki değerlendirmelerden yola çıkarak kişisel verilerin sadece eşya hukukundaki mülkiyet hakkı çerçevesinde ele alınması doğru olmayacaktır. Çünkü veri koruma hukuku bir yönüyle ilgili kişilere özel hayatların gizliliği kapsamında, diğer yönüyle ise veri sorumlusu küresel şirketlerin ticari faydalarına bir koruma sağladığı görülmektedir. Dolayısıyla da bu hukuk kapsamında çok yönlü ve kendine özgü karma bir yapının benimsenmesi, kanaatimizce sağlamaya çalıştığı koruma gözetildiğinde daha uygundur. Yine sadece ikinci yaklaşım ile veri sahibi kişilerin eşya hukukunda mülkiyet hakkının korunmasına dair hukuki yollarla tam korunması da kanaatimizce mümkün olmayıp kendine özgü kuralları olması gereken bu hukuk nezdinde bu hali ile koruma yetersiz kalabilecektir. Mülkiyet hakkı kapsamında yapılan bir değerlendirme, veri sahibinin haklarının bu hak çerçevesinde hukuki çare ve davalarla korunması gerektiğini de beraberinde getireceğinden mülkiyet hakkını koruyucu yol ve dava türlerinin hemen hiçbiri (örneğin: yed'in iadesi TMK m.982 ya da taşınır davası TMK m.989) kişisel verilerin korunmasını doğrudan sağlamamaktadır. Hem fikri hak hem de mülkiyet hakkı görüşüne karşılık veri koruma hukukunun temel amacının mali sorunların çözülmesinden daha çok kişiye ait değerlerin güvence altına alınmasının sağlanması olduğu söylenebilir[25].

Kıta Avrupası hukuk ekolünde ise kişisel veri temel insan hakları ya da kişilik hakkı çerçevesinde ele alınmaktadır[26]. Hukukumuzda kişisel verilerin korunması hakkının dayanağı Anayasa'mızın 20. maddesi, yani özel hayatın gizliliğidir. Özel hayatın gizliliği kişilik hakkı kapsamındaki kişisel değerlerdendir[27]. Klasik kişilik

[22] Litman, s.1292.; Samuelson, s.1135.
[23] Aksoy, 2010, s:57; Taştan, s:55; Dülger, s:44.
[24] Ayözger Öngün, s.17.
[25] Dülger, 2019, s.46.
[26] Samuelson, s.1125; Taştan, s.54.
[27] Hatemi, Hüseyin, Kişiler Hukuku, İstanbul, On İki Levha, 2018, s:66; İmre, Zahit, Kişilik Hakkının Korunmasına İlişkin Genel Esaslar, Özellikle İsim Hakkı ve İsim Hakkının Korunması, Seçkin Armağanı, Ankara, 1974, s.801; Akkurt, Sinan Sami, Sosyal Medyada Gerçekleşen İhlâller Karşısında

hakkı görüşü kişisel veri kavramını kişilik hakkı kapsamında değerlendirir[28]. Kişilik haklarının temel özelliği mutlak hak olması ve hak sahibinin bunu herkese karşı ileri sürebilmesidir[29]. Dolayısıyla da kişisel verisi hukuka aykırı işlenen veya bu işleme nedeniyle zarara uğrayan kişi kişilik hakkı kapsamında bu zararı yanında kişisel verilerine saygı gösterilmesini ve yapılan müdahalelerin önlemesini isteklerini herkese karşı ileri sürebilecektir[30]. Kişinin özel hayatına dahil verilerinin sahibinin rızası dışında, hukuka aykırı olarak kullanılması kişilik hakkının ihlâline yol açacaktır[31]. Ancak mülkiyet ve fikri haklar görüşünde olduğu gibi kişilik hakkı görüşünde de kanaatimizce özel hayatın gizliliğini korumaya yönelik kuralların, sadece şahsın özel alanına dair kişisel değerleri koruyabildiği söylenebilir. Bu kapsamda örneğin, sahibi tarafından alenileştirilmiş veriler koruma kapsamı dışında kalacaktır. Kanaatimizce, kişisel verinin kanunda belirtilen geniş sayılabilecek kapsamı itibarıyla, ne sadece mahremiyet ne de sadece mülkiyet/fikri haklar kavramları gibi kesin ayrımlar yapılmadan daha bütüncül bir yaklaşımla, verinin kategorizasyonu yapılarak, 'karma' ve sadece veri hukukuna özgü bir yaklaşımın benimsenmesi ile 'kendine has' bir yaklaşımla ele alınması daha isabetli olacaktır. Bu kapsamda geniş çerçeveli bağımsız bir hak niteliğinde değerlendirilmesi gerektiği görüşü de belirtilmiştir[32]. Ek olarak belirtmek gerekir ki; Türk veri koruma hukuku açısından, insan hakkı (AY.m.20/ III), kişilik hakkı (TMK m.23,24, 26 vd.; TBK m.58) ve bağımsız hak (AY m.20/ III; KVKK m.1 vd.) birleşimi karma bir yaklaşımın benimsendiği söylemek mümkündür.

Kişilik Hakkının Korunması, Ankara, Seçkin, 2019, s.29; Koyuncuoğlu, Tennur, Tarihsel Yaklaşımla Hak ve Özgürlük İlişkisinin Saptanması, İstanbul Üniversitesi Mukayeseli Hukuk Araştırmaları Dergisi, 2011, s.27; Ayan ve Ayan, s.90.

[28] Terminoloji için bkz. Taştan, s. 65.

[29] Kahraman, Zafer, Medeni Hukuk Bakımından Tıbbi Müdahaleye Hastanın Rızası, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt 7, Sayı 1, 2016, s.482; Dural, Mustafa, Öğüz, Tufan, Türk Özel Hukuku Cilt II Kişiler Hukuku, 12 Basıdan 13. Tıpkı Basım, Filiz, İstanbul, 2013, s.103; Kılıçoğlu, Ahmet, Şeref Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk, 4. Bası, Turhan Kitapevi, Ankara, 2013, s.8; Bilge, Necip, Hukuk Başlangıcı, Ankara, Turhan Kitabevi, 2007, s.217.

[30] Helvacı, Serap, Gerçek Kişiler, İstanbul, Legal Yayıncılık, 4. Bası, 2012, s.101.

[31] Çelik, Yeşim, Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, Türkiye Adalet Akademisi Dergisi, 8/32, 2017, s.391 vd.; Belge, Ayşe Merve, Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 19, (Şeref Ertaş Armağanı Özel Sayısı), 2017, s.1029-1030; Uncular, Selen, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, Seçkin Yayıncılık, Ankara, Güncellenmiş ve Genişletilmiş 2. Baskı, 2018, s.21; Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3.Baskı, İstanbul, 2020, s.13.

[32] Dülger, 2019, s. 47; Taştan, s.66.

Kurum web sayfasında yer alan 'Kişisel Verilerin Korunmasına İlişkin Genel Hususlar' başlıklı rehberinde ifade ettiği üzere[33] hukukumuzda kişisel verilerin korunması hakkı, Anayasa'mızın 20. maddesine dayanmaktadır. Bu nedenle de temel olarak her bir hakkın kullanılması ve başka haklar lehine sınırlanmasına dair yasal düzenlemeler kişisel verilerin korunması hakkında da Anayasa gereği ancak kanun yoluyla gerçekleştirilebilmelidir. Kaynağı Aanaya m. 20, f.1 olan kişisel verilerin korunması, özel hayatın gizliliği ile doğrudan ilgili ve bu hakkın parçası olup[34], bu kapsamda kişisel veri gerçek kişiye sıkı sıkıya bağlı şahıs varlığı hakkı olarak değerlendirilebileceğinden KVKK'da yer alan özel hükümlerin yanı sıra TMK'da yer alan kişilik haklarını koruyan (TMK m.23, 24 ve 25 hükümlerine dayanarak) genel hükümlere göre de korunabilir[35]. Kişisel veriler üstünde denetimin sağlanması kişisel verilerin korunmasını sağlarken; aslında korunan değer, veri sahibinin kişiliği yani kişinin kişisel durumları ile birlikte manevi varlıklarıdır[36]. Çünkü bir aykırılıkta aslında veri değil ilgili kişi zarar görmektedir. Yani kişisel verilerin korunması, Anayasa'da güvence altına alınan bir temel hak[37] olup bu hak ilgilinin rızası bulunmaksızın kişisel verilerine yapılan müdahalelere karşı bireyin korunmasını[38] ve kişisel verilerine ilişkin karar verme hürriyetinin güvence altına alınmasını amaçlar[39].

[33]Bkz. 'Kişisel Verilerin Korunmasına İlişkin Genel Hususlar' başlıklı rehber; https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular s.15, E.T.:06.08.2022.

[34]Aksoy, 2010, s:55; Kılınç, Doğan, Anayasal Bir Hak Olarak Verilerin Korunması, AÜHFD, 61/3, 2012, s:1103; Ünsal, Çağrı Zeybek, Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Marta 2012 Tarihinde Yayınlanan Politikasının Kişisel Verilerin Korunması ile Uyumluluğu ve Avrupa Birliğinin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi, 3/1, 2013, s.102.

[35] Oğuzman, Mustafa Kemal, Seliçi, Özer, ve Oktay Özdemir, Saibe, Kişiler Hukuku (Gerçek ve Tüzel Kişiler), 17. B, İstanbul, Filiz Kitapevi, 2018, s.172; Aksoy, 2010, s.80.

[36] Velidedeoğlu, Hıfzı Veldet, Türk Medeni Hukuku, Umumi Esaslar, İstanbul Üniversitesi Yayınları, İstanbul, C.1, 5. Bası, 1956, s.9; Akipek, Jale G., Akıntürk, Turgut, Ateş Karaman, Derya, Türk Medeni Hukuku, Başlangıç Hükümleri, Kişiler Hukuku, 11. Bası, C.I, Beta Yayınevi, İstanbul, 2014, s.233; Gürkan, Ülker, Kişilik Kavramının Evrimi. Prof. Dr. Hamide Topçuoğlu'na Armağan, Ankara, 1995, s.51.

[37] Gürpınar, Damla, Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-2017, s.684; Zevkliler, Aydın, Havutçu, Ayşe, Gürpınar, Damla, Medeni Hukuk(Temel Bilgiler), Ankara, Turhan Kitabevi, 6. Bası, 2008, s.82.

[38] Helvacı, s.101.

[39] Şimşek, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Yayınları, İstanbul, 2008, s.114.

B. Özel Nitelikli Kişisel Veriler

108 sayılı Avrupa Konseyi Sözleşme'sinde "hassas veri" şeklinde tanımlanan *"özel nitelikli kişisel veriler",* nitelikleri gereği şahısların hak ve hürriyetlerini doğrudan ihlal edebilecek seviyededir ve bu sebeple özel şekilde korunmaları[40] zorunludur. Öte yandan, yasal düzenlemelerde özel nitelikli kişisel verilerin tanımlanması yoluna gidilmemiş ve ne tür verilerin bu sınıfa gireceği genel bir sayma yöntemiyle belirlenmiştir[41].

Özel nitelikli kişisel veriler, KVKK m.6'da; kişinin ırk, köken, siyasi düşünce, felsefi inanç, din, vakıf, dernek, sendika üyeliği gibi bilgileri ile kişinin sağlığı, cinsel hayatına ilişkin bilgileri, genetik ve biyometrik verileri, ceza mahkûmiyeti veya güvenlik tedbirlerine dair bilgileri ile kılık kıyafet bilgileri şeklinde ifade edilmiştir[42]. KVKK m. 6'da bulunmayan bir kişisel veri kategorisi, özel nitelikli kişisel verilerin içine konulamaz. Bu maddede hassas veri olarak da nitelendirilen[43] bu verilerin sınırlı sayma şeklinde belirlendiği görülmektedir[44]. Ayrıca, özel nitelikte kişisel veriler için kanunda daha yüksek bir seviyede koruma getirilmiştir, zira bu veriler başkası tarafından ele geçirilirse ayrımcılığa sebep olabilir[45]; mesela kişinin siyasi düşüncesi öğrenildiğinde o toplumda o kişi hakkında bir önyargı oluşabileceğinden sosyal hayatı olumsuz yönde etkilenebilir. KVKK, özel nitelikli kişisel verinin işlenmesi amacıyla zorunlu şekilde açık rıza ararken (KVKK m. 6, f. II), diğer taraftan bu tür verinin hukuka aykırı olarak kaydedilmesinde suçun nitelikli hali olarak da daha ağır müeyyide öngörmüştür (TCK m. 137, f. I-b).

KVKK'da yer alan veri tanımıyla, bilgi belli koşullar dahilinde kişisel veri haline gelebilmektedir. Örneğin; kişinin uçak bileti alırken seçtiği yemek, dini inancını gösteriyorsa, bu bilgi özel nitelikli veridir[46]. Yine işçinin sendika üyeliği, kişinin uyuşturucuya bağımlı olduğuna ilişkin tedavi kayıtları veya ceza mahkûmiyeti

---

[40] Beyleveld vd., s.28.
[41] Aksoy, 2010, s.30.
[42] Beytar, Erbil, İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2018, s.54.
[43] Bainbridge, David, Data Protection, Welwyn Garden City: CLT Professional Publishing, s:88; Aksoy, 2010, s:30.
[44] Aksoy, 2010, s.32.
[45] Uncular, s.114.
[46] Kaya, Cemil, Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFM, 2011, C. 69, S.1-2, s.322.

kayıtları özel nitelikli kişisel veridir[47]. Bu nedenle, hassas kişisel veriler, daha yüksek bir düzeyde korunmakta ve özel nitelikli kişisel verilerin yasada yer alan durumlar haricinde işlenmemesi hali olan, kesin işlem yasağına tabi olmaktadırlar[48].

Kişinin devletin faaliyetlerinin amaç, içerik, yöntem açısından ne şekilde düzenlenmesi gerektiğine dair görüşleri (siyasi görüş), kişinin inanç ve tapınma sistemi (felsefi ve dini görüş), kişinin fiziksel ve kalıtsal olarak hangi topluluğa ait olduğu (ırk ve köken), cinsel eğilimi ve cinsel ilişkileri (cinsel hayat), sağlığıyla ilgili tüm bilgiler ve sendikal bağlantıları, özel nitelikli kişisel verileridir[49].

Kural olarak kişisel veriler işlenirken açık rıza aranmaktadır. Açık rıza hususunda KVKK'da bir ayrıma gidilmiştir. Buna göre sağlık ve cinsel hayata dair veriler haricindeki özel nitelikli hassas veriler kanunlarda gösterilen durumlarda işlenebilecektir[50]. KVKK m.6/3 gereği; ancak kanunlarda öngörülen hallerde *"sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir*".

Aynı şekilde Direktif'in 8. maddesi ve Regülasyon'un 9. maddesinde yer alan düzenlemesinde hassas kişisel verilerin işlenme koşulları ayrı bir şekilde düzenlenmiştir.

II. KİŞİSEL VERİLERİN İŞLENMESİNDEKİ GENEL İLKELER

Kişisel verilerin işlenirken temel olan husus, işlemenin hukuka uygun olmasıdır. İlgili kişiye ait verinin işlenmesi "açık rıza"yla ya da bunun haricinde mevzuatta işlemenin açık bir biçimde izin verildiği hukuka uygunluk nedenlerinden birisi çerçevesinde işlenmesi durumunda veri işleme eylemi hukuka uygun hale

[47] Özkan, Oğulcan, Kişisel Verilerin Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 2020, s.23.
[48] Taştan, s.44.
[49] Akdağ, Hale, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Adalet Yayınevi, 1. Baskı, 2013, s.33-34.
[50] Özkan, s.23.

gelmektedir[51]. Kişisel veri işlemede genel ilkelere uyulmaması halinde, veri işleme faaliyeti hukuka uygun olmayacak ve bu durum başka hukuki sorunlara yol açabilecektir. Örneğin, bir hekimin hastaya önerilen tedavi ve riskleri, teşhis, maliyeti varsa alternatif yöntemler hakkında aydınlatılmış rıza olmadan yapacağı müdahale hekimin hukuki ve cezai sorumluluğunu doğurabilecektir[52]. Çünkü bir tıbbi müdahale aslında kişinin, sağlığı ve hayatı gibi mutlak haklarıyla ilgili olup, veri sahibi kişinin bu hakkına zarar verecek durum hukuka aykırı ve mutlak hak ihlali olacaktır[53]. Kişisel verilerin işlenmesi faaliyeti; kişinin menfaatlerini ve haklarını gözetmeli, kişinin temel hak ve hürriyetlerini korumalıdır. Bu kapsamda kişisel verilerin işlenmesindeki genel ilkeler ulusal ve uluslararası mevzuatta düzenlenmiştir.

Direktif m.6'da üye devletlerin uymak zorunda olduğu esas prensipler belirlenmişti. Bu prensipler; verilerin hukuka uygun şekilde işlenmesi, belli, açık ve yasal amaçlarla işlenmesi, verilerin alınma amacı ile ilgili ve bu amacı geçmeyecek biçimde işlenmesi, verilerin doğru ve güncel halde olması, verinin ait olduğu kişinin kimliğinin tespitini sağlayacak biçimde saklanma amacı için gereken süre kadar verinin saklanmasıydı. "Veri kalitesi prensipleri" şeklinde adlandırılan bu ilkeler, OECD Rehber İlkeleri ile de benzerlik göstermektedir[54].

"Başlangıç Hükümleri" TMK'da ne kadar önemliyse, KVKK'da da *"kişisel verilerin işlenmesinde genel ilkeler"* o kadar önemlidir. Bu ilkeler, veri koruma hukukunun temel yapı taşlarıdır. Çünkü bu genel ilkeler, KVKK'nın uygulamasında dikkate alınması gereken ana kurallardır[55]. Kurul verdiği bir kararda[56], veri işlemede KVKK m.4'deki ilkelerin bütününün göz önüne alınması gerektiğini yerinde bir şekilde ifade etmiştir. Bu ilkeleri ihlal eden veri işleme faaliyeti belirlediğinde Kurul, ihlal kararı verebilmektedir. Gerçekten de temel yapı taşları niteliğinde ki genel ilkelerin bir bütün olarak bulunmadığı her türlü veri işleme faaliyeti hukuka aykırı sayılmalıdır.

---

[51] Taştan, s.152; Develioğlu, Hüseyin Murat, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2017, s.51.
[52] Kahraman, s.479.
[53] Kahraman, s.479 ve 480.
[54] Aksoy, 2010, s.101.
[55] Akdağ, s.71.
[56] Kurul Kararı, 25.03.2019 T., 2019/78 K., bkz. https://www.kvkk.gov.tr/Icerik/5434/2019-78, E.T.: 06.07.2021.

KVKK kişisel verilerin işlenmesinde izlenmesi zorunlu olan ilkeleri saymıştır (m.4/2). KVKK m.4/2'de kişisel verilerin işlenmesinde izlenmesi zorunlu olan ilkeleri saymıştır. Bu maddeye göre uyulması gereken beş ilke; *"hukuka ve dürüstlük kurallarına uygun olma", "doğru ve gerektiğinde güncel olma", "belirli, açık ve meşru amaçlar için kullanma", "işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme"*dir[57].

A.Hukuka ve Dürüstlük Kuralına Uygun Olma İlkesi

Hukuka ve dürüstlük kuralına uygun biçimde veri işlenme ilkesi, öteki ilkelerin de temeli vasfını taşıyan ve ilk sırada gelen bir ilkedir. Bu ilke sayesinde ilgili kişinin, özgürlük ve güvenlikleriyle doğrudan ilgili olan[58] ve aleyhinde veri toplayan kişiden bilgi sahibi olması, bilgi edinmesi, verisini düzeltme ve sildirme gibi katılım haklarını kullanması kolaylaşacaktır. Direktif m.6/1'de de verilerin hukuka ve dürüstlük kuralına uygun biçimde işlenmesi zorunluluğu belirtilmişti. Bu ilke, veri işleme faaliyetinin başlangıcından sonuna kadar bulunması gereken temel ilke şeklinde kabul edilmektedir.

Bu ilkenin iki unsurundan biri olan, *"hukuka uygun olma ilkesi",* kişisel veri işleme eylemlerinin kanunlar ve diğer mevzuata uygun olması gerektiği anlamına gelir. Hukuka uygunluk, elbette mevzuata uygunluktan daha geniş bir anlama gelmektedir[59].

Veri işleme faaliyeti, dürüstlük kuralına da uygun şekilde gerçekleştirilmelidir. Dürüstlük kuralıyla kasıt, veri işleyen kişilerin veri işlenmesi sürecinde veri sahibinin menfaat ve beklentilerini dikkate almasıdır[60]. AB hukukunda dürüstlük kuralı ilkesi ile

[57] Özkan, s.103.
[58] Döner, Ayhan, Şeffaf Devlette Bilgi Edinme Hakkı ve Sınırları, İstanbul, Oniki Levha Yayınları, 2010, s.101; Akgül, Tez, s.170 vd.
[59] Özdemir, Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin, Ankara 2009, s.137; Küzeci, Elif, Kişisel Verilerin Korunması, Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara, 2019, s.201.
[60] Küzeci, 2010, s.196; Çekin, Mesut Serdar, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 1.Bası, İstanbul, Onikilevha Yayınevi, 2018. s.45.

veri denetçileri, veri işlemedeki amaçlarını anlamaya çalışırken, ilgili şahısların menfaatlerini ve ölçülü beklentilerini göz önüne almaları gerekmektedir[61].

TMK m.2'deki dürüstlük kuralının[62] KVKK bakımından karşılığı ise *"*dürüstlük kuralına uygun olma ilkesi"dir[63]. Ayrıca TMK m.2'de belirtildiği gibi, dürüstlük ilkesi gereğince, taraflar, veri işleme faaliyeti öncesi ve sonrasında birbirlerini aldatmamalı ve bu hakkı kötüye kullanmamalıdır. Dürüstlük kuralı hakkın kullanılmasına bağlı, kullanılmasıyla gelişen bilgi verme, sadakat, inanç, özen gibi yükümlülükleri içermektedir[64]. Emredici nitelikte olan bu kural bu niteliğine rağmen olaya uygulanacak özel nitelikte bir hükmü bertaraf etmez[65]. Bu kapsamda veri işleme faaliyeti dürüstlük kuralı çerçevesinde yapılmalı, veri işleme amacının aşılmasından kaçınılmalıdır. Veri işleme amacının aşılması halinde, işleme faaliyeti hukuka aykırı olur[66].

Bununla birlikte, dürüstlük kuralı çerçevesinde veri sorumlusu, veri işleme faaliyetini gerçekleştirirken şeffaf olmalı, ilgili kişiye yönelik bilgilendirme ve uyarı görevlerini yerine getirmeli[67], *"ilgili kişinin menfaatlerini ve uygun beklentilerini"* de göz önüne almalıdır[68]. İlgili kişinin bilgilendirilmesi de dürüstlük kuralı ile yakından ilişkilidir. Kurul yeni bir kararında[69], veri sorumlusunun, veriyle ilişkili kişiye, veriye sahip olmasına karşın elinde bulunmadığını ifade etmesinin şeffaflıkla uyumlu olmadığını ve dolayısıyla bu durumun dürüstlük kuralını ihlal ettiğine karar vermiştir. Yine Kurul, Facebook aleyhine yapılan bir başvuruya ilişkin verdiği kararda[70], bu uygulama kurulurken bir oyunun, şahsın açık profili ve şahsın bu oyunu oynayan kişilere erişim sağlanması için izin aldığı, ancak bu kişinin paylaşılmasına izin verdiği

---

[61] Bygrave,Lee Andrew, Data Protection Law, Oxford University Press, 2014, s.58.
[62] '*Dürüstlük kuralı, hak ve borçlarını yerine getirirken orta zekalı, makul ve dürüst bir kişiden aynı durum ve koşullarda yapmaları beklenecek şekilde davranma yükümlülüğüdür'*, bkz. Antalya, O. Gökhan/ Topuz, Murat, Medeni Hukuk C. I, Genişletilmiş 3. Baskı, Ankara 2019, s.494.
[63] Özdemir, s.138.
[64] Akyol, Şener, Dürüstlük Kuralı ve Hakkın Kötüye Kullanılması Yasağı, Filiz Kitapevi, İstanbul, 1995, s:3.
[65] Akyol, s.15.
[66] Kuşkonmaz, s.83; Özkan, s.105.
[67] Kaya, Afra Ece, Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu, Terazi Hukuk Dergisi, Cilt:12, Sayı:125, Ocak 2017, s.67-80.
[68] Küzeci, 2019, s.201.
[69] Kurul Kararı, 01.10.2019 T., 2019/294 K.,
bkz. https://www.kvkk.gov.tr/Icerik/6556/2019-294, E.T.: 07.07.2021.
[70] Kurul Kararı, 11.04.2019 T., 2019/104 K.,
bkz. https://www.kvkk.gov.tr/Icerik/5450/2019-104, E.T.: 06.07.2021.

kişisel verilerin hangileri olduğunu bilmesine ve gizlilik ayarında seçim yapmasına olanak sağlanmadığı belirtilerek, kişisel verilerin işlenmesi açık ve özgür bir rızaya dayanmadığından, KVKK m.4/2'da yer alan hukuka ve dürüstlük kuralına uygun olma ilkesinin ihlal edildiğine karar vermiştir. Kurul'un bu ilkeye bakış açısını gösterdiği bir diğer kararı ise, başka hukuka uygunluk sebepleri bulunuyorsa açık rıza hukuka uygunluk nedenine dayanılmasının, dürüstlük kuralına aykırı bir davranış olacağı yönündedir[71]. Bu ve paralellik gösteren kararlar dikkate alındığında her olay özünde bu ilkenin özenli bir bakış açısı ile değerlendirmeye alındığı görülmektedir. '..*Hukuk sadece doğru olanı değil sadece kurallara uygun olanı değil kurallar uygulandığı zaman başkasına haksızlık, başkasına zarar, başkasına kötülük olmayanı da gerektirir, destekler..*[72]' değerlendirmesi dürüstlük kuralı ile yakınen ilişkili olup, kanaatimizce Kurul kararları işte tam da bu noktada her olayı bu yönüyle kendine özgü bir inceleme ile ve bu değerlendirmeye yakın şekilde yaptıkça dürüstlük kuralı denetiminin tam anlamıyla gerçekleştiğinden bahsedilecektir.

B.Verilerin Doğru ve Güncel Olması İlkesi

Veri işlenme faaliyeti yapılırken uyulması zorunlu bir başka ilke,*"doğru ve gerekirse güncel olması"* ilkesidir. Ulusal ve uluslararası veri koruma ilkelerinin kanuni, adil ve şeffaf özellikte olması gerekmektedir[73]. Bu ilke çerçevesinde kişisel verilerin doğru, güncel ve eksiksiz olması, gerekli olandan fazla verinin tutulmaması ve en az seviyede verinin tutulması hedeflenmiştir.

Bu ilke aslında, veriyle ilişkili şahsın, bu verilerin düzeltilmesini isteme hakkıdır. KVKK m. 11/1/d uyarınca, veriler eksik ya da yanlış şekilde işlenmişse veri sahipleri bunların düzeltilmesini isteyebilir. Bu maddeye göre, doğru ve güncel biçimde verilerin tutulmaması halinde ilgili kişi düzeltme hakkını kullanabilecektir[74]. Veri sorumlusu, verilerin doğru ve güncel şekilde tutulması amacıyla gereken idari ve teknik önlemleri almakla sorumludur[75]. Aynı zamanda verileri doğru, hataya yer

[71] Kişisel Verileri Koruma Kurulu Kararı; bkz. https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi, E.T. 10.08.2022.
[72] Akyol, s.2.
[73] Dağ, Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Marmara Üniversitesi, Yayımlanmamış Doktora Tezi, İstanbul, 2011, s.118.
[74] Akgül, Tez, s.170.
[75] Ayözger Öngün, s.145.

vermeksizin ve güncel olarak bulundurmak konusunda kendisinden umulan özeni göstermelidir[76].

Regülasyon m.5/1(d)'de, verilerin işlenme amacı dikkate alınarak, hatalı olan kişisel verilerin hemen düzeltilmesi ya da silinmesi için gerekli faaliyetlerin yapılması gerektiği ifade edilmiştir. OECD Rehber İlkeleri m.8'de kişisel verilerin tam, doğru ve güncel şekilde kaydedilmesi gerektiği ifade edilmiştir.

Verilerin doğru ve gerçeğe uygun olarak işlenmesi, yalnızca veri ilk defa işlenirken değil tüm işleme sürecinde temin edilmelidir. İlgili kişilerin, haklarındaki bilgilerin gerçekle uyumlu olup olmadıklarını denetleyebilme imkânı olmalıdır. Gerçekle uyumlu olmayan ya da güncel olmayan kişisel verilerin de düzeltilmesi veya kaldırılması gerekir[77].

Bahse konusu ilke kapsamında, veri işlendiğinde doğru iken, daha sonra doğruluğunu kaybetmiş olabilir. Bu yüzden veri sorumlularının da, bilgilerin güncelliğini ve doğruluğunu devamlı surette denetlemeleri gerekmektedir. Örneğin, kredi verme işleminde veri sorumlusunun bu ilke çerçevesinde bulunan *"aktif özen yükümlülüğü",* veri sahibi için olumlu veya olumsuz sonuçlara yol açabilir[78].

Verinin doğru olmaması ya da güncel olmaması sebebiyle, ilgili veya bazı durumlarda veri sorumlusu şirketlerde maddi veya manevi zararlar oluşabilir. Örneğin, verilerin yanlış tutulması, müşterilerin adresleri veya elektronik posta adreslerinin yanlış tutulması sonucu şirketler de zarara uğrayabilirler. Bu ilke, veri sorumlusunu bile korumaktadır[79].

Veri sorumlusunun verinin devamlı surette doğru ve güncel tutulması yükümlülüğü devredilemez niteliktedir. Veri sorumlusu, ilgili kişinin ne tür bilgilerinin sürekli olarak güncellendiğini devamlı surette belirleyemeyebilir. Bu halde ilgili kişi, kişisel verilerinde değişiklik meydana gelmesi halinde veri sorumlusuna bilgi vermelidir[80]. Ek olarak belirtmek gerekir ki; belirli bir amaç güdülmeden *"bir gün gerekli olursa"* fikri ile verilerin tutulması, veri sahibini potansiyel suçlu haline getirebilir[81].

[76] Bainbridge, s.61; Çekin, 2018, s.52.
[77] Özdemir, s.138, Ünsal, s.115.
[78] Özkan, s.107.
[79] Develioğlu, s.122.
[80] Küzeci, 2019, s.214.
[81] Küzeci, 2019, s.255.

Bununla birlikte, veriyle ilişkili kişinin ulaşamayacağı bir bilginin doğru olup olmadığını belirlemesi olanaksız olup, ilgili kişinin bu bilgilere erişebilmesi gerekir. Bu açıdan kişisel verilerin doğru ve güncel tutulması ilkesi ile kişinin verilerine erişim hakkı birbirinin içine girmektedir[82].

C.Verilerin Belirli, Açık ve Meşru Amaçlar İçin İşlenmesi İlkesi

Belli, açık ve meşru amaçlarla verilerin işlenmesi ilkesi, veri sorumlusunun amacının net ve kesin şekilde ortaya konulması ve bu amacın belirsiz olmamasıdır. Bununla birlikte, açık şekilde anlaşılabilen amacın meşru olması da gereklidir. Hatta veri sorumlusu, kişisel veri işlerken, hangi veri işleme koşuluna dayandığını ilgili kişiye açık şekilde ifade etmelidir. Bunun yapılamaması halinde bu ilke ihlal edileceğinden, veri işleme işlemi hukuka aykırı hale gelir[83].

Veri sorumlusunun veri iletirken belirlediği amaçla, veri işlediği amaç uyumlu değilse de bu ilkeye aykırılık gündeme gelir. Bu aykırılığın neticelerine veri sorumlusu katlanacaktır. Bunun dışında kişisel bilgilerin gelecekte faydalı olabileceği olasılığına karşın saklanması da amacın belirli olmasını ve açık olmasını ihlal edecektir[84].

İşleme amacının belirli ve açık olması, hem ilgili kişi hem de veri sorumlusu bakımından da geçerli olmalıdır. Diğer bir deyişle, veri sahibi kişi bakımından da amacın anlaşılabilir olması gerekmektedir. İşleme amacının yer aldığı form veya metinlerin bu ilkeyle uyumlu olabilmesi için belirsiz ve ilgili kişinin anlayamayacağı ifadelerin bulunmamasına gayret edilmelidir[85]. Veri sorumlusu, aydınlatma yükümlülüğünü bir metinle yapıyorsa bu metin anlaşılır, sade ve aydınlatıcı bir niteliğe sahip olmalıdır. İlgili kişinin veya başka kişilerin anlamayacağı bir metin kapsamında verilen açık rıza, hukuka uygun bir rıza olmayacaktır. Veri ilgilisi kişi, açık rızasını baskı ve etki altında kalmaksızın, özgür iradesiyle açıklamalıdır. İlgili kişinin, tüm verilerini içerecek biçimde ve genel nitelikte, yani toplu rıza şeklinde bir açık rıza beyanında bulunması da hukuka aykırı olacaktır[86].

---

[82] Kuşkonmaz, s.92.
[83] Kurul Kararı, 01.10.2019 T., 2019/294 K.;
bkz. https://www.kvkk.gov.tr/Icerik/6556/2019-294, E.T.: 07.07.2021.
[84] Küzeci, 2019, s.203; KVKK Gerekçe m.4.
[85] Ayözger Öngün, s.136; Özkan, s.108.
[86] Ayözger Öngün, s.137.

Bu ilke yönünden, Direktif m.6/1(b), Regülasyon m.5/1(b) ve 108 sayılı Avrupa Konseyi Sözleşmesi m.5/b düzenlemeleri ile verilerin ele geçirilmesi esnasında verilerin işlenme amacının, veri sorumlusu tarafından kişiye bildirimi yükümlülüğü getirildiği görülmektedir. 29. Madde Çalışma Grubu casus yazılımların kullanıcılara bilgi vermeden kullanıcı verilerini aktarmalarının meşruluk ilkesiyle bağdaşmadığı yönünde görüş açıklamıştır[87].

KVKK m.4 gerekçesine bakıldığında meşru amaç, veri sorumlusunca işlenen verilerin, yaptığı iş veya hizmetle ilgisinin olması veya bunlar açısından gerekli olması şeklinde belirtilmiştir. Kurul bir kararında[88] şikâyetçinin müşterisi olduğu bankaya verdiği iletişim bilgisinin, eşine ulaşılmada kullanmak için işlenmesinin, KVKK m.4/2/c-ç'de yer alan meşru amaçla ve ölçülü işlenme ilkelerini ihlal ettiğini ifade etmiştir. Meşru olmanın sınırları gereği alınan rızanın amaca uygun olması gerekliliğinin yanı sıra bu rızanın emredici düzenlemelere, kamu düzenine ve kişilik haklarına aykırı (TBK m. 27) olmaması da gerekmektedir. Kanaatimizce, Kurul iletişim bilgisi ile alakalı verdiği yukarıda bahsedilen kararının gerekçesinde, sadece ölçülülük ilkesinden bahsetmekle yetinmeyerek tüm ihlalleri hukukun genel ilkeleri ve kanunun getiriliş amacıyla olan bağlantısını daha detaylı izah ederek ortaya koymalıdır. Çünkü her işleme eyleminin hukuka uygun olabilmesi genel ilkelere ve Kanunun amacına uygun olunması ile mümkün olacaktır.

D.Kişisel Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü İşlenmesi İlkesi

Amaçla bağlılık ilkesi, kişisel verilerin hukuka ve dürüstlük kuralına uygun şekilde işlenmesi ilkesinin somut olayda tatbik edilip edilmediğini göstermektedir[89]. Kişisel veriler, belirli bir amaca uygun şekilde işlenmeli ve bu amaç haricinde işlem yapılmamalıdır. Veriyle ilişkili kişiye sunulan amaç ile verinin işlenme amacı aynı

[87] Article 29 Working Party, Working document on determining the international aplication of EU data protection law to personal data processing on the Internet by non-EU based websites, WP 56, s.12. bkz. http://www.interlex.it/testi/pdf/wd5035.pdf, E.T.: 15.09.2021.
[88] Kurul Kararı, 18.09.2019 T., 2019/277 K., bkz. https://www.kvkk.gov.tr/Icerik/5545/2019-277, E.T.: 06.07.2021.
[89] Kuşkonmaz, s.89.

olmalıdır[90]. Çünkü kişisel verisinin işlenme amacını bilmeyen kişi, doğru bir şekilde karar veremez ve aynı zamanda veri işlenmesini denetleyemez[91].

Verilerin işlenmesindeki amaç; hukuki bir dayanağa sahip olursa, diğer yasal gereklilikler yerine getirilirse ve bu faaliyetten elde edilen fayda ile uyumlu olursa meşru hale gelir[92]. Örneğin, pizza teslimi için satıcının, ilgili kişinin telefon numarasını kaydetmesi ve sonradan kampanya ve indirimlere ilişkin bu numaraya SMS göndermesi halinde, kayıt amacı ile sonradan kullanım amacı farklı olacak ve bu kişisel veri işleme faaliyeti hukuka aykırı bir veri işleme faaliyeti haline gelecektir. Veriye ulaşılmasındaki amaçla işlenmesindeki amaç farklı olursa, veri sorumlusunun yeniden ilgili kişiye başvurması ve rızasını yeniden farklı amaç için alması gerekmektedir[93].

Amaca bağlılık ilkesinin anlamı, verinin sadece meşru amaçlar kapsamında işlenebileceğidir ve bu ilke ile verinin işlenmesine sınır getirilmektedir. Diğer bir deyişle, gelecek bir zamanda meydana çıkacak ve günümüzde bilinmeyen amaçlar için kişisel verilerin işlenmesi de mümkün değildir. Veri işleme faaliyetinin amacı kapsamında ulaşılacak veya elde edilecek veri miktarı, amacı yerine getirecek seviyede olmalıdır.

İlgili amacı yerine getirecek zorunlu veri miktarı ne ise o veri miktarı ile veri işleme faaliyeti sınırlandırılmalıdır. Veri sorumlusu veriyi ele geçirirken verilerin, veri işleme amacına uygun olup olmadığını belirlemeli, amaca uygun olmayan verileri de asla veri işleme faaliyeti kapsamına sokmamalıdır[94].

Kişisel verinin işlenme amacı tespit edilirken, bu amaç için gerekli bir süre belirlenmeli ve bu şekilde işlenme amacı bulunmayan veya kalmayan verinin de işlenmesinin önüne geçilmesi gerekmektedir[95].

Ölçülülük ilkesi, kişisel verinin işlenmesi amacı ile işlenen veri arasında bir dengenin kurulması gerekliliğine denilmektedir[96]. Örneğin dans kursu üyeliği için

[90]Aydın, Sedat Erdem, AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu, On İki Levha Yayıncılık, İstanbul, 1. Baskı, 2015, s.30; Develioğlu, s.46.
[91] Küzeci, 2019, s.209.
[92] Korkmaz, İbrahim, Kişisel Verilerin Ceza Hukuku Kapsamında Korunması, Seçkin Yayıncılık, Ankara, 1. Baskı, 2017, s.115.
[93] Ayözger Öngün, s.138.
[94] Özdemir, 2009, s.142; Korkmaz, 2017, s.116.
[95] Akdağ, s.75.
[96] Özkan, s.112.

başvuran bir kimsenin çalışma hayatına dair veri istenmesi, ölçülülük ilkesi ile uyuşmayacaktır. Bununla birlikte, veri minimizasyonu ilkesi, ölçülülük ilkesinin farklı bir görünümü olarak adlandırılmaktadır. Bu ilke uyarınca veri sorumlusu, gereksinim duyduğu kadar veri işlemeli ve bundan fazla veriyi işlemekten sakınmalıdır.

Veri işlemenin sınırlı olması, en asgari miktarda veri kullanması gerekliliği anlamına gelmektedir. Örnek olarak, güvenlik kamerası bulunan bir mağazada, kameranın mağaza dışını da kayıt altına almasının amaç dışı, sınırı aşan bir veri işleme faaliyeti olduğu belirtilmektedir[97]. Kurul bir kararında[98] spor kulübünde girişte biyometrik veri olan avuç içi izi verisi kaydının KVKK m.4/2'de düzenlenen işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi ile uyuşmadığına ve alternatif seçenekler aranması gerektiğine karar vermiştir. Danıştay da bir kararında, işçilerin iş giriş ve çıkış saatlerinin belirlenmesi için parmak izi taraması yapılmasının hukuka aykırılığına karar vermiştir[99].

OECD Rehber İlkeleri'nde bu ilkeye yer verilmemiştir. Kişisel verilerin elde edilme ve sonrasında işleme amaçları bakımından yeterli, ilgili ve aşırı olmaması gerektiği Direktif'in m.6/1(c) hükmünde belirtilmişti. Regülasyon m.5/1(b) ve 5/1(c)'de ise kişisel verilerin belirli, açık ve meşru amaçlarla elde edilmesi, bu verilerin işleme amaçları bakımından yeterli, onlarla ilgili ve gerekenle sınırlı olması gerektiği ifade edilmiştir.

E. Mevzuatta Yer Alan ya da İşlendikleri Amaç İçin Gereken Süre Boyunca Saklanma İlkesi

Kişisel veriler gerektiği kadar ve en fazla kanunda belirtilen süre kadar tutulmalı veya saklanmalıdır. Direktif m.6/1(e)'de, verilerin ele geçirildiği esnadaki ya da sonrasındaki işleme amaçları açısından gerekli olan süre kadar[100] ve veri öznelerinin tespitini olanaklı kılacak şekilde tutulması gerektiği belirtilmekteydi. Regülasyon m.5/1(e)'de işlenme amaçlarına bakılarak kişisel verilerin gereğinden fazla muhafaza edilmemesi gerektiği belirtilmiştir. Kişisel verinin tutulması, gerek

[97] Küzeci, 2019, s.209.
[98] Kurul Kararı, 25.03.2019 T., 2019/81 K. ve 31.05.2019 T., 2019/165 K.;
bkz. https://www.kvkk.gov.tr/ Icerik/5496/2019-81-165, E.T.: 07.07.2021.
[99] Danıştay İDDK., 09.12.2015 T., 2014/2242 E., 2015/4991 K. (Kazancı, E.T.: 07.07.2021).
[100] Bainbridge, s.61; Küzeci, 2010, s.203; Taştan, s.49; Develioğlu, s.49.

veri sorumlusu gerekse ilgili şahıs bakımından daima bir tehlike oluşturmaktadır. Kişisel verilerin tutulması, ulaşılması istenen amaca varılması sürecine kadar hukuka uygun kabul edilir[101].

Gereken süre kadar tutulma ilkesi aynı zamanda unutulma hakkı ile bağlantılıdır. Unutulma hakkı da kişisel verilerin saklanılması gereken süreden daha fazla tutulamayacağı veya depolanamayacağı anlamına geldiği gibi bireylerin denetim hakkını da ifade eder[102]. Kişisel verinin tutulması amacı; amacın bitmesi, işlenmeye konu hedefin kalmaması, amaç bakımından verinin fonksiyonunun kalmaması, amaca varılması durumlarında ortadan kalkmaktadır. Bu hallerde amaç ve veri arasındaki nedensellik bağı bitmekte, veri işleme faaliyeti işlevsiz duruma gelmektedir[103]. Unutulma hakkı kapsamında Regülasyon'un 17. maddesi gereği veriler çok uzun süredir toplanma amacı kapsamında kullanılmıyorsa veri denetçisi, veri sahibinin verilerini gecikme olmaksızın silmek ve yayılmalarını önlenmek zorundadır. Henüz bu hakla ilgili KVKK'da açık hüküm bulunmamakta olup, HGK'nun "*Unutulma hakkı tanımlarına ilişkin olarak, her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği*" şeklindeki hukuki tespiti önemlidir[104]. İlgili kişi bu hakkı kapsamında yayılmasını, görülmesini istemediği verilerini kaldırabilmektedir. Koruma sağlayan bu hak kapsamında insanca yaşama hakkı, insan onuru, şahsın maddi ve manevi varlığını geliştirme hakkı ve kişinin kendine özgü kişiliği doğrudan etkilenmektedir[105]. İlgili kişi mutlak hakkı kapsamında koruma talebini TMK'daki dava türleri ile herkese karşı ileri sürebileceği gibi bu hakkının korunmasını olası ihlalin özellikle dijital ortamlar nedeniyle gündeme gelebildiği nazara alındığında, TMK'nun yanı sıra "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", "5237 sayılı Türk Ceza Kanunu (TCK)", "6102 sayılı

[101]Akgül, Tez, s.158; Başalp, Nilgün, Kişisel Verilerin Korunması Ve Saklanması, Ankara, Yetkin Yayınları, 2004, s.39.
[102] Carter, Edward L., "The Right To Be Forgotten" Oxford Research Encyclopedia of Communication, bkz. http://communication.oxfordre.com/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-189, Kasım, 2016, E.T. 10.08.2022.
[103] Küzeci, 2019, s.215.
[104] Yargıtay Hukuk Genel Kurulu'nun 17.06.2015, 2014/4-56 E, 2015/1679 K. sayılı kararı.
[105] Ünsal, s.121.

Türk Ticaret Kanunu (TTK)", "5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK)", "6098 sayılı Türk Borçlar Kanunu (TBK)" gibi farklı düzenlemeler ile de isteyebilecektir.

Kişisel verinin işlenmesi için belli bir süre getirilmiş ise sürenin sonunda veriyi tutmaya devam edilebilmesi için bu verinin anonim hale getirilmesi gerekmektedir. Örneğin işine son verilen işçinin kişisel verilerini saklama gibi yasal yükümlülüğü bulunmayan veri sorumlusu işveren bu verileri silmeli, yok etmeli veya anonimleştirmelidir. Bu bağlamda veri sorumlusu, veri tutma prensipleri oluşturmalı veya gereken idari ve teknik önlemleri almalıdır.

Mevzuatta süre getirilmesinin ya da gereken süre kadar saklama ilkesinin esas amacı, "*veriyi yeri geldiğinde kullanırım"* fikrini engellemektir. Aksi halde hukuki yollarla alınmış veri, veri sorumlusunca bir ömür boyu saklanabilir ve bu şekilde veri sahibinin hakları ve özgürlüğü tehdit edilebilir[106]. Kurul bir kararında[107] veri sahibinin, verilerinin silinmesi için veri sorumlusu olan bankaya başvuruda bulunsa da, 5411 sayılı Bankacılık Kanunu m.42'de düzenlenen 10 yıllık saklama süresi geçmediğinden ihlal bulunmadığına karar vermiştir. Kurul yerinde olarak konu hakkında özel bir kanuni düzenleme var ise bu düzenleme doğrultusunda verinin veri sorumlusu tarafından silinemeyeceğini izah etmiştir.

Veri sorumlusu, veri sorumluları siciline bildirdiği makul süreden evvel ilgili verinin işleme amacı sona ermişse, veri sorumlusu bildirdiği süre sonunda değil, amacın sona ermesine istinaden kişisel veri işlenmesini bitirmelidir. Kişisel verinin işlenmesine gerek duymayan veri sorumlusu, ilgili veriyi silmeli ve kanunda aksi bir düzenleme yoksa gösterdiği sürenin bitmesini beklememelidir[108]. Sonuçta kişisel verilerin işlenmesine ilişkin ilkelerin amacı; veri sorumlularını kişisel veri işlemede gereken tedbirleri alma, gereken planlamaları yapma ve bu şekilde veri korumanın bir kültür haline gelmesini sağlamaktır[109].

---

[106] Kuşkonmaz, s.94.

[107] Kurul Kararı, 05.12.2018 T., 2018/142 K.; bkz: https://www.kvkk.gov.tr/Icerik/5424/-Ilgili-mevzuatta-ongorulen-veya-islendikleri-amac-icin-gerekli-olan-sure-kadarmuhafaza-edilme-ilkesi-gereginceKisisel-verilerin-silinmemesi-hakkinda-Kisisel-Verileri-Koruma-Kurulunun-05-12-2018-tarihli-ve-2018-142-sayili-Karari-Ozeti, E.T.: 07.07.2021.

[108] Göçmen Uyarer, Sinem, Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, 1. Baskı, Seçkin Yayıncılık, Ankara, 2019, s.125.

[109] Aydın, S., s.31.

III. KİŞİSEL VERİLERİN AKTARILMASI

Kişisel verilerin işlenmesi, verilere ilişkin tüm işlemleri kapsamaktadır (KVKK m.3/1/e). Bu sebeple kişisel verilerin aktarılması da, veri işleme işlemleri arasında kabul edilmektedir. KVKK m. 8/1'de kişisel verilerin veri ilgilisi kişinin açık rızası olmaksızın aktarılamayacağı hükmü yer almış ve 2. ve 3. fıkralarda istisnalar düzenlenmiştir. Yine KVKK m.9'da verilerin yurt dışına aktarılması hususu yer almıştır. KVKK m. 8'in yurt içinde kişisel verilerin aktarımını düzenlediği görülmektedir. Her iki hüküm de farklı düzenlemeler içerdiğinden yurt içi ve yurt dışı veri aktarım koşulları ve usulleri farklıdır. Bu sebeple bu verilerin transferi, kişisel verilerin yurt içinde ve yurt dışına aktarılması şeklinde ikili ayrıma tabi tutularak incelenmektedir[110].

A.Yurt İçi Aktarım

KVKK m.8'e göre, kişisel verilerin yurt içerisinde aktarım koşulları, KVKK m.5/2'de yer alan kişisel verilerin işlenme koşullarıyla aynıdır. KVKK m.8/1 gereğince kişisel veriler, ilgili şahsın açık rızasının var olması durumunda aktarılabilecektir. Açık rızanın bulunmaması halinde veri aktarımının gerçekleştirilebilmesi için aranan şartlarda,m. 5 ve 6'ya gönderme yapılmıştır. Kişisel verilerin aktarım işlemi de, veri işleme faaliyeti kabul edildiğinden bu atfın makul olduğu ifade edilmiştir[111].

KVKK m. 8/1 gereğince kişisel verilerin aktarılmasında kişinin açık rızası, hukuka uygunluk nedenidir. Şayet veriyle ilgili şahsın açık rızası bulunuyorsa verilerinin üçüncü kişilere aktarımı yapılabilecektir.

Açık rızanın bulunmaması halinde kişisel veri aktarımının gerçekleştirilebilmesi için KVKK m.8/2'deki hükme bakılması gerekmektedir. Bu maddeye göre kişisel veriler, KVKK m.5/2 de ya da yeterli tedbirler alınmak şartıyla, m.6/3'de yer alan koşullardan birinin bulunması durumunda ilgili kişinin açık rızasının alınmasına gerek olmaksızın aktarılabilir. Bu madde uyarınca genel nitelikli verilerin aktarımı için KVKK m.5/2'ye bakılır ve o durumlardan birinin varlığı durumunda

[110] Özkan, s.158.
[111] Özkan, s.158.

hukuka uygun şekilde aktarım gerçekleştirilebilir. Özel nitelikli kişisel verilerin açık rıza aranmaksızın transferinde ise "*yeterli tedbirler alınmak şartıyla"* m.6/3'deki koşullara uyulmalıdır. Kişisel verilerin işlenme koşulları (m.5-6) ile bu verilerin yurtiçinde aktarımı koşulları (m.8) aynıdır.

KVKK m.8 çerçevesinde, hangi durumların veri aktarımı kabul edileceği konusunda sorunlar olabilir. Veri sorumlusu tüzel kişinin kendi organları arasında gerçekleştirdiği aktarımlar, KVKK çerçevesinde bir veri aktarımı sayılmayacaktır. Fakat veri aktarımı bir üçüncü kişiye, diğer bir deyişle, farklı bir tüzel kişiye yapılırsa bu çerçevede veri aktarımı sayılacaktır. Örnek olarak, (TTK) m.195'de düzenlenen *"şirketler topluluğu"*nda birden çok şirket ve dolayısıyla birden çok tüzel kişilik bulunmaktadır. Ancak aynı şirketler topluluğuna bağlı olsalar da şirketler arasında gerçekleştirilen veri aktarımı, KVKK m.8'de yer alan veri aktarımıdır. Çünkü aynı şirketler topluluğuna bağlı olsalar da, farklı tüzel kişilikler arasında veri aktarımı gerçekleştirildiğinden işlem, KVKK m.8'e tabi olacaktır[112]. Bu sebeple KVKK m.8 koşullarına uyulması gerekir. Bu şirketler arasındaki veri aktarımı, açık rızanın bulunması durumunda yapılabilecektir. Fakat açık rıza bulunmasa bile şirketler topluluğundaki şirketler arasındaki veri işleme faaliyetleri, örneğin şartları sağlıyorsa KVKK m. 5/f *"meşru menfaat*" koşuluna dayandırılabilir[113].

Kişisel verilerin aktarımı farklı veri sorumluları kapsamında gerçekleşebileceği gibi, veri sorumlusu ve veri işleyen kapsamında da olabilir[114]. Veri işleyen bahse konu ilişkide üçüncü bir kişi değil, ana unsurlardan biridir. Bununla birlikte, veri işleyen, veri sorumlusuyla yaptığı sözleşme uyarınca veri işleme faaliyeti yapmaktadır. Bu sebeple, veri işleyene gerçekleştirilen aktarım, KVKK m.8'de sayılan koşullara tabi olmamalıdır[115]. Bu aktarıma ilişkin başka kanunlarda bulunan düzenlemeler, KVKK m. 8/3 uyarınca saklı kabul edilecektir. Öte yandan, m. 9/6'da kişisel verilerin yurt dışına aktarılmasında bu Kanun dışındaki yasal düzenlemelerin saklı olduğu belirtilmiştir.

[112] Kurum, Uygulama Rehberi, s.89-90.
[113] Çekin, 2020, s.121-122.
[114] Ayözger Öngün, s.199.
[115] Çekin, 2020, s.122 vd.

B.Yurt Dışı Aktarım

Teknolojideki gelişmelerle beraber çok büyük boyutlara varan veri aktarım miktarı, bilhassa ekonomik ilişkilere bağlı olarak sınır ötesi şekilde günden güne artmaktadır. Kişisel verilerin korunmasının bir amacı, önemli miktarlara varan veri dolaşımının bireylerin hak ve hürriyetlerine zarar vermeyecek biçimde gerçekleştirilmesinin sağlanmasıdır. Burada özellikle uluslararası ticaretin önemi ve kişisel verilerin bu konuda yerinden kısaca bahsetmek gerekir. Uluslararası ticaretin büyümesiyle, bu ticaretin engellerle karşılaşmaması için kişisel verilere her geçen gün ihtiyaç duyulmaktadır. AB temel olarak Maastricht Anlaşması (m. 9,30,42,48,59,73b) ile malların kişilerin, hizmetlerin ve sermayenin serbestçe dolaşımı düşüncesi üzerine kurulmuş bir sistemdir. Belirtilen dört hedefin icrasında, kişisel verilerin elde edilmesi ve işlenmesinin bir mecburiyet olduğu belirtilmektedir[116]. Ülkelerin verilerin korunması ve işlenmesine yönelik mevzuatları birbirinden farklı olduğu için bu husus özellikle veri aktarımı hususunda sorunlar ortaya çıkarabilmektedir. AB üyesi olmayan devletlerde faaliyet gösteren uluslararası ticaret aktörler açısından kişisel verilerin AB haricine aktarılması ve bu transferde uyuması gereken kurallar önem arz etmektedir. AB nezdinde kişisel verileri koruma amacıyla yapılan düzenlemeler veri sahibi kişileri koruma amacına ek olarak, bu koruma sağlanırken verilerin serbestçe dolaşımını sekteye uğratmama amacını taşımaktadır. Nitekim AB nezdindeki ilk yasal düzenleme olan 95/46/EC sayılı Direktif m.1'de kişisel verilerin işlenmesinde özel hayatın gizliliği ile gerçek şahısların hak ve hürriyetlerinin korunmasının ve bu verilerin AB içinde serbest şekilde dolaşımının hedeflendiği açıkça belirtilmektedir. Direktif ile bir taraftan kişisel verilerin hukuka aykırı işlenmesinin önlenmesi hedeflenirken, diğer taraftan serbest şekilde veri dolaşımı temin edilerek şahısların çıkarları ile veri işleyenlerin çıkarları arasında bir denge oluşturulması amaçlanmıştır[117]. Avrupa Birliği önemli bir pazar olduğundan, kişisel verilerin korunması hukuku, sadece Birlik içindeki şirketlerde değil, küresel düzeyde çalışan tüm şirketler için önemli olacaktır.[118] Aslında hem ekonomik hem de siyasi birlik olan AB'nin, sadece Birlik'e üye ülkeler üstünde değil başka ülkeler üstünde de etkili

[116] Başalp, s.25.
[117] Turan, s.41; TBMM 117 sayılı Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, bkz. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf, (TBMM Komisyon Raporu), s.6, E.T.:03.09.2021.
[118] Akgül, Tez, s.198.

olduğu söylenebilir[119]. Bu etki uluslararası şirketlerin bu kuralları gözetme zorunluluğunu ortaya çıkartmaktadır. Tüm bu açıklamalar ışığında küresel ekonominin gelişiminin sağlanabilmesi açısından kişisel verilerin sınır ötesine aktamının engellenmesinin arzu edilmediği, bilakis; bilhassa yurt dışına gerçekleşecek veri aktarımlarının küresel ticarette gittikçe önem arz eden bir değer haline gelmesi nedeni ile küresel bir hukuk zemininde yurt dışı aktarımların kolay şekilde yapılmaya çalışıldığı söylenebilir.

Bu uluslararası ticaret ve ekonomik ilişkiler sebebiyle, kişisel verilerin yurt dışına aktarımının tamamen yasaklanması mümkün değildir[120]. Fakat bir ülkede kişisel verilerin korunması, işlenmesi ve aktarılmasına dair mevzuat ve uygulamaya ne kadar önem verilirse verilsin, başka ülkelerde aynı düzeyde mevzuat ve fiili koruma yeterli olmayabilir. Bu durumda bir ülkede korunan kişisel veriler diğer bir ülkede korunamayabilir. Bu neticede bireylerin temel hak ve hürriyetlerinin ihlaline neden olabilecektir. Bu sebeple yurt dışına kişisel verilerin aktarımında, bazı özel koşullar ve hükümler koymak gereklidir. Yasa koyucu da bu çerçevede verilerin yurt dışına aktarılmasını farklı bir maddede düzenlemiştir.

Yurt dışına aktarımda da açık rıza, hukuka uygunluk nedenidir[121]. Veri ilgilisi şahsın açık rızası bulunuyorsa verilerinin yurt dışına aktarılması mümkün olabilecektir. Bu duruma ilişkin KVKK m. 9/1'de de ilgili şahsın açık rızası bulunmaksızın kişisel verilerin yurt dışına aktarılamayacağı hükmü getirilmiştir. Bununla birlikte açık rızanın aranmadığı haller ise 2. fıkrada düzenlenmiştir. Kişisel verilerin yurt içi aktarımında açık rızanın aranmadığı hallerde olduğu gibi yurt dışı aktarımın söz konusu olduğu durumlarda da aynı şekilde KVKK m.5 ve 6'ya gönderme yapılmıştır. Ek olarak, açık rızanın aranmadığı hallerde, KVKK m. 9/2 ikili bir düzenleme yapılmıştır. Kişisel verilerin yurt dışına açık rıza aranmaksızın aktarımı düzenlemeleri, verinin aktarılacağı yerde*"yeterli koruma"*nın olup olmadığına göre farklılaşmaktadır[122].

[119] Turan, s.39.
[120] Küzeci, 2019, s.357.
[121] Göçmen Uyarer, s.137.
[122] Özkan, s.161.

1.Yeterli Korumanın Bulunması

Kişisel verilerin korunması hususunda bilinçli olan ve bu verilerin korunması hakkına saygı gösteren ülkeler, yeterli korumanın bulunduğu ülkelerdir. Bu sebeple, bu ülkelere veri aktarımında ek koşullar aranmasına gerek bulunmamaktadır. Kişisel Verileri Koruma Kurulu da bahsedilen ülkeleri güvenli ülkeler olarak görecektir.

KVKK m. 9/2 gereğince, m. 5/2 ve 6/3'de düzenlenen koşulardan birinin bulunması ve veri aktarımının yapılacağı yabancı ülkede yeterli korumanın olması şartıyla kişisel verilerin, şahsın açık rızası aranmadan yurt dışına aktarımı sağlanabilir. Yurt içinde aktarım kurumunda olduğu gibi yurt dışına aktarımda da, verilerin işleme koşullarının yer aldığı m. 5 ve 6'ya göndermede bulunulmuştur. Yeterli korumanın olduğu bir yabancı ülkeye verilerin aktarımı için m.5/2 ve m. 6/3'da yer alan veri işleme koşullarından birinin bulunması yeterlidir. Diğer bir deyişle, şayet gönderme yapılan iki fıkradaki koşullardan biri bulunuyorsa, yeterli koruma sağlayan ülkeye kişisel verinin aktarımı yapılabilecek, açık rıza ya da farklı bir koşul aranmayacaktır.

KVKK, yeterli korumanın olduğu ülkelerin belirlenmesini Kurul'a bırakmıştır. Kurul, yeterli korumanın bulunduğu ülkeleri tespit ederek ilan eder (m. 9/3). Fakat Kurul'un bu ilanı yapmadığı görülmektedir. Kurul tarafından ilan yapılana kadar tüm ülkelerin güvenli olmayan ülke şeklinde kabul edilerek aktarım yapılması gerektiği, çünkü bir ülkede yeterli korumanın olup olmadığı belirlenmediği belirtilmiştir[123]. Kanaatimizce özellikle Avrupa Birliği ülkelerinde veri koruma ve aktarımı kuralları ve kurumları yerleştiğinden Kurul tarafından ilan yapılamamış olsa bile bu ülkelerin gerekli korumayı sağladığı kabul edilmelidir.

Kurul, KVKK m.9/4'e göre yabancı ülkede yeterli koruma sağlanıp sağlanamadığına, ülkemizin taraf olduğu uluslararası sözleşmeleri, karşılıklılık halini, verinin niteliği ile işlenme amaç ve süresini, aktarımın yapılacağı ülkenin düzenlemeleri ile tatbikini, aktarılacak ülkedeki veri sorumlusunca taahhüt edilen tedbirleri dikkate alarak karar verir. Kurul bir kararında bu maddede sayılan kıstasları genişleten bir form yayınlamış ve bu maddeye ilave olarak birtakım ek kıstaslar getirilmiştir[124]. Örnek olarak, verinin aktarılacağı ülkede bağımsız bir veri koruma

[123] Özkan, s.162.
[124] Kurul Kararı, 02.05.2019 T., 2019/125 K., bkz: https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-formhakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari, E.T.:05.07.2021.

idaresinin bulunması ve bu ülkenin veri koruma aktarım sözleşmelerine taraf olması gibi kıstaslar getirilmiştir.

2.Yeterli Korumanın Bulunmaması

Kişisel verilerin korunması bakımından yeterli mevzuat, bağımsız idari otorite ve uygulamanın olmadığı ülkeler, yeterli korumanın bulunmadığı ülkelerdir. Yukarıda belirtildiği üzere Kurul, bir ülkede yeterli koruma olup olmadığına karar verir. Yeterli korumanın olmadığı ve veri aktarımı için ilave koruma tedbirleri istenecek ülkeler, Kurul'un güvensiz bulduğu ya da yeterli koruma olmadığını kabul ettiği ülkelerdir. Fakat, bu güvenli veya güvensiz değerlendirmesi, sadece kişisel veriler açısından yapılan bir değerlendirmedir.

Açık rızanın bulunması halinde yeterli korumaya sahip olan ve olmayan ülke ayrımı yapmaya gerek bulunmamaktadır. Veri aktarımı yapılacak ülkenin, yeterli koruma bulunmayan bir ülke olsa da açık rıza bulunuyorsa verinin yurt dışına aktarılabileceği ifade edilmektedir[125]. Bu görüşe katılmakla birlikte, aktarılacak ülkenin yeterli bir korumaya sahip olmadığının ilgili kişiye yapılan aydınlatma metni içerisinde bulunması gerektiği kanaatindeyiz. Açık rızanın bulunmadığı hallerde ise yeterli korumanın olmadığı ülkelere veri aktarımı yapılabilmesi için ek koşullar gerekmektedir.

Veri aktarımının gerçekleştirileceği ülke, yeterli korumanın olmadığı bir ülke ise ilk olarak KVKK m.9 uyarınca, m.5/2 ve 6/3'deki veri işleme koşullarından birinin olması gerekmektedir. Yetersiz korumanın bulunduğu ülkelerde Kanunda öngörülen ek şartlar önem kazanmaktadır. Yeterli korumanın olmaması halinde Türkiye'deki ve yabancı ülkedeki veri sorumluları yeterli korumayı yazılı şekilde taahhüt ederse ve Kurul da izin verirse, şahsın açık rızası aranmaksızın verilerinin yurt dışına aktarılabilmesi olanaklıdır (m.9/2-b). Diğer bir deyişle, yeterli korumanın olmadığı ülkeye kişisel verilerin aktarımına yönelik gerekli ek şartlar; veri sorumlusunca yeterli korumanın olduğuna ilişkin yazılı taahhütte bulunulması ve Kurul'un izninin bulunmasıdır.

[125] Özkan, s.164; Aydın, Muhammet, Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu ve Yargısal Denetimi, Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 2020, s.17.

Yeterli korumanın olmadığı yurt dışı ülkeye, hukuka uygun veri aktarımının yapılabilmesi, bu iki koşulun da sağlanmasına bağlıdır. Kurul da izin verirken, KVKK m.9/4'deki kıstasları dikkate alarak karar verecektir. Açık rızanın bulunması durumunda ilgili kişinin verisinin yurt dışına veri aktarımı yapılıyorsa, veri sorumlusunca taahhütname verilmesine gerek bulunmamaktadır[126].

Kurul bir kararında yurt dışına veri aktarımında veri sorumluları tarafından düzenlenecek taahhütnamede bulunması gereken asgari unsurları belirlemiştir[127]. Kurul, sonraki bir açıklamasında bu taahhütnamelerin *"çok uluslu şirket toplulukları"* açısından yetersiz kalabileceğini belirtmiştir. Kurul, bunu dikkate alarak bu şirketlerin yapacağı yurt dışı veri aktarımına ilişkin *"Bağlayıcı Şirket Kuralları"*nı yayımlamıştır[128]. Yine Kurul *"yurt dışına kişisel veri aktarımında hazırlanacak taahhütnamelerde dikkat edilmesi gereken hususlara ilişkin duyuru"*da bulunmuştur[129]. Bu taahhütnameler düzenlenirken Kurul'un ifade ettiği konulara uyulması, Kurul'un yurt dışına aktarım izni vermesi bakımından önemlidir.

Ayrıca KVKK m.9/5 uyarınca, uluslararası sözleşmelerdeki düzenlemeler saklı kalmak şartıyla, Türkiye'nin ya da kişinin çıkarının ciddi bir biçimde zarar göreceği durumlarda, ilgili ülkede yeterli koruma bulunup bulunmadığına bakılmaksızın bu veriler yurtdışına aktarılabilir. Ancak bunun için diğer bir koşul, ilgili kamu kurumunun görüşünün alınması ve Kurul'un izin vermesidir. Dolayısıyla bu madde, veri aktarımının yapılacağı ülkede yeterli koruma olmasa da uygulama alanı bulabilecektir. Kişisel verilerin aktarımının yapılacağı ülkede yeterli koruma olsa ve m.5 ve m.6 veri işleme koşulları oluşsa bile *"ciddi anlamda menfaat ihlali"nin* gerçekleşeceği hallerde bu verilerin yurt dışına aktarımı amacıyla Kurul'un izni aranmaktadır. Maddede yer alan "*Türkiye'nin ya da ilgili kişinin çıkarının ciddi bir şekilde zarar göreceği"* ibaresi, muğlak bir ibare olduğundan haklı olarak eleştirilmektedir[130].

---

[126] Kişisel Verileri Koruma Kurulu, 6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar, Yayın No: 31, Ankara 2020, s.34.
[127] Kurul, 16.05.2018 T., bkz. https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar, E.T.:06.07.2021.
[128] Kurul, 10.04.2020 T., bkz. https://www.kvkk.gov.tr/Icerik/6728/yurt-dısına-kısısel-verıaktarımında-baglayıcı-sırket-kuralları-hakkında-duyuru, E.T.:06.07.2021.
[129] Kurul, 07.05.2020 T., bkz. https://www.kvkk.gov.tr/Icerik/6741/yurt-dısınakisisel-verı-aktarımında-hazırlanacak-taahhutnamelerde dıkkat-edılmesı-gereken-hususlara-ılıskın-duyuru, E.T.:06.07.2021.
[130] Küzeci, 2019, s.356-357.

C.İşleme ve Aktarma Kavramı

KVKK'da kişisel verilerin işlenmesi; verinin otomatik bir metotla veya bir veri sistemi kapsamında olmak koşuluyla otomatik olmayan metotlar aracılığıyla elde edilmesi, aktarılması, sınıflandırılması gibi işlemlerin tümü olarak tanımlanmıştır (m.3)[131]. Başka bir ifadeyle işleme; verinin ele geçirilmesiyle başlayıp, aktarma, paylaşma, silme, yok etme gibi bütün faaliyetler anlamına gelmektedir.

İşleme, otomatik bir sistemle veya elle yapılabilir. Otomatik şekilde yapılan işleme, bilgi teknolojileri alanında görülmekte olup, verinin bir işleme tabi tutulması bu metotla yapılmaktadır. Herhangi bir teknolojik alet kullanmaksızın elle yapılan veri faaliyeti ise otomatik olmayan işleme yöntemi olarak tanımlanmaktadır. İki metot arasındaki fark, insan müdahalesinin olup olmamasıdır[132]. KVKK, otomatik metotlarla işlenen veriyi korurken, otomatik olmayan metotlarla alınmış veriyi, bir veri kayıt sisteminin parçası olması halinde korumaktadır. Veri, ister otomatik isterse otomatik olmayan yöntemlerle işlensin, koruma standartları bakımından bir farklılığı bulunmamaktadır. İki yöntem bakımından da aynı koruma standartları tatbik edilecektir[133].

Kişisel verilerin aktarılması, diğer bir deyişle, her türlü nakli ve el değiştirmesi aslında kişisel verilerin işlenme çeşitlerinden biridir[134]. İlgili kişinin rızası bulunmaksızın kişisel verilerin yurt içinde ya da yurtdışında aktarılması, kural olarak yasaklanmıştır. Kişisel verilerin üçüncü kişilere aktarılması ise KVKK m. 8'de düzenlenmiştir. Bu madde uyarınca, kişisel verilerin aktarılmasında ilgili kişinin açık rızasına ihtiyaç duyulmaktadır. KVKK m.8/2'de, kişisel verilerin açık rıza bulunmaksızın aktarımının yapılabileceği istisnai haller belirtilmiştir. Veri aktarımı yapılırken KVKK m.5 ve 6'da yer alan hukuka uygunluk nedenleri ile genel ilkeler göz önüne alınmalıdır[135]. Ayrıca, m. 9/1 gereğince kişisel veriler, ilgili şahsın açık rızası bulunmaksızın yurt dışına gönderilemez. Yine m.9/2'de kişisel verilerin açık rıza bulunmaksızın yurt dışına aktarımının yapılabileceği istisnai durumlar gösterilmiştir.

---

[131] Korkmaz, s.95.
[132] Dülger, 2019, s.16; Korkmaz, 2017, s.95.
[133] Dülger, 2019, s.16.
[134] Küzeci, 2019, s.354; Ayözger Öngün, s.199.
[135] Çekin, 2018, s.54.

AB mevzuatında AB dışında üçüncü ülkeler ve uluslararası örgütlere yapılacak kişisel veri aktarımları, Regülasyon'un 40 ila 50. maddeleri arasında düzenlenmiştir. Regülasyon'a göre Avrupa Komisyonu'nun, temin ettiği koruma seviyesini yeterli gördüğü üçüncü ülkelere kişisel veri aktarımına izin verilmektedir (Regülasyon m.45)[136]. Bunun yanında, m.46 gereğince Komisyon'un yeterlilik (adequacy) kararının olmadığı durumlarda bile, veri sorumlusunun veya veri işleyenin yeterli ve uygun güvenlik tedbirlerini alması ve verilerin transfer edileceği ülkede veri özneleri açısından hakların ve etkili hukuki çözümlerin getirilmiş olması şartıyla, aktarım olanaklıdır. Bunlar haricinde m.47'de uygun güvenlik önlemlerinden biri olan bağlayıcı şirket kurallarına dair esaslar yer almış, m.48 ve m.49'da da AB hukukunda izin verilmeyecek veri aktarımları ve istisna durumları düzenlenmiştir[137].

1.Transit Geçiş

Transit geçiş, veri aktarımı ile aynı manaya gelmemektedir. Kişisel veri yalnızca elektronik olarak AB dışında bir ülkeye yönlendirilmişse ve aslında bir AB ülkesinden başka bir AB ülkesine gönderilecekse, yönlendirme yapılan AB dışı ülkeye aslında bir aktarım yoktur. Örneğin, transit geçişte kişisel verilerin, AB üyesi olan Fransa'daki bir veri sorumlusunca İtalya'daki bir veri sorumlusuna Avustralya'daki bir sunucu üstünden aktarımı yapılmaktadır. Avustralya'da iken kişisel verilere erişilmesine ya da bu verilerin kötüye kullanıma dair bir durum bulunmamaktadır. Bu sebeple, bu örnekte transit geçişle aktarım aslında sadece İtalya'ya yapılmaktadır[138].

D.Yurt Dışına Veri Aktarımına Yol Açan Bazı Uygulamalar

Son yirmi yılda internet ortamında ortaya çıkan çerezler, bulut teknolojileri veya hizmet sağlayıcısının sunucuları (server) gibi teknolojiler yurt dışına kişisel veri aktarımına yol açan teknolojilerden bazıları olmuştur. Avrupa Birliği Adalet Divanı'nın (ABAD) verdiği Bodil Lindqvist Kararı (C-101/01), yeni teknolojilerle

---

136 Küzeci, 2019, s.180.

137 Yörük, Onur Doğan, (AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması, İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü Yüksek Lisasn Tezi, İzmir, 2019, s.107.

138 ICO GDRP Guidence, bkz. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, E.T:23.05.2022.

veri aktarımına ilişkin önemli örneklerden biridir. Hemen belirtmek gerekir ki, kararın verildiği dönemde bulut teknolojisi henüz gelişmemişti. Anılan kararda verinin sadece internete konulmasının yurt dışına aktarma manasına gelmediğine karar verilmiştir[139].

Bodil Lindqvist kararıyla getirilen ölçüte göre, bir üçüncü ülkeye veri aktarımı olabilmesi için, verilerin doğrudan o ülkeye gönderilmesi zorunludur. Bu kararın verildiği dosyada özetle; İsveçli Bayan Lindqvist, yalnızca kendisinin ve çalıştığı kilise cemaatinden tanıdığı bazı arkadaşlarının erişebildiği çevrim dışı içeriğinde bazı kişisel verileri barındıran bir web sitesi kurmuştur. Başvurucu bir arkadaşının sağlık kişisel verisini bu web sitesinde yayınlamış; fakat şikâyetleri üstüne içeriği derhal kaldırmıştır. Buna rağmen, İsveç KVKK'na istinaden internet sitesinin varlığı ile ilgili İsveç Kişisel Verileri Koruma Kurumunu bilgilendirmediği, ilgili kişilerin özel verilerini rızaları alınmaksızın işlediği ve bu verileri yurt dışına aktardığı (internet sağlayıcısının bulunduğu yer İsveç sınırları dışındadır) gerekçe gösterilerek başvurucu aleyhinde dava açılmıştır. Dava devamında AAD'den Bayan Lindqvist'in özellikle web sitesinin çevrim dışı çalışan bir bağlantısı olduğu savunması doğrultusunda bu tür bir web sitesine kişisel veri yüklemenin tamamen kendisiyle veya ev halkıyla ilgili faaliyetler kapsamında değerlendirilip değerlendirilemeyeceği görüşü talep edilmiştir. AAD, Bayan Linqvist'i internet sitesini kurmadan evvel arkadaşlarına bilgi vermediği ve arkadaşlarının bilgilerini rızalarını almaksızın paylaştığı gerekçesiyle haksız bulmuş[140], "kişisel verilerin internet ortamında belirsiz sayıda kişiye ulaşabilecek şekilde erişilebilir hale getirilerek işlenmesinin" kişisel veya ev halkı ile ilgili faaliyet kapsamına girmediğini de belirtmiştir[141]. Veri sorumlusu olarak gerçek bir kişiyi tanımlayan ilk dava olması bakımından da önemli olan bu karar, yerel bir bir bilgisayar bağlantısının kullanılmasının üçüncü ülkeye aktarım olup olmayacağını irdelemiş ve bir verinin sırf internet üzerinde erişime açılması ve üçüncü bir ülkeden de erişimin olanaklı olmasını veri aktarımı için yeterli kabul etmemiştir. Karar yer sağlayıcılar

---

[139] Çekin, 2020, s.130.

[140] Várkonyi, Gizem Gültekin, Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları, Kişisel Verileri Koruma Dergisi, Cilt:2, Sayı:2, 2020, s.24 vd.; ayrıca bkz. https://kisiselveriihlali.com/Anasayfa/2967/, E.T:09.08.2022., konu hakkında bkz.;
https://wayback.archive-it.org/org-1495/20200226202722/http://european-convention.europa.eu/EN/glossessent/glossessent2352.html?lang=EN, E.T. 09.08.2022.

[141] AAD, Adalet Savcısı Tizzano'nun görüşü, C-101/01-Lindqvist, par. 47.

tarafından gerçekleştirilen faaliyetlerin yanı sıra üçüncü ülkeye veri aktarımı amacında olunup olunmamasını da dikkate alarak (Mahkeme bu hususta erişilebilirlik olsa da bunun kast edilmediği sonucuna varmıştır) bu sonuca varmıştır. Hizmet sunucusunun fiziksel olarak üçüncü bir ülkede bulunup bulunmadığının araştırılmasını dahi gereksiz bulmuş ve amaca odaklanmıştır. Bu kararda elbette o dönemde bulut teknolojisi bulunmadığından ABAD, üçüncü bir ülkeye veri aktarımı olabilmesi için, verilerin doğrudan o ülkeye gönderilmesini zorunlu bulmuş ancak bu teknolojiye ilişkin bir kıstas getirmemiştir. Bu karara bakıldığında, bulut teknolojisi kullanımında da verinin sadece internete yüklenmesi sebebiyle, yurt dışına aktarım kabul edilmeyeceği gibi bir görüş akla gelebilir. Katıldığımız görüş uyarınca, Bodil Lindqvist kararı ile getirilen ilkeler Regülasyon kapsamında incelenirse, bulut bilişim hizmeti sağlayıcısının sunucularının AB haricinde olması halinde, üçüncü ülkelere veri aktarımı yapıldığı söylenebilir[142].

Ayrıca kısaca değinilecek olursa, tüm dünyada internet ve dijital ortamlarda bu gelişmeler çok hızlı bir şekilde devam etmekte, verilerin işlenmesi, ulaşılabilirliği her geçen gün daha hızlı ve kolay bir hale gelmektedir. 97/66 EC sayılı Direktif ile cep telefonu ağları, dijital televizyon, telefon ile başkaca telekomünikasyon araçlarının dahil olduğu özel bir koruma düzeni getirilmiştir[143]. Ardından 2002/58 sayılı Direktif ile spam maillerinde, cookielerin ve spy-ware'in kullanımındaki sorunlara çözüm bulunması için önlemler getirilmiştir. Türk mevzuatında özellikle teknolojinin yarattığı kolaylıklar nedeni ile oluşan farklı veri işleme süreçlerine özel ve etkin koruma hükümleri henüz getirilmemiştir. Bu hükümler gelene kadar özellikle Kurul'un bu yönde alacağı kararların ve yapacağı açıklamaların mevzuatımızda eksik kalan bu gibi hususları tamamlayıcı ve diğer yandan veri sahibinin haklarını daha koruyucu olacağı kanaatindeyiz.

Ek olarak belirtmek isteriz ki; kanaatimizce özellikle teknolojik gelişmeler karşısında aydınlatma metni içeriklerinin ilgili kişinin veri işleme süreci açısından öngörüsünü kolaylaştıran şekilde olmasının ilgili kişinin korunma düzeyini arttıracağı şüphesizdir. İlgili kişinin verisinin işlenme süreci hususunda şeffaf ve etkin şekilde

[142] Toparlak, Rüya Tuna, Genel Veri Koruma Tüzüğünde Bağlayıcı Şirket Kuralları: Avrupa Birliği Hukukunda Uygulama, Türk-Alma Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul 2021, s.84.
[143] Akgül, Tez, s.151.

bilgilendirilmesi ile etkin şekilde korunması mümkün olabilecektir. Amacın değişmesi ve verinin yeni bir işleme tabi tutulması durumunda ilgili kişinin bu hususta tekrar bilgilendirilmesinin de etkin korunmanın sağlanması açısından önemi büyüktür.

E.Kişisel Verilerin Aktarımında Menfaatler Dengesi

1.İlgili Kişinin Temel Hak ve Özgürlükleri

Kişisel verilerin korunması, 2010 yılında Anayasa m.20/3'de temel hak olarak düzenlenmiştir. Bu hak, kişilik hakkının bir alt kategorisi olup, kişileri, veri işleme faaliyetlerinden gelen tehlikelerden korumaktadır[144]. Kendisine ait kişisel verilerin nasıl ve ne amaçla tutulduğu veya işlendiğinden bilgisi olmayan kişinin, aslında hareket alanı sınırlanmaktadır

Verilerin ne amaçla, nasıl kaydedildiği ve işlendiğine ilişkin tehlike, sadece kişilere yönelik olmayıp toplumu da ilgilendirebilmektedir. Kişinin gizli ve başkaları tarafından öğrenilmesini istemediği bilgilerinin, başkası tarafından elde edilmesi, kişinin rızası olmadan işlenmesi, aktarımı veya üçüncü kişilere devredilmesi kişilerin kendi geleceğini belirleme olanağını önemli ölçüde sınırlayabilir[145].

Kişisel veriler, Anayasa'da korunan temel bir hak ve özgürlük ve dolayısıyla hukuki menfaat olsa da, başka temel hak ve özgürlükler ve menfaatlerle çatışması durumunda, özüne dokunmamak şartıyla sınırlanabilir. Bu çatışma genellikle Anayasa m.26'da yer alan düşünceyi açıklama ve yayma özgürlüğü ile çatışmaktadır. Kişisel verileri açığa vurulan kişinin bu bilginin mahremiyeti hususundaki menfaati ile bilginin yayılması menfaati çatışmaktadır.

2.Veri Sorumlusunun Menfaatleri

Veri sorumlusu, verilerin işleme amaçları ve araçlarına karar veren, veri kayıt sisteminin kurulması ve idaresinden sorumlu olan gerçek ya da tüzel kişidir (KVKK m.3/1-ı). Kanunda "veri kayıt sisteminin kurulması ve idaresinden" sorumlu olmak ifadesinin kullanılması haklı olarak eleştirilse de, veri işleme faaliyetinin amacı temel

[144] Çekin, 2020, s.14; Kılınç, s.1090 vd.
[145] AİHM Reklos ve Davourlis, Yunanistan'a karşı, Başvuru No: 1234/05; K.T.: 15 Nisan 2009.

alınarak, kişisel verilerin neden işlendiğinin tespiti gerekmektedir. Kişisel verilerin neden ve ne şekilde işleneceğini tespit yetkisine sahip kişi, veri sorumlusu olacaktır. Bu kapsamda fiili veya hukuki yetki kavramları gündeme gelmektedir. Veri sorumlusu, taraflar arasında yapılan sözleşme gereğince veri işleyen olsa da, kişisel verileri kendi amaçları çerçevesinde işlemektedir. Veri sorumlusunun menfaati hukuka uygun, somut ve mevcut bir menfaat olmalıdır. Bununla birlikte, veri işleme, bu menfaat bakımından gerekli olmalıdır. Son olarak veri işleme faaliyeti, şahsın hak ve özgürlüklerine zarar vermemelidir[146].

3.Faydaların ve Risklerin Dengelenmesi

Fayda ve risk dengelemesi yapılırken yani menfaat dengesi kurulurken, ilk yapılması gereken veri işleme eylemlerinin, ilgili kişinin hak ve hürriyetlerine zarar vermemesinin sağlanmasıdır. Bu bağlamda, ilgili şahsın hak ve özgürlükleri ile veri sorumlusunun yararları arasında bir denge oluşturulmalıdır. KVKK'da meşru menfaatin "*zorunluluğu*" aranırken, Direktif ve Regülasyon'da menfaatin "*gerekliliği*" aranmakta olup, Direktif m.6/1(f) 'da yer alan düzenlemede, veri sorumlusunun ya da verinin açıklanacağı üçüncü şahsın meşru çıkarı için gerekli olması durumunda kişisel verilerin işlenebileceği belirtilmişti. Regülasyon m.6/1(f) bendinde durum benzer şekilde ifade edilerek, ek olarak Regülasyon'un başlangıç bölümündeki 47. paragrafta bu hukuka uygunluk durumunun kamu kurumları açısından geçerli olmayacağı ifade edilmiştir. Direktif gereğince kurulan Çalışma Grubu, meşru yarara dair yayımladığı Raporda; politik kampanyalar ve sivil toplum kuruluşları açısından yapılan kampanyaları da kapsayacak şekilde ticari amaç izlemeyen ve talep edilmeksizin gerçekleştirilen mesaj gönderimleri yanında olağan doğrudan pazarlama, başkaca pazarlama amacıyla işlemeleri de içerecek şekilde, araştırma için yapılan işlemelerde meşru yararın ilgili şahsın hak ve özgürlüğüne ağır bastığını belirterek bu tür durumlarda verilerinin işlenebileceğini belirtmiştir[147]. Bu kapsamda kurulan dengede veri sorumlusunun faaliyetinin hukuka uygun olabilmesi için veri sorumlusunun

[146] Çekin, 2020, s.54, 104 vd.
[147] Article 29 Working Party, Opinion 06/2014, bkz: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf, E.T:15.09.2021

yararının, ilgili kişinin hakları karşısında eşit ya da üstün gelmesi aranmalıdır. ABAD bir kararında veri sahibinin, arama motorunda yapılan arama sonuçlarında kişisel verilerinin herkes tarafından ulaşılabilecek biçiminde olmasını istememeye dair menfaatinin, arama motorunu yöneten şirketin iktisadi menfaati ile kamunun bu verilere ulaşma menfaatinden daha üstün olduğuna karar vermiştir[148].

Menfaat dengesi kurulurken, daha önce söz edildiği gibi, veri sorumlusunun menfaati, hukuka uygun, somut ve mevcut bir menfaat olmalıdır. Ayrıca, veri işleme, bu menfaat bakımından gerekli olmalıdır. Kişisel verilerin korunması hakkı; verinin özelliği, ilgili kimsenin veri sorumlusuna yönelik haklı ve meşru beklentileri ve öngörülebilirlik gibi kriterler göz önüne alınarak değerlendirilmelidir. İşlenen verilerin içerdiği bilgiler, bu verilerin türü ve önemi, veri işleme faaliyetinin amacı ile karşılaştırılmalıdır. Hassas veriler, ilgili kimsenin daha fazla korunmaya değer verileri olmakla birlikte, özel olmayan örneğin mesleki verilere ilişkin veri işlem faaliyetinde bu koruma gereksinimi daha düşük olacaktır.

İlgili kimsenin kişisel verileri, veri işlemenin amacı bakımından önemli değilse, veri sorumlusunun meşru menfaatinin olduğundan bahsedilemez. Hatta verinin herkese açık bir kaynaktan alınması dahi veri sorumlusunun meşru menfaatinin bulunduğunu göstermemektedir. ABAD'ın Google Spain kararında[149] herkese açık kaynaktan verinin elde edilmesi veri işleme faaliyetini doğrudan meşru hale getirmemektedir. Bu kararda, kişisel verinin işlenmesinin üzerinden çok zaman geçmişse, kamunun o bilgiye ulaşmasından menfaatinin azalacağı ifade edilmiştir.

Menfaat dengesi belirlenirken, ilgili kimsenin hangi menfaatlerinin tehlike altında olduğu belirlenmeli ve veri sorumlusunun da menfaatinin belirlenmesi gerekmektedir. Bunun yanında, ilgili kimsenin menfaatlerini daha az veya hiç ihlal etmeyen seçeneklerin bulunup bulunmadığına da bakılmalıdır. İşleme faaliyetinin toplum gözünde benimsenmesi, işleme faaliyetinin ilgili kimse bakımından açık ve anlaşılabilir olması gibi kıstaslar da veri sorumlusunun lehine değerlendirilebilecek hususlardır[150]. Kişisel verilerin her geçen gün daha kolay ve hızla işlenmesinin

[148] Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014, bkz. https://curia.europa.eu/juris/liste.jsf?num=C-131/12, E.T.:10.08.2022
[149] ABAD, 13.5.2014, C-131/12.
[150] Çekin, 2020, s.105-109.

getirdiği yarar ve avantajlar yanında verilerin istismar edilme riskini ortaya çıkarması, tarafların menfaati arasında meşru ve makul bir dengenin kurulmasını gerektirir.

İKİNCİ BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN YURTDIŞINA AKTARILMASI

I.İLGİLİ KİŞİNİN AÇIK RIZASI İLE AKTARIM

A.Açık Rıza

Verinin "açık rıza" kapsamında işlenmesi halinde veri işleme hukuka uygun duruma gelir[151], yani açık rıza bir hukuka uygunluk sebebidir. Gerek özel nitelikli gerekse diğer kişisel verilerin işlenmesini hukuka uygun hale getiren açık rıza, KVKK m.3'de belirli bir konuya ilişkin olan, aydınlatmaya dayanan ve özgür iradeyle açıklanan rıza şeklinde belirtilmiştir. Açık rıza; kişinin, kendi talebi veya karşı tarafın talebi üstüne kişisel verisinin kaydedilmesi ve işlenmesine onay vermesidir. Açık rıza, ilgili kişi için rehberlik edici olup ilgili kişi, işlenen verisinin içeriği, tutulma süresi gibi niteliklerinde söz sahibi olma hakkına sahip olacaktır[152]. KVKK'daki tanımdan görüleceği üzere, geçerli bir açık rızanın üç unsuru bulunmaktadır. Bu unsurlar; belirli bir konu, bilgilendirme (aydınlatma) esası ve özgür iradeyle açıklamadır. KVKK'nın gerekçesinde açık rızanın *"tereddüde yer vermeyecek açıklıkta olması"* gerektiği belirtilmişse de bu durum, ilgili kişinin irade beyanına ilişkindir ve özgür iradeyle açıklama unsurunun kapsamına girmektedir[153]. Açık rıza, şahsın verisinin işlenmesine kendi talebiyle ya da gelen talep üstüne onay vermesidir[154]. Açık rıza şartına, Regülasyon m.6/1(a) bendinde yer verilmiş, Regülasyon m.4/11'de ise rıza, özgür iradeyle açıklanmış, belli bir konuya dair, bilgilendirmeye dayanan ve tereddüde

[151] Taştan, s.152; Develioğlu, s: 51.
[152] Çekin, 2020, s.74; Dülger, 2019, s.22; Kişisel Verileri Koruma Kurumu, Açık Rıza Alırken Dikkat Edilecek Hususlar, bkz. https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar, E.T.:08.07.2021.
[153] Taştan, s.157; Avcı Braun, Cihan, Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, Haziran 2018, s.19.
[154] KVKK Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi; bkz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf, s.13, E.T: 09.09.2021.

mahal vermeyecek şekildeki bir beyan ya da olumlu manadaki bir eylem vasıtasıyla ilgili şahsın kişisel verilerinin işlenmesine onayını gösteren irade açıklaması olarak tanımlanmıştır.

Birden fazla kişisel veri varsa ilgili kişiden her biri için ayrı açık rıza beyanı alınmalıdır[155]. Açık rıza, ilgili kişinin kişisel verilerinin işlenebilmesi için veri sorumlusunun gideceği esas yoldur. Başka bir deyişle, ilgili kişinin kişisel verilerinin işlenmesi, kanunda sayılan istisnalar arasına girmiyorsa bu verisinin işlenebilmesi amacıyla tek geçerli yol açık rızasının alınması olacaktır. Kişisel Verileri Koruma Kurulu, istisnai durumların bulunması halinde alınan açık rızanın ilgili kişiyi yanlış yönlendirebileceği ve bu biçimde elde edilen açık rızanın hukuka aykırı olduğunu belirtmiştir[156].

Rızanın ehliyet ve yukarıda açıklanan bulunması zorunlu unsurları yönüyle ele alınması uygun bulunmuştur.

1. Rıza Gösteren Kimsenin Ehliyeti

Kişisel verilerin, temyiz kudretine sahip olan hak sahibi (sujesi) kişi[157] tarafından irade sakatlanması bulunmadan rıza göstermeye yetkili olan ilgili kişilerden elde edilmesi gerekir[158]. TMK gereği rızanın geçerli olması için ilk olarak rıza sahibinin hak ve fiil ehliyetine sahip olması[159] gerekmektedir. Bir kişinin fiil ehliyetine[160] sahip olması için TMK m. 10 gereği ergin olması, ayırt etme gücüne sahip olması ve kısıtlı olmaması gerekmektedir.

Belirttiğimiz üzere, ilgilisinin gerçek kişiler olduğu veri sahipleri yönünden hangi şahısların kişisel verilerinin açıklamaya rıza göstermeye ehil olduklarının belirlenmesi amacıyla ilk olarak kişisel veriler üzerindeki bu hakkın niteliğinin tespiti gerekmektedir. Çalışmanın ilk bölümünde bahsedildiği üzere kişisel veri yönünden Türk veri koruma hukuku açısından kişilik hakkı ve bağımsız hak birleşimi karma bir

---

[155] Göçmen Uyarer, s.109.
[156] Dülger, 2019, s.27-28; bkz.;
https://www.kvkk.gov.tr/Icerik/4214/Kurul-Kararlari, E.T.: 08.07.2021.
[157] *'..hak sahibi, hak süjesi anlamına gelmektedir..'*, bkz. Akipek, Jale G., Akıntürk, Turgut, Ateş Karaman, Derya, Türk Medeni Hukuku, Başlangıç Hükümleri, Kişiler Hukuku, 11. Bası, C.I, Beta Yayınevi, İstanbul, 2014, s.229; Helvacı, s.20.
[158] Baindbridge, s.59.
[159] Eren, Fikret, Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, 21. Bası, Ankara, 2017, s.625.
[160] GDPR'da yer alan 8. maddeye göre, kişisel verilerin işlenmesinde, çocuk 16 yaşından büyükse rızasına geçerlilik tanınmakta, 16 yaşından küçükse yasal temsilcisi tarafından verilen rıza da geçerli kabul edilmektedir.

yaklaşımın benimsendiği söylemek mümkündür. KVKK'nın gerekçesine ve amacına bakıldığında, hem veri işleme sürecinde bir disiplinin sağlanması hem de bilgi güvenliği ve ilgili kişinin temel hak ve özgürlükleri esas olmak üzere mahremiyete önem verildiği ve bunları korumanın ve sağlamanın esas alındığı görülmektedir[161]. Kişisel verilerin hukuki niteliğine ilişkin bunların kişiye sıkı sıkıya bağlı hak olduğuna ilişkin bazı görüşler ileri sürülmüştür[162]. Kişiye sıkı sıkıya bağlı haklar, miras yoluyla geçmeyen, başkasına devredilemeyen, hak sahibinin kişiliği ile ilgili haklar olup, kural olarak temsilci vasıtasıyla kullanılamayan ve hak sahibi tarafından kullanılması gereken haklardır[163]. Kişiye sıkı sıkıya bağlı bir hak olan rızanın da bizzat hak sahibince verilmesi gerekir[164]. TMK gereği tam ehliyetli ile sınırlı ehliyetli veri sahipleri, verilerinin işlenmesinde herhangi bir kişinin izin ya da onayına gereksinim duymadan rıza gösterebilirler. Tam ehliyetsiz ilgili veri sahipleri açısından kişisel verilerin işlenmesine rıza gösterme hakkı, bu hakkın mutlak manada şahsa sıkı sıkıya bağlı hak mı, yoksa nisbi manada şahsa sıkı sıkıya bağlı hak mı olduğu hususunda değerlendirme gerektirir[165]. Kanuni temsilcinin şahsa sıkı sıkıya bağlı hakların kullanılması açısından bir temsil yetkisi bulunmamaktadır[166]. Bu konuda çeşitli görüşler bulunsa da[167], kanaatimizce KVKK m. 3, f. I-d bendinde yer alan tanımdan kişiyi tanımlayan bilgi karşısında kişisel verinin, nisbi anlamda kişiye sıkı sıkıya bağlı hak olduğu değerlendirmesi yapılabilir. Mutlak haklar yönüyle kanun temsilcisinin temsil yetkisi bulunmadığı, nispi nitelikteki haklarda bulunabileceği gözetildiğinde bu şekilde bir değerlendirme, ilgili kişinin bu hakkını gerektiğinde kullanabilmesi yönüyle kanuni temsilin gerekliliği de göz önüne alındığında kanaatimizce zaruridir.

[161] Bkz. 'Madde Ve Gerekçesi İle Kişisel Verilerin Korunması Kanunu Bilgi Notu' Başlıklı Rehber, https://www.kvkk.gov.tr/Icerik/5388/Madde-ve-Gerekcesi-ile-Kisisel-Verilerin-Korunmasi-Kanunu-Bilgi-Notu-ve-Kisisel-Verilerin-Korunmasina-Iliskin-Terimler-Sozlugu, s:7, E.T.:08.08.2022.
[162] Bu konuda bkz. Aksoy, 2010, s.37-68; Küzeci, 2010, s.60-102.
[163] Dural, Mustafa, Öğüz Tufan, Türk Özel Hukuku Cilt II Kişiler Hukuku, 16. Baskı, Filiz Kitabevi, İstanbul 2015, s.79.
[164] Kahraman, s.486.
[165] Bu konuda bkz. Oğuzman/ Seliçi/ Oktay Özdemir, 2014: 83; Dural/ Ögüz, 2015, s.79 vd.
[166]Akipek/Akıntürk/Ateş-Karaman, s:316; Oğuzman/ Seliçi/ Oktay-Özdemir,2014, s.82.
[167] Bu konudaki görüşler için bkz.; Kahraman, s:488,489; Oktay Özdemir, Saibe, Tıbbi Müdahaleye ve Tıbbi Müdahalenin Durdurulmasına Rızanın Kimler Tarafından Verileceği, Prof. Dr. Rona Serozan'a Armağan, C.II, On İki Levha Yayıncılık, İstanbul 2010, s.1323-1324; Oğuzman/Seliçi/Oktay-Özdemir, 2014, s.83; Akipek/ Akıntürk/ Ateş-Karaman, s.317.

2.Aydınlatma Yükümlülüğü

Aydınlatma yükümlülüğü KVKK m.10'da düzenlenmiş olup, veri sorumlusu veya veri işleyen; işlenen kişisel verilerin hangileri olduğu, kişisel verilerin hangi amaçla işleneceği ve başkalarına aktarılabileceği, kişisel verilerin hangi nedenle ve usullerle elde edildiği konularında (ilgili kişinin m.11'de sayılan hakları kapsamında) ilgili kişiye bilgi vermekle yükümlüdür[168].

Veri güvenliği için ilgili kişinin veri işleme faaliyetine dair aydınlatılması büyük önem taşımaktadır. Verilerinin işlendiğini bilmeyen ilgili kişi, anılan haklardan tam olarak yararlanamayacaktır. Bu açıdan ilgili kişinin aydınlatılması, gerek kişinin haklarını kullanabilmesini sağlayacak gerekse veri sorumlusuna veri işleme sırasında şeffaflık getirecektir. KVKK'nın veri sorumlusuna yüklediği bu yükümlülük ile veri sorumlusu, keyfi şekilde veri işleyemeyecek ve sürekli veri sahibi ilgili kişinin denetimi ve gözetimi altında olacaktır. Veri işleme faaliyetinin bu şekilde yapılması dürüstlük ve şeffaflık ilkelerinin bir gereğidir[169].

KVKK'da genel olarak düzenlenen aydınlatma yükümlülüğü, Kurum tarafından yayımlanan *"Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"* ile ayrıntılı şekilde yer almıştır. Bu Tebliğ uyarınca aydınlatma yükümlülüğü, veri sorumlusunca sözlü veya yazılı yapılabilir. Örneğin bu yükümlülük; internet sitesinde yayınlanma, işyerinde ilan panosuna asma, ses kaydı, çağrı merkezi gibi fiziksel ya da dijital vasıtalarla yerine getirilebilmektedir[170].

Her veri bakımından aydınlatma yükümlülüğü, farklı olabilmektedir. Veri sorumlusunun işleme faaliyetinde bulunduğu her yeni veri için aydınlatma yükümlülüğü tekrarlanacaktır. Veri sorumlusunun bu yükümlülüğünün işlerlik kazanması için ilgili kişinin istemde bulunmasına gerek bulunmamaktadır[171]. İlgili kişi istemde bulunmasa bile veri sorumlusu, aydınlatma yükümlülüğünü icra etmelidir. Bu yükümlülüğün yapıldığını ispat yükü, veri sorumlusuna düşmektedir.

Açık rıza ve aydınlatma yükümlülüğü birbirinden ayrılmaz niteliktedir. Ancak iki hususunda farklı araçlarla ayrı ayrı yerine getirilmesi gerekmektedir. Kişi, ilk olarak verisinin hangi amaçla işleneceği hususunda aydınlatılmalı, sonra ise kişinin

[168] Taştan, s.158.
[169] Dülger, 2019, s.297.
[170] Çekin, 2020, s.141; Dülger, s.298.
[171] Dülger, 2019, s.300.

açık rıza beyanı alınmalıdır. Nitekim anılan Tebliğ m.5/1-a'ya göre, açık rıza ve aydınlatma yükümlülüğü ayrı ayrı yerine getirilmelidir. Tebliğ'de belirtildiği üzere aydınlatma; verinin ele geçirilmesinden başlayarak uygun bir süre içinde, verinin ilgili şahısla iletişim kurma için kullanılması halinde ilk iletişimin kurulduğu esnada, veri aktarılıyorsa ilk aktarımın yapıldığı sırada gerçekleştirilmelidir[172].

Aydınlatma yükümlülüğünü icra ederken veri sorumlusu, hangi verilerin ne tür amaçlarla işleneceği hususunda basit ve anlaşılır bir dil kullanmalı ve veri ilgilisi kişinin anlayacağı bir biçimde aydınlatma faaliyetini gerçekleştirmelidir. Aydınlatma yükümlülüğü kapsamında alınan bilgiler ile veri sorumluları siciline (VERBİS) kaydedilen bilgiler birbiriyle uyuşmalıdır[173]. Sicile kaydı yapılan her veri açısından, aydınlatma yükümlülüğü yerine getirilmiş olmalıdır.

3.Rızanın Belirli Bir Konuya İlişkin Verilmesi

Belirli bir konuya dair olması ve verinin hangi amaçla işleneceğinin açık şekilde ifade edilmesi, açık rızanın geçerliliğinin bir diğer koşuludur. Veri işlemede genel ilkelerden biri olan amaca bağlılık ilkesi de bu başlık altında ele alınmaktadır[174]. Belirli bir konuya ilişkin olmayan, *"battaniye rıza (blanket consent)"* yani genel nitelikteki bir rıza, geçerli bir açık rıza şeklinde sayılamaz. Örnek olarak, ilgili kişinin *"kişisel verilerimin işlenmesini kabul ediyorum"* beyanı çok geniş kapsamlı olduğundan geçerli bir *"açık rıza"* olmayacaktır[175].

Açık rızada, hangi amaç için rıza gösterildiği belli olmalıdır. *"Gelecekteki istemler", "daha fazla iş"* ve *"diğer şirketlerle işbirliği"* gibi ileride oluşabilecek nedenlerle veri işlenmesi amacıyla beyan edilen rıza, belli konuya dair olmadığından geçersiz olacaktır[176].

Açık rızanın belirli olması yanında, anlaşılabilir olması da gerekmektedir. Açık rızada veri işlemenin ayrıntılı biçimde kapsamı ve işlemenin neticeleri ifade

[172] Çekin, 2018, s.58; Dülger, 2019, s.303.
[173] Dülger, 2019, s.301.
[174] Eraslan Türkmen, Sevgi, Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller,1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019, s.121.
[175] Taştan, s.158.
[176] Han, s.443; Özkan, s.127.

edilmelidir. Ayrıca veri işlendikten sonraki işlemler için de, örneğin verilerin üçüncü kişilere aktarılması gibi ayrı bir açık rıza alınması gerekir[177].

4.Rızanın Özgür İrade ile Açıklanması

Açık rıza, özgür iradeyle açıklanmalıdır. Aşağıda bir sonraki başlıkta izah edildiği üzere rızanın hukuki işlem olduğu yönünde görüşler mevcut olup bir hukuki işlemin kurucu öğesi irade beyanıdır[178]. Şahsın kararı tamamen kendisinin vermesi ve bu iradesini dış dünyaya özgür şekilde aktarabilmesi, özgür irade açıklamasıdır. KVKK m.3/1(a)'da düzenlenen "özgür iradeyle açıklanan" ifadesi, Direktif m.2/h ve Regülasyon m.4/11'de "*özgürce verilen*" şeklindedir. Özgür ve hukuka uygun bir açık rızadan söz edebilmek için beyan edilen rıza, tereddüde yer vermemelidir. İlgili şahsın kişisel verilerinin işlenmesine rıza vermesi, şahsın bu verilere ilişkin geleceğini tayin etme hakkının bir yansımasıdır ve dolayısıyla ilgili kişi zorlama, tehdit, baskı altında bulunmaksızın açık rıza beyanını yapabilmelidir. Özgür bir rıza beyanı, kişinin kendi duygu ve düşüncelerini göstermeli ve gerçek anlamda kişiye bir seçim olanağı vermelidir[179].

Taraflar arasında ekonomik ve sosyal ilişkilerde güçlü güçsüz ayrımının bulunduğu hallerde bu durum dikkate alınmalı ve rızanın özgür bir irade beyanına dayanıp dayanmadığı konusu araştırılmalıdır[180]. Örneğin, veri sorumlusu olan işveren, ilgili kişi olan işçiye *"işe giriş çıkışlarda mesai kontrolü için yüz tarama bilgilerimin, retina bilgilerinin, parmak izimin alınmasına açık rızam vardır"* beyanları yazan bir belge imzalatmaya çalıştığında, bu verilerin alınmasına rızası olmayan işçinin işten çıkarılma tehdidi altında bu bilgilerinin alınmasına açık rıza beyanında bulunması, geçersiz bir rıza olarak kabul edilecektir[181]. Yine sözleşmenin ifasında rızanın aranmadığı bir halde, ifanın rıza şartına bağlanması rızayı geçersiz kılacaktır[182]. Ayrıca internet kullanıcıları, internet sayfalarında yer alan ve *"cookie"* adıyla bilinen

---

[177] Özkan, s.127.
[178] Serozan, Rona, Medeni Hukuk/ Genel Bölüm/Kişiler Hukuku, Yayın No:253, Vedat Kitapçılık, İstanbul, 2011, s.297.
[179] Taştan, s.160; Dülger, 2019, s.25.
[180] Eraslan Türkmen, s.119.
[181] Kuner, Christopher, European Data Protection Law (Corporate Compliance and Regulation), Second Edition, Oxford University Press, 2007, s.68; Çekin, 2020, s.97.
[182] Yücedağ, Nafiye, "Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri", İÜHFM, 2017, C. 75, S. 2, s. 774; Çekin, 2020, s.98.

çerezleri, sayfaya girebilmek için kabul etmek zorunda kalmaktadırlar. Bu durumda ilgili kişinin internet sayfasına girebilmek amacıyla zorunlu şekilde çerezi kabul etmesi, özgür bir irade beyanı şeklinde kabul edilemez[183].

Özgür irade beyanı, somut olay çerçevesinde değerlendirilebilecek bir kavramdır. Örneğin bir malın satışını yapmak için müşterinin kişisel verilerine gereksinim duyan satıcının, malını pazarlamak için satış stratejisi kapsamında veri ilgilisi kişi olan müşteriyi etkileme çabaları, özgür iradenin sakatlanması manasına gelmeyecektir[184].

Veri ilgilisi kişi, açık bir biçimde kişisel verisinin işlenmesi hususunda rıza beyanında bulunmamışsa fakat satıcının ısrarı neticesinde rıza beyanında bulunmuşsa, bu ısrar, ilgili kişinin iradesini sakatlamaya dair bir fiil şeklinde kabul edilebilecektir. Açık rızanın KVKK'ya uygun olarak görülebilmesi için, rızanın bir koşula bağlanmaması gerekir. Örneğin, açık rıza verilmesi durumunda hizmetin yapılacağı dayatması ilgili kişiye yapılıyorsa, bu durumda da yasal anlamda bir açık rızadan bahsedilemeyecektir[185].

B.Açık Rızanın Şekli ve Rızanın Geri Alınabilirliği

KVKK, veri ilgilisi kişinin açık rızasının alınmasına dair bir şekil şartı öngörmemiş olup[186] rızanın hangi usulle verileceğinin, kapsamının ve niteliğinin ne olacağı hususlarında açık bir hüküm yoktur. Açık rıza, yazılı veya sözlü de alınabilir, hatta hareketlere dayanan örtülü bir irade beyanıyla da verilebileceği genel kabul görmektedir[187]. Fakat rızanın yazılı alınması, gelecekte karşı karşıya kalınabilecek uyuşmazlıklarda ispat açısından önemli olacaktır[188]. Veri sorumlusunun, hukuka uygunluk nedenlerinden açık rızaya dayanarak veri işlediğini ispatlaması

[183] Avcı Braun, s.22.
[184] Aydın, S., s.12; Dülger, s.27; Çekin, 2020, s.98.
[185] Dülger, 2019, s.30.
[186] Çekin, 2020, s.98.
[187] Eren, s.625; İşgüzar, Hasan, "3444 Sayılı Kanunla Değiştirilen Borçlar Kanununun 49. Maddesine Göre Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları", Ankara Barosu Dergisi, 1990/6, s.865; Parlak Börü, Şafak, "Esra Kararı Işığında Bir Hassas Denge Değerlendirmesi: Kişilik Haklarının Korunması vs. Sanat Özgürlüğü", İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 8, Sayı: 2, Yıl: 2017, s.262; Polat, Alperen, Sorumluluk Hukukunda Rıza, On İki Levha Yayıncılık, İstanbul 2019, s.122.
[188] Dülger, 2019, s.29.

gerektiğinden[189], yazılı veya kayıt altına alınabilir yöntemleri kullanması ispat kolaylığı yönünden yararına olacaktır[190] .

Rıza beyanının hukuki niteliği konusunda doktrinde genel kabul gören görüş, tek taraflı bir hukuki işlem olduğu yönündedir[191] . Bu görüş doğrultusunda hukuki işlem olan rızanın geçerli olabilmesi için hukuki işlemlerin genel geçerlilik şartları olan ehliyet, şekle uygunluk, hukuka ve ahlaka uygunluk ve irade bozukluğunun bulunmaması şartlarını da taşıması gerekir[192]. Hukuka uygun bir rıza, temyiz kudretine sahip (TMK m. 9) olan gerçek bir şahıs tarafından irade sakatlanmasına yol açmadan verilmelidir.

İlgili kişi açık rıza beyanını istediği zaman geri alabilecektir. "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik*"te yer alan m.5/2-d'ye göre, kişisel verileri işlemenin sadece açık rızaya dayanması halinde şahsın rıza beyanını geri alması durumunda, veri işleme koşullarının ortadan kalktığı kabul edilmektedir[193].

Bu durumda, açık rızanın geri alınması, geçmişe etkili olmaz, yani ileriye dönük etkili olacaktır[194]. Açık rıza, verildiği ve geri alındığı süre içindeki usule uygun veri işleme faaliyetleri açısından bir değişiklik olmayacak ve rızanın geri alınması bu süreç için sonuç doğurmayacaktır. Rızanın geri alınması talebinin veri sorumlusuna ulaşmasından sonra, açık rızaya tabi olan bütün işlemlere veri sorumlusunca son verilmelidir[195].

---

[189] KVKK, Açık Rıza Rehberi, s.3; KVKK, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2019, s.48; WP 29, Opinion 15/2011 on the Definition of Consents, 2011, s.21; Avcı Braun, s.27.

[190] Aşıkoğlu, s.119; Kaya, C., s. 929; Öztürk, Bahri, Altınok Çalışkan, Elif, "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu", Fasikül Hukuk Dergisi, Cilt: 10, Sayı: 100, Mart, 2018, s.293; Kocabaş, Gediz, "KVKK'da Yer Alan Kurum ve Kavramların TMK ve Kıta Avrupası Hukuk Sistemi Kapsamında Değerlendirilmesi", Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, Editörler: Leyla Keser Berber, Ali Cem Bilgili, Marmara Hukuk Bilimsel Toplantılar Serisi-I, 17 Nisan 2019, On İki Levha Yayınları, İstanbul, Ocak 2020, s.110.

[191] Eren, s.625; Çekin, 2018, s. 57; Determann, Lothar; Kişisel Verilerin Korunması Uygulama Kılavuzu – Şirketlerin Uluslararası Mevzuata Uyumu, Çeviri: Av. Hilal Temel, On İki Levha Yayınları, İstanbul, Ocak 2020, s.108; Rızanın hukuki niteliğine ilişkin görüşler için bkz. Polat, s.11-18.

[192] Serozan, 2011, s.344 vd.

[193] Çekin, 2020, s.84-85.

[194] Dülger, 2019, s.28.

[195] Kurum, Türkiye'de Veri Koruma, bkz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/5c02cb3c-7cc0-4fb0-b0a7-85cb90899df8.pdf, E.T.: 08.07.2021.

II.TAAHÜTNAME VERİLEREK YURT DIŞINA VERİ AKTARIMI

Kurul "*Taahhütnameler*"i, Türkiye'de mukim veri sorumlusunun, yeterli veri koruması olmayan ülkelerde mukim veri sorumlusu ya da veri işleyene veri aktarımında, tarafların yeterli korumayı yazılı şekilde sağlamalarına yönelik yöntemlerden biri olarak belirlemiştir. Hazırlanan bu taahhüt içeriğinde veri sorumlusu doldurduğu bilgi ve taahhütte aykırılıktan ve oluşan zarardan ilgili kişiye ve Kurul'a karşı sorumlu olacaktır. Bağlayıcı şirket kurallarında da benzer şekilde bağlayıcı kuralların taahhüt edilmesi nedeniyle bunlara uyulmamasından kaynaklı çalışmanın ilerleyen bölümlerinde incelenen sorumluluk halleri Taahhütler için de geçerlidir.

Türkiye'de mukim olan veri sorumlusunca yeterli veri koruması olmayan ülkelere veri aktarımı için hazırlanacak sözleşmelerde asgari olarak, veri aktarımı yapan veri sorumlusunun yükümlülükleri, veri alıcısı veya işleyenin yükümlülükleri ve ortak hükümlerin yer alması zorunlu tutulmaktadır (KVKK m.9/2-b ve 12/2)[196]. Bu şekilde yapılacak aktarımlarda taraflarca Taahhütname hazırlanarak Kurul'un onayına sunulacaktır. Türkiye'de mukim olmayan bir Grup üyesinden, grup üyesi olmayan bir şirkete gerçekleştirilecek sonraki veri aktarımı ihtiyacı halinde Kurul'un 02/04/2018 tarih ve 2018/33 sayılı kararı ekinde bulunan "Taahhütnameler"in doldurulması gereklidir.

A.Veri Sorumlusundan Veri Sorumlusuna Aktarım

Veri sorumlularından veri sorumlularına aktarım işlemlerinde, taahhütlerde veya sözleşmelerde düzenlenmesi öngörülen hükümler genel olarak şu şekildedir:

a)Veri aktaran veri sorumlusunun sorumlulukları,

b)Veri alıcısının sorumlulukları,

c)Ortak hükümler vb.

Taahhütnamenin sonunda da veri aktaran ve veri alıcısı namına hareket eden kişinin adı, soyadı, açık adresi, irtibat numarası, e-posta adresi ve onay için imza veya

[196] Turan, s.147.

kaşe bölümü bulunmaktadır. Bu unsurlara, sözleşmenin geçerli olabilmesi için başkaca öğeler de eklenebilmektedir[197].

Bu taahhütler veya sözleşmelere ek bölümler de eklenebilmektedir. Buna göre taahhüdün ek bölümünde tarafların doldurması gereken konular; veri konusu kişi grubu ve grupları, veri kategorileri, aktarımın amacı, aktarımın hukuki nedenleri, alıcı grupları, veri aktarılan alıcılar tarafından alınacak idari ve teknik önlemler, VERBİS bilgileri, irtibat kişisi iletişim bilgileri gibi konuları içerebilmektedir[198].

B.Veri Sorumlusundan Veri İşleyene Aktarım

KVKK m.9/2-b ve m.12/2 uyarınca veri sorumlularından veri işleyenlere yurt dışına yapılacak veri aktarımında hazırlanacak sözleşmelerde; veri aktarımı yapan veri sorumlusunun yükümlülükleri, veri alıcısı veya işleyenin yükümlülükleri ve ortak hükümlerin bulunması zorunludur.

Taahhütnamenin sonunda da veri sorumlusu adına ve veri işleyen namına hareket eden kişinin adı, soyadı, açık adresi, irtibat numarası, e-posta adresi ve onay için imza ya da kaşe bölümü yer almaktadır. Ek bölümler veri sorumlusu, veri işleyen, aktarımın hukuki nedeni, veri konusu kişiler, veri kategorileri, veri işleyenler tarafından alınacak idari ve teknik önlemler, VERBİS bilgileri, irtibat kişisi iletişim bilgileri gibi konuları kapsamaktadır.

Yurtdışı aktarımlar uluslararası nitelikte olduğu için uyuşmazlıkların çözüm yolları ve uyuşmazlık çözümünde yetkili organların da belirlenmesi gerekir. Aktarımın yapılmasına ilişkin elektronik ortamların özellikleri de sözleşmeler kurulurken dikkate alınmalıdır. Bu aktarımlar yapılırken, standart ve modellerin geliştirilmesi de önem arz etmektedir[199].

III. GÜVENLİ ÜLKE LİSTESİNE GÖRE YURT DIŞINA VERİ AKTARIMI

[197] Kurum, Taahhütnameler, https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler, E.T.: 08.07.2021.
[198] Turan, s.146.
[199] Turan, s.148.

A.Yeterli Korumanın Sağlanması

Yurt dışına kişisel verinin aktarımının yapılabilmesi için KVKK m.9 uyarınca üç durumdan birinin bulunması gerekir. Bunlardan ilki, ilgili şahsın rızasının varlığı gerekmektedir[200]. İkinci durum ise, yeterli korumanın olduğu ülkelere yapılacak aktarımda, aktarılacak kişisel verinin özelliğine göre m.5/2 veya m.6/3'da yer alan işleme koşullarının bulunmasıdır. Üçüncü durum ise yeterli korumanının bulunmadığı ülkelere ilişkindir[201].

Bu maddeye göre kişisel veri, Kurulca tespit edilerek duyurulan yeterli korumaya sahip ülkelerden birine[202] aktarılacaksa bu verinin özel nitelikli kişisel verilerden olup olmadığına bakılacaktır[203].

1.Aktarılacak Verinin Özel Nitelikli Veri Olmaması

Aktarılacak verinin özel nitelikli veri olmaması durumunda, yurtdışına veri aktarımı için KVKK m.5/2'de düzenlenen koşullardan birinin varlığı gereklidir. Hukuka uygunluk şartları olarak da nitelendirilebilecek[204] bu koşullar şunlardır:

- Yasalarda açık şekilde yer alması,
- Fiili olanaksızlık sebebiyle rızasını açıklayamayacak halde olan ya da vereceği rıza hukuken geçerli olmayan şahsın kendisinin ya da başka bir kişinin yaşamı veya bedensel bütünlüğünün korunması açısından zorunlu olması,
- Bir sözleşmenin yapılması veya edimlerin yerine getirilmesiyle doğrudan ilişkisi olması şartıyla, tarafların kişisel verilerin işlenmesinin gerekmesi,
- Veri sorumlusunun hukuki yükümlülüğünü ifa edebilmesi için mecburi olması,
- Verinin ilgili şahısca aleni hale getirilmiş olması,
- Bir hakkın doğumu, kullanımı ya da muhafazası amacıyla veri işlemenin mecburi olması,
- İlgili şahsın hak ve hürriyetlerine zarar vermemek koşuluyla, veri sorumlusunun meşru çıkarları için veri işlenmesinin mecburi olması.

---

[200] Çekin, 2020, s.109.
[201] Dülger, 2019, s.422.
[202] Kurul halen güvenli ülke listesi oluşturmamıştır, bkz: https://www.kvkk.gov.tr/ıcerik/6828/yurtdısına-verı-aktarımı-kamuoyu-duyurusu, E.T.: 08.07.2021.
[203] Aygözer Öngün, s.200.
[204] Çekin, 2020, s.109.

Bu koşulların bulunması durumunda, ilgili şahsın açık rızasına gerek olmaksızın yeterli koruması olan ülkelerden birine veri aktarılabilecektir[205].

2.Aktarılacak Verinin Özel Nitelikli Veri Olması

Özel nitelikli verinin yurtdışına veri aktarımı için KVKK m.6/3'de yer alan koşullardan birinin bulunması gerekmektedir. Bu koşullar şunlardır;

- Sağlık ve cinsel hayat haricindeki özel nitelikli kişisel veriler, yasada açık şekilde düzenlenmesi durumunda,
- Sağlık ve cinsel hayata dair özel nitelikli kişisel verilerse, sadece kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yapılması, sağlık hizmetleri ile finansmanının planlanması ve idaresi için, sır saklama yükümlülüğü olan kişiler ya da yetkili kurum ve kuruluşlar tarafından işlenmesi durumunda,

ilgili şahsın açık rızasına gerek olmaksızın yeterli korumaya sahip ülkelerden birine aktarılabilir.

IV. BAĞLAYICI ŞİRKET KURALLARI

Şirketlerin hesap verebilirliği, kişilerin özel hayatlarının gizliliğini yani mahremiyetlerinin korunmasını sağlayan bir yükümlülük ve önemli bir ilkedir. Hesap verebilirlik, yürürlükteki veri koruması mevzuatının şirket tarafından uygulanması ve bunların uygulandığının herhangi bir zamanda kanıtlanabilir olması anlamına gelmektedir[206]. Hesap verebilirliği sağlamak için Regülasyon'da idari ve teknik tedbirler, risk analizleri gibi birçok yükümlülük öngörülmüştür. Bağlayıcı şirket kuralları da (binding corporate rules) alınması gereken bu idari ve teknik tedbirleri açık şekilde hüküm altına almakta, taahhüt etmekte ve şirketlerin hesap verebilirliğini arttırmaktadır[207].

Bağlayıcı şirket kurallarının temel düzenlenme amacı, bunu taahhüt eden küresel şirket toplulukları içerisinde serbest veri aktarımının temin edilmesidir. Bu

[205] Aygözer Öngün, s.201.
[206] Toparlak, s.3.
[207] Moerel, Lokke, Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers, Oxford University Press, 2012, s.18-19.

nedenle bağlayıcı şirket kuralları, Regülasyon içinde üçüncü ülkelere veri aktarımı için getirilen makul güvenlik tedbirleri başlığı altında yer almıştır. Fakat bağlayıcı şirket kurallarının birçok başka avantajı da bulunmaktadır. Öyle ki, bu kurallar, grup şirket içinde yapılacak veri koruması hukuku uyumunun esasını oluşturabilecek yükümlülüklerin yapılmasını ve ispat edilmesini sağlayabilecektir.

Günümüzde veri işleme ve aktarma faaliyetleri, ülkelerin sınırlarını aşmıştır. Hızlı ve güvenli bir şekilde verileri üçüncü ülkelere aktarabilmek, gerek bilgi toplumları gerekse ticari hayat açısından büyük öneme haizdir. Bu nedenle çok uluslu bir şirket topluluğu bünyesinde sunulacak benzer bir taahhüdün, Türk kişisel veri koruma hukukuna getirebileceği faydaların anlaşılması üzerine Kişisel Verileri Koruma Kurumu 10.04.2020'de, Türkiye'de yerleşik veri sorumluları tarafından bağlayıcı şirket kuralları getirilebileceğini duyurmuştur. Doktrinde, AB hukukunda Regülasyon kapsamında getirilen hükümlerin bağlayıcı şirket kuralları olduğu, KVKK kapsamında Kurum tarafından oluşturulan bağlayıcı şirket kurallarının ise alternatif uygun güvenlik tedbiri anlamına geldiği belirtilmiştir[208].

[208] Toparlak, s.4.

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA BAĞLAYICI ŞİRKET KURALLARI

I. BAĞLAYICI ŞİRKET KURALLARINA İLİŞKİN GENEL HÜKÜMLER

Bağlayıcı şirket kuralları, çok uluslu şirket topluluğu üyelerinin, Regülasyon'da yer alan yükümlülükleri yerine getireceklerini taahhüt etmeleridir. Bununla birlikte, çok uluslu şirketin kendi gereksinimleri, yapısı ve işleyişi dikkate alınarak konulan düzenlemeler de içermektedir[209]. Bunun dışında bağlayıcı şirket kuralları oluşturulurken şirket topluluğu üyelerinin bağlı oldukları ülkesel mevzuat da dikkate alınmaktadır. Bu nedenle, doğru uygulanması durumunda bu kurallar, düzenleyenlerin veri koruması düzenlemelerine uymasını temin etmekte ve ispat vasıtası şeklinde kullanılabilmektedirler[210].

Regülasyon m.32, veri sorumlusu ve işleyenin riski tespit ederek, ölçülü güvenlik tedbirleri almalarını öngörmektedir. Bu şekilde sorumluluk, şirketlere mal edilmekte ve işledikleri verilerin nitelik ve özelliklerini tespit etmeleri ve veriyle ilgili kişi açısından oluşabilecek riskleri ele almaları öngörülmektedir. Başka bir deyişle, veri sorumluları tarafından yükümlülüklerin ifa edilmesi ve veri koruma otoriteleri tarafından mevzuattaki denetimlerin yapılması şartıyla daha fonksiyonel bir veri koruma sisteminin oluşturulması hedeflenmiştir.

Bağlayıcı şirket kuralları, veri sorumlularına belirli bir serbestlik verdiğinden bu amaca da hizmet etmektedir. AB hukukunda bağlayıcı şirket kuralları terimi, 95/46 nolu Direktif m.29 gereğince kurulmuş bir veri koruma çalışma grubu olan Md.29 Çalışma Grubu kararları[211] ile doktrin ve uygulamada kullanılmıştır. Fakat bağlayıcı

[209] Kuner, s.218 vd.
[210] Toparlak, s.3
[211] Çalışma Grubu 29'un Bağlayıcı Şirket Kuralları hakkında 2008 yılında düzenlenmiş dokümanı 2017 yılında yenilenmiştir, dokümanın 2017'deki güncellenmiş versiyonu için bkz. https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/binding_corporate_rules

şirket kuralları ilk kez Regülasyon ile AB mevzuatında düzenlenmiştir. Bağlayıcı şirket kuralları, Regülasyon'da yer alan tüm yükümlülükleri taahhüt etmesi nedeniyle Regülasyon'a uyum sağlamakta ve Regülasyon'un genel mantığına, koyduğu ilkeler ile veri güvenliği ilkelerine atıf yapabilmektedir. Bağlayıcı şirket kuralları, Regülasyon m.4'te tarif edilmiş ve bu kuralların nasıl uygulanacağı da m. 47'de ifade edilmiştir.

AB hukukunda uzun bir süredir var olan bağlayıcı şirket kuralları, birden çok ülkede yerleşik şirketler bakımından veri aktarımında büyük kolaylıklar sağlamaktadır. Türk hukukunda da Kurum 10.04.2020'de "bağlayıcı şirket kuralları"na dair bir duyuru yayımlamıştır[212]. Duyuru kapsamında bulunan şirketlerin, belirtilen formu doldurup yönergeleri izleyerek Kurum'a başvuru yapması gerektiği ifade edilmiştir. KVKK m. 9/2 (b) gereğince, bahse konu başvurular, Kurul'un iznine tabidir[213].

Kurum'un yayımladığı metnin, aslında Çalışma Grubu'nun meydana getirdiği belgelerin bir çevirisi olduğu görülmektedir. Kaldı ki, her iki metin arasında küçük farklılıklar bulunduğu görülmektedir. Kurum'un duyurusu, özgünlük açısından eleştiriye konu olsa da bağlayıcı şirket kurallarının kabulü, Türk hukukunda kişisel verilerin yurtdışına aktarımı bakımında önemli bir adım olarak değerlendirilmiştir[214]. Kurul tarafından güvenli kabul edilen ülkelerin isimlerinin henüz yayımlanmaması ve yurtdışına veri aktarımı amacıyla Kurum'a sunulan taahhütnamelerin cevapsız bırakıldığı göz önüne alındığında, veri sorumluları açısından yurtdışına veri aktarımı yapılmasında, ilgilinin rızasını almak haricinde bir yol getirilmesinin uygulamada hayati öneme sahip olduğu kabul edilmektedir[215].

_for_controllers.pdf , dökümanın 2008'deki güncellenmemiş hali için bkz. https://ico.org.uk/media/for-organisations/binding-corporate-rules/1042457/bcr_table_wp153.pdf, E.T.:15.08.2022.

[212] Kurul, Bağlayıcı Şirket Kuralları, bkz. https://www.kvkk.gov.tr/ıcerik/6728/yurt-dısına-kısısel-verı-aktarımında-baglayıcı-sırket-kuralları-hakkında-duyuru, E.T: 08.07.2021.

[213] Çabuk, Ezgi, Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul 2020, s.104.

[214] Dülger, Murat Volkan, KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları, 11 Nisan 2020, s.6, bkz. https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html, E.T.: 09.07.2021.

[215] Çabuk, s.105.

II. AKTÖRLER

A. Grup Şirketleri

"*Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu*"nda "Grup" tanımı, "*Bir şirketler topluluğuna bağlı olarak faaliyet gösteren şirketler, teşebbüsler ile ortak bir ekonomik faaliyette bulunan veya veri işleme faaliyetine ilişkin ortak bir karar mekanizması bulunan veri sorumlularının tümü*" olarak yapılmıştır. Grup Şirket, bir şirketler topluluğuna tabi şekilde faaliyette bulunan şirketler, girişimler ile ortak bir ekonomik faaliyet yapan ya da veri işlemeye dair ortak bir karar sistemi olan veri sorumlusudur. Grup Üyesi ise şirketler topluluğunun bünyesinde olan bir şirket veya girişimle ortak bir ekonomik faaliyeti olan veyahut veri işleme faaliyetine dair ortak bir karar sistemi olan bir gruptaki veri sorumlusudur. Türkiye'de yerleşik bir merkezi bulunmayan Grup Şirketin böyle bir durumda kişisel verilerin korunması konusunda bir Grup üyesini yetkilendirmesine ihtiyaç bulunup, bu kişi yetkili Grup üyesini ifade etmektedir.

Bağlayıcı şirket kuralları, grup şirketler içerisindeki veri aktarımlarında uygun bir güvenlik önlemi olarak kabul edilmektedir. Bu kurallar, şirketler topluluğu bünyesinde bulunan bütün şirketler arasında kişisel verilerin serbestçe dolaşımını temin etmektedir. Grup şirket içerisinde küresel çapta, Regülasyon ile uyum içinde olan aynı veri koruma sisteminin oluşturulması, aktarım sürecini de daha kolay yapmaktadır. Bunların yanı sıra bu kurallar aktarımı 'Grup' için daha kolay idare edilebilir ve bu sürecin ilgili kişiler tarafından da daha rahat anlaşılabilir durumuna getirmektedir.

Regülasyon'da bağlayıcı şirket kurallarının, grup şirket veya ekonomik iş birliği statüsündeki girişim yapısı içinde, veri işleyen ya da veri sorumlusu için hazırlanabileceği belirtilmektedir. Veri sorumlusu bağlayıcı şirket kuralları; veri aktarımlarını içerecek şekilde, veri sorumlusu vasfıyla gerçekleştirilen bütün veri işleme faaliyetlerini düzenlemektedir. Veri işleyen bağlayıcı şirket kuralları ise, dış kaynak bulma gibi (*outsourcing*) müşteriler namına görüşmeler yapılırken

kullanılmaktadır. Öte yandan, m.29 Çalışma Grubunca yayımlanan ilk bağlayıcı şirket kuralları taslağı, veri sorumlularını dikkate alarak düzenlenmişti[216].

Bununla birlikte, Regülasyon m. 4/20'deki bağlayıcı şirket kuralları tanımında veri sorumlusu ve veri işleyen ayrımlarına yer verilmemiştir. Ancak her iki kavram için de bağlayıcı şirket kuralları düzenlemek olanaklıdır ve bu durum ilgili şirketin kararına bırakılmıştır[217].

Regülasyon m.5/2 uyarınca veri sorumlusu olan grup şirketleri, veri işleme ilkelerine uymalıdır ve bu durum aynı zamanda hesap verebilirliği de sağlamaktadır. Çalışma Grubu m.29'un çalışmaları ve Regülasyon'a göre veri sorumlusu/ veri işleyen grup şirketlerinin bağlayıcı şirket kuralları asgari şu koşullara sahip olmalıdır:

-Ortak girişim ya da bir şirketler grubu ve üyelerinin yapısı ve irtibat bilgileri,

- Kişisel verileri işleme amaçları, veri ilgilisi kişilerin türü ve ayrıca üçüncü ülke ya da ülkelere dair taahhüt ve açıklamaları kapsayacak şekilde veri aktarım dizisi ile bunların hukuki bağlayıcılık niteliği,

-79. madde gereğince AB üyesi devletlerin yetkili kontrol merciine ve yargı organlarına şikâyet etme hakkı, tazminat talep etme hakkı ve veri ilgililerinin gerekirse bağlayıcı şirket kurallara dair bir ihlalden ötürü tazminat hakkını da kapsayacak şekilde kişisel veri işlenmesine dair hakları ve bu hakları kullanma usulleri,

-Amaç sınırlaması, saklama sürelerinin sınırlandırılması, olağan ve özel veri koruması, işleme eylemine dair hukuki dayanak, özel kategorilerdeki kişisel verilerin işlenmesi öncelikli olmak kaydıyla genel veri koruma ilkeleri, veri güvenliğinin temin edilmesine dair önlemler ve bağlayıcı şirket kuralları olmayanlara transit aktarımlara dair protokollerin uygulanması,

- (d), (e) ve (f) bentlerinde gönderme yapılan düzenlemeler öncelikli olmak kaydıyla bağlayıcı şirket kurallarına dair bilgilerin m.13. ve 14'e ilave olarak veri ilgililerine ne şekilde temin edildiği,

- 22. madde gereğince sadece otomatik işleme eylemine dayanan kararlara tabi olmama hakkı,

[216] Bowman, John, Gufflet, Myriam, 'Meeting the Challenge of a Global GDPR and BCR Programme', European Data Protection Law Review, C. 3, S. 2, 2017, s.257-261.
[217] Toparlak, s.61.

- AB üyesi devlette yerleşik veri sorumlusu ya da veri işleyicinin AB içinde yerleşik bulunmayan herhangi bir üye şirketçe bağlayıcı şirket kuralların ihlal edilmesi konusunda yükümlülüğü üstlenmesi,
- 37. madde gereğince tespit edilen bir veri koruma görevlisinin veya ortak girişim grubu ya da bir işletmeler grubu içinde bağlayıcı şirket kurallarına uyumluluğun takip edilmesinin yanında eğitimin takibi ve şikayetlerin sonuca bağlanmasından sorumlu olan diğer şahıslar ya da kuruluşların görevleri,
- Şikâyet yöntemleri,
-Ortak girişim ya da bir işletmeler grubu içinde bağlayıcı şirket kurallarına uyumluluğun doğrulanmasının teminine dair sistemler,
-Kurallara dair yapılan değişikliklerin rapor edilmesi, kaydedilmesi ve bu değişikliklerin yetkili denetim makamına rapor edilmesine ilişkin mekanizmalar"[218].

Sonuç olarak, bağlayıcı şirket kurallarını taahhüt eden ve veri sorumlusu/veri işleyen Türkiye'deki üye şirket, onaylanan bu şirket kurallarına uymalıdır. Bilhassa veri işleme ilkelerine, hukuka uygunluk nedenlerine ve veri sahibi şahıslardan alınacak rızalara Regülasyon'da yer alan ve bağlayıcı şirket kurallarında yazıldığı biçimde uymalıdır. Türkiye'deki şirket, aynı zamanda bağlayıcı şirket kuralları kapsamında kendisine aktarımı yapılan verileri, üçüncü bir tarafa aktarırken yeri geldiğinde Regülasyon'da yer alan veri aktarımı yükümlülüklerine de uymalıdır[219].

1.Veri Sorumlusu Grup Şirket

Veri sorumlularının bağlayıcı şirket kuralları, ilgili kişilere ait verilerin, Türkiye'de kurulu veri sorumlularından aynı grup içindeki ve Türkiye haricindeki başka veri sorumluları ya da veri işleyenlere aktarımı amacıyla kullanılır. Veri sorumlusu, KVKK m.3'de kişisel verinin işleme amacını ve araçlarını belirleyen, veri kayıt mekanizmasının kurulması ve idaresinden sorumlu olan gerçek ya da tüzel kişi şeklinde tarif edilmiştir. Gerçek kişiler haricinde şirketler, vakıf, dernek gibi tüzel kişiler de veri sorumlusu olabilir[220]. Bu bağlamda grup şirketler de veri sorumlusu olabilecektir. Grup şirketler açısından değerlendirildiğinde şirket grubunu meydana

[218] Dülger, Makale, s. 6.
[219] Toparlak, s.63-64.
[220] Memiş, Tekin,Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt:3, Sayı:6, Aralık 2017, s.9-23.

getiren her bir şirketin tüzel kişiliği bulunduğundan, bu şirketlerin ayrı ayrı veri sorumlusu olması olanaklıdır. Ancak her bir şirket içinde bulunan bölüm veya birimler ayrı bir tüzel kişiliğe sahip olmadığından, bunların veri sorumlusu olması olanaksızdır. Veri sorumlusu ya da işleyen kavramları değişkenlik gösterebilmekte olup, örneğin bir kredi kuruluşu kendi çalışanı ile ilgili veri sorumlusu iken, müşterileri ile ilgili veri işleyen haline de gelebilmektedir. Veri sorumlusu, kişisel verilerin işleme faaliyetine dair karar verme yetkisine sahip olup, verilerin işlenme amacı ve usulüne karar veren kişi yine veri sorumlusudur. Yani ortada bir veri işleyen dahi olsa veri işleme faaliyet çerçevesinde kendi namına karar alma yetkisi bulunan ve veri işlenmesinin gerekçesini ve ne şekilde yapılacağını cevaplayacak olan taraf veri sorumlusudur[221]. Veri sorumlusu belirlenirken bazı ölçütler kullanılmaktadır. Bunlar; kişisel verilerin işlenip işlenmediği, işlenecekse işlenme amacı, işlenecek kişisel verilerin çeşitleri, bu verilerin üçüncü kişilere aktarılıp aktarılmadığı veya ne amaçla aktarıldığı, bu verilerin saklanma süresi gibi ölçütlerdir. Bu ölçütler çerçevesinde hareket eden, karar organı görevini yapan şirket veya kişi veri sorumlusudur[222].

Uygulamada veri sorumlusu genelde tüzel kişiler ve çoğunlukla şirketler olmaktadırlar. Veri sorumlusu şirket, KVKK'daki düzenlemeleri uygulayan olduğundan, sorumluluklarla yüz yüze olan ve oluşabilecek zararların sorumlusudur[223].

Veri sorumlusu şirketler, kişisel verilerin hukuka uygun şekilde işlenebilmesi için gereken örgütlenmeyi sağlamalı, veri işleme faaliyetinde gereken teknik ve idari önlemleri almalıdırlar.

Şirketlerin, veri sorumluluğu görevini organları aracılığıyla veya gerçek kişilerle ifa etmesi KVKK'dan kaynaklanan yükümlülüklerini kaldırmayacaktır. Bu yükümlülüklerin gerektiği gibi yerine getirilmemesinden doğan sorumluluk, veri sorumlusu şirkete ait olacaktır ve bu şirket hukuki yaptırımlara da uğrayabilecektir[224].

Ayrıca, bazı şartlara haiz veri sorumlu şirketlerin kayıt zorunluluğunun bulunduğu ve veri işleme faaliyetlerine dair ilgili bilgilerin bildirildiği Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) isimli bir kayıt sistemi bulunmaktadır. Bu

[221] Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,
bkz: https://www.kvkk.gov.tr/Icerik/2030/Rehberler .PDF, s.57, E.T:17.10.2021.
[222] Dülger, 2019, s.17; Çekin, 2020, s.53-54.
[223] Memiş, s.12.
[224] Dülger, 2019, s.25.

sistemin amacı, veri sorumlularının kim olduğunu kamuya açıklamak ve dolayısıyla kişisel verilerin korunması faaliyetlerini etkili bir biçimde devam ettirmektir[225]. Bu sicilin tutulması, kamuya açıklık ilkesine dayanmakta olup, bu ilke ile veri sorumlusunun hukuka aykırı bir biçimde veri işlemesi engellenmektedir. Öte yandan, veri ilgilisi kişi, kişisel verilerinin korunması açısından kendini güvende hissedip hak ihlali halinde başvuracağı veri sorumlusunu bilebilecektir.

Veri sorumlusu şirketi, veri işleyenden de ayırmak gerekmektedir. KVKK'daki pek çok yükümlülüğün muhatabı veri sorumlusu şirket iken veri işleyenin sorumluluk sahasının sınırlı olduğu söylenebilir. Veri sorumlusu, yöntemle ilgili hususlarda örneğin, verilerin hangi usulle muhafaza edileceği, verilerin elde edilmesi, korunması için hangi sistemlerin ya da metotların kullanılacağını, kişisel verilerin aktarımının, yok edilmesi, silinmesi ve anonimleştirilmesinin hangi yöntemle yapılacağını, veri işleyene aralarında yapacağı sözleşmede detaylarını net şekilde belirtmek sureti ile bırakabilir. Bağlayıcı şirket kurallarını uygulayacak veri sorumlusu şirketin veri aktarımında bulunacağı diğer şirketleri ile yapacağı kişisel veri işleme sözleşmelerinde sınırları ve yöntemleri çok net ve detaylı şekilde belirlemiş olması gereklidir.

2. Veri İşleyen Grup Şirket

KVKK m.3/ğ uyarınca veri işleyen, veri sorumlusunun devrettiği yetkiye istinaden onun namına kişisel veri işleme faaliyeti yapan gerçek ya da tüzel kişidir. Veri işleyen şirket veya gerçek kişi, veri sorumlusundan bağımsız değildir ve veri sorumlusu adına yani onun verdiği yetkiyle hareket ettiğinden onun vekili sıfatıyla hareket etmektedir. Veri işleyen şirketler; kişisel verinin aktarımı, kaydı, silinmesi, saklanması gibi kişisel veri işleme faaliyetleri yürütmektedirler[226].

Veri işleyen şirketin veri sorumlusu şirket veya gerçek kişiden bağımsız şekilde karar verme yetkisi bulunmamaktadır. Diğer bir deyişle, veri işleyen şirket veri sorumlusunun emir ve yönergeleri doğrultusunda hareket etmelidir. Veri işleyen şirket, şirket veya grup şirket içinde tek bir şirket olmak zorunda değildir. Veri sorumlusu, veri işleyen farklı şirket veya şirket gruplarına sorumluluk verebilir.

---

[225] Kişisel Verileri Koruma Kurumu, Veri Sorumluları Sicili Nedir?, bkz: https://www.kvkk.gov.tr/Icerik/2043/Veri-Sorumlulari-Sicili-Nedir?, E.T.:13.09.2021.
[226] Aşıkoğlu, s.72.

Veri işleyen şirket, grup şirket içinden bir şirket veya grup şirket dışından bir şirket olabilir. Veri işleyen şirketin, veri sorumlusu şirketten farklı bir tüzel kişiliğe sahip olması zorunlu değildir. Hatta veri sorumlusu ve veri işleyen aynı şirket de olabilir. Örneğin bir grup şirket mali konular açısından veri sorumlusu şirket olup, şirketin muhasebecisi gerçek kişi veya hesap işlerine bakan şirket, veri işleyen olacaktır. Bunun yanında veri işleyen şirketin, birden fazla veri sorumlusu şirketin veri işleyeni de olabilmesi mümkündür[227].

Veri sorumlusu şirket; kişisel verilerin toplanacağı teknolojik sistemlerin belirlenmesi, verilerin saklanma yöntemleri ve verilerin korunması için alınması gereken güvenlik tedbirleri, verilerin aktarımının yapılma yöntemleri, kanuni sınırlar içinde verilerin saklanacağı süreler, verilerin silinmesi, anonim hale getirilmesi, yok edilmesi gibi konularındaki yetkilerini veri işleyen şirkete yapacağı kişisel veri işleme sözleşmesi ile bırakabilir.

Yetki devri, sorumluluk devri anlamına gelmemektedir. Anılan konulardaki yetkiler veri işleyen şirkete devredilmiş olsa bile, veri sorumlusu şirketin kişisel verinin işlenmesinden doğan zararlar bakımından hukuki sorumluluğu sürecektir. Kişisel verilerinin işlenmesinden dolayı zarar gören veya hakları ihlal edilen veri ilgilisi kişi, veri işleyen şirkete değil veri sorumlusu şirkete başvurmalıdır[228]. KVKK m.12/2'de düzenlenen şartları haizse veri sorumlusu ve veri işleyenin müştereken sorumlu olmaları söz konusudur. Sonuçta kişisel verilerin korunmasında veri ilgilisi kişinin oluşan zararlarından da veri sorumlusu ve işleyen müştereken sorumlu olacaktır. Veri işleyen şirket ve veri sorumlusu şirket arasındaki ilişkinin ve sorumluluğun sınırlarını tespit için taraflar arasında yazılı bir sözleşme yapılması isabetli olacaktır[229].

B.İlgili Kişi

Lafzından anlaşıldığı üzere, KVKK'nun sağladığı korumadan gerçek kişiler faydalanabilmektedir. Ayrıca belirtmek gerekir ki, açık bir hüküm KVKK kapsamında yer almıyor olsa da; Türk Medeni Kanunu'nda düzenlenen kişi kavramı ve kişiliğin

[227] Memiş, s.15.
[228] Dülger, 2019, s.21.
[229] Aşıkoğlu, s.73.

sağ ve tam doğma koşuluyla ceninin ana rahmine düştüğü andan başlaması (TMK m. 28) ile ölümle sona erdiği temel alındığında, ölen şahıslara ait verilerin KVKK'nda yer alan veri koruma mevzuatı hükümlerinden yararlanmasının mümkün olamayacağı söylenebilir. Yani KVKK hayatta olan gerçek kişilere koruma sağlamaktadır. Çalışma Grubu m.29'un çalışmaları sonucu oluşturulan Regülasyon uyarınca bağlayıcı şirket kuralları ilgili kişi açısından asgari şu koşulları içermelidir: Regülasyon m.79 gereğince veri ilgililerine; AB üyesi devletlerin yetkili denetim makamlarına ve yetkili mahkemelerinde dava açma, tazminat talep etme ve bağlayıcı şirket kurallarına dair bir ihlalden ötürü tazminat hakkını da içerecek şekilde işleme faaliyetine dair hakları ve bu hakları kullanma yöntemlerine ilişkin bilgi verilmesi gerekmektedir. Yine (d), (e) ve (f) bentlerinde gönderme yapılan maddeler öncelikli olmak üzere bağlayıcı şirket kurallarına dair bilgilerin m.13 ve 14'e ilave olarak veri ilgililerine ne şekilde temin edildiği hususunda bilgi verilmelidir[230].

Türk hukukunda Kurul tarafından 10.04.2020'de yayınlanan duyuruya göre, Türkiye'de yerleşik şirket grubunun Kurul'a bağlayıcı şirket kurallarına ilişkin yaptığı başvurunun Kurul tarafından onaylanması durumunda Kurum bunu ilgilisine bildirir, gerekirse de ilan edilir.

C.Kişisel Verileri Koruma Kurulu

Kurum'un 10.04.2020 tarihli duyurusu uyarınca, kişisel verilerin yurtdışına aktarımına ilişkin taahhütnamelerin, çoğu zaman şirketlerin arasında yapılacak iki taraflı veri aktarımlarını kolaylaştırsa da birden fazla devlette yerleşik şirket toplulukları arasında gerçekleştirilecek veri aktarımları açısından uygulamayı temin etmekte yetersiz kalabildiği ifade edilmiş; bu sebeple Kurulca bu tür şirketler arasında yapılacak uluslararası veri aktarımlarında kullanılacak bir usul olmak üzere bağlayıcı şirket kurallarının belirlendiği açıklanmış ve sonrasında bu kavrama dair bir tanım getirilmiştir.

Kurul'un yaptığı tanım uyarınca; bağlayıcı şirket kuralları, yeterli korumanın olmadığı devletlerde işlem yapan ve eylemde bulunan çok uluslu grup şirketler için kişisel verilerin yurt dışına aktarılmasında yeterli bir korumanın yazılı şekilde taahhüt

[230] Dülger, Makale, s.6.

edilmesini temin eden veri koruma kurallarıdır. Bu tanımın içeriğine giren şirketler, Kurum tarafından yayınlanan formu doldurup, yönergeleri takip ederek Kurul'a bağlayıcı şirket kuralları başvurusu yapmalıdır (KVKK m.9/2(b))[231].

III. BAĞLAYICI ŞİRKET KURALLARINDA BULUNMASI GEREKEN ASGARİ HUSUSLAR

A.Bağlayıcılık Unsurunun Sağlanması

Bağlayıcı şirket kurallarında bağlayıcılık, bu kuralları hazırlayan grup şirket ya da ekonomik ortak girişimin bütün üyelerine ve işçilerine tebliğ edilecek emir ve yönergelerle temin edilmektedir. Bu zincir sisteminin ne şekilde oluşturulacağı hususunda ise şirket özgür kılınmıştır. İç ve dış bağlayıcılık, bağlayıcı şirket kurallarının geçerli olması için bulunması gereken unsurlardandır (Regülasyon m. 47/2-c). Bununla birlikte, Regülasyon, iç ve dış bağlayıcılık kavramını açıklamamaktadır. KVKK da Regülasyon'da yer alan iç ve dış bağlayıcılık, paralelinde bir düzenleme içermektedir. KVKK'nın gerekçesinde yer aldığı üzere, KVKK'nın getirilme amaçlarından biri de AB hukukuna uyum sağlanmasıdır. Buna karşın Kanun tasarısı hazırlanırken örnek alınan mülga 95/46 sayılı AB Direktifi ile KVKK arasında uyumsuzluklar bulunduğu görülmektedir[232]. Öte yandan, Regülasyon'un yürürlüğe konulmasıyla AB hukuku ve tüm dünya, veri koruma hukukunda farklı bir hukuki düzenlemeyle karşılaşmıştır. Kaldı ki Kurul, birçok kararında, doğru olarak Regülasyon'daki düzenlemeleri göz önüne almaktadır. Bu manada KVKK'ndaki veri koruma ilkeleri, Regülasyon'un koruma düzeyine yükseltilmeye çalışılmaktadır. Bağlayıcı şirket kurallarının düzenlendiği Regülasyon ile bu uyumun yakalanması, Türk veri koruma hukukuna önemli katkılar sağlayacaktır[233].

---

[231] Kurul bununla birlikte "Veri Sorumluları İçin Bağlayıcı Şirket Kuralları Başvuru Formu" ve "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman" yayımlanmıştır; Çabuk, s.104.

[232] Kama Işık, Sezen, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış: 2016/679 Sayılı GVKT ile 6698 Sayılı KVKK'nın Detaylı Analiz ve Karşılaştırması, 1. Basım, On İki Levha Yayıncılık, İstanbul, Türkiye 2020, s.357.

[233] Kama Işık, s.358.

İç bağlayıcılık, grup şirketin bütün üyeleri ve işçileri için hukuki olarak geçerli ve kanıtlanabilir şekilde bağlayıcı bir biçimde kuralların düzenlenmesi manasına gelmektedir[234]. Bağlayıcı şirket kuralları formunda bu kıstasın hangi belge ve ne tür usullerle sağlandığına dair bilgi talep edilmektedir. Bağlayıcı şirket kurallarının Grup şirket içerisinde bağlayıcı niteliğinin başvuru formunda açıklanması zorunludur. Bu zorunluluk kapsamında;

- Gruptaki tüm üyeler için hukuki olarak geçerli ve kanıtlanabilir bir ya da daha fazla usul ile kuralların bağlayıcılığı sağlanmalı,
- İşçiler üstünde bağlayıcılığın temin edilmesi için iş sözleşmesi, gizlilik sözleşmesi, etik ilkeler, iç yönergeler gibi usullerden bir veya bir kaçı kullanılmalı,
- Hukuken bağlayıcılığın sağlanması için bağlayıcı şirket kurallarına uyma konusunda işçileri de kapsayacak şekilde bütün grup üyelerine yönelik açık bir yükümlülük konulmalıdır.

Dış bağlayıcılık unsuru, ilgili kişi bünyesinde kuralların bağlayıcılığı anlamına gelmektedir. İlgili kişinin haklarını kullanabilmesi ve bağlayıcı şirket kurallarına aykırı davranıldığına ilişkin iddiaları için şikâyet olanağı tanınmalıdır.

Bağlayıcı şirket kuralları, KVKK'nun ilgili kişiye verdiği tüm haklara ilave olarak, diğer taahhütleri de bünyesinde barındırmalıdır. Verilerin yurtdışında kurulu grup şirket üyeleri tarafından işlenmesinden kaynaklanan bazı konularda da taahhüt verilmelidir. Diğer bir önemli husus da, grup şirket üyeleri dışında, veri işleyen üçüncü kişiler ile yapılacak sözleşmelere ilişkindir. Üçüncü kişilerle yapılacak bu hizmet akitleri, bağlayıcı şirket kurallarında yer alan taahhütleri kapsamak zorundadır.

Bağlayıcılığa ilişkin bir diğer ehemmiyetli konu; yabancı ülkede kurulu grup şirket üyelerinin bağlı oldukları ulusal düzenlemelerde bulunan veri koruma hükümleriyle ilgilidir. Ulusal düzenlemelerde bağlayıcı şirket kurallarında verilen taahhütlere aykırı hükümlerin tespit edilmesi ve Kurum'un haberdar edilmesi gerekir. Bununla birlikte, bağlayıcı şirket kurallarının uygulanması açısından geçerli olan yasal düzenlemelerin KVKK olduğu açık şekilde belirtilmeli ve Kurul, yetkili makam olarak tayin edilmelidir.

[234] Toparlak, s.54, 105.

Bağlayıcı şirket kurallarında, üçüncü ülkelerin iç mevzuatından kaynaklanabilecek, idari denetim otoritelerinin denetim yetkisine ilişkin bir istisna yer almaktadır. Bahse konu istisna, "*her halükârda demokratik bir devlet düzenlemesinin gereklerini aşmayacak şekilde*" ibaresiyle, belirsiz bir şekilde hüküm altına alınmıştır. Bu konu, bilhassa *Schrems II* kararıyla konulan kriterlerden sonra, AB standartları için fazla muğlak olacaktır.

*Schrems II (*C-311/18*)* esas olarak AB ile ABD arasında gerçekleşen kişisel veri aktarımında uygulanan Gizlilik Kalkanı'na *(Privacy Shield)* dair bir karardır. Fakat karar, üçüncü ülkelere AB'den veri aktarımı amacıyla uygun bir güvenlik tedbiri olan standart veri koruma hükümlerine ilişkin de tespitler içermektedir. Kararda uygun güvenlik tedbirleri için konulan kriterlerin genel niteliğine bakıldığında, bu kararın bir başka güvenlik tedbiri olan bağlayıcı şirket kuralları açısından da geçerli sayılacağını söylemek olanaklıdır[235].

Schrems II kararında ABAD, "*veri aktarımının yapıldığı ülkede yeterli bir veri koruma güvenlik seviyesinin bulunması*" terimini, AB vatandaşlarının AB içerisinde kendilerine sağlanan hak ve olanaklardan, verilerin aktarımının yapıldığı üçüncü ülkede de aynı kolaylıkta ve şekilde faydalanabilmeleri şeklinde yorumlamıştır. Bu kıstas ABAD'ın uluslararası veri aktarımına dair önceki kararları ile de tutarlıdır.Bu nedenle yeterli bir güvenlik seviyesinin belirlenmesi; üçüncü ülkenin aldığı uygun güvenlik tedbirleri, ilgili kişilere tanınan ve kullanabilecekleri haklar ile yasal olanaklar çerçevesinde yapılmaktadır. Değerlendirmede dikkate alınan diğer iki önemli kıstas ise, verilerin aktarımının yapıldığı ülkedeki devlet idaresinin, aktarımı yapılan verilere erişimini temin eden iç hukuk kuralları bulunup bulunmadığı ve hukuk sisteminin genel görünümüdür[236].

Bağlayıcılık kavramına dair son konu ise tazminat taleplerine dairdir. Grup şirketin ülkemizdeki merkezi ya da ülkemizde kurulu yetkilendirilmiş üyesi veyahut aktarım yapan veri sorumlusu, bağlayıcı şirket kurallarının ihlali nedeniyle doğabilecek tazminat ödemelerini ve aykırılığın tazmini yükümlülüklerini uygulamayı kabul etmelidir. Grup şirketin uyguladığı politikalar kapsamında, yükümlülüğün tek

[235] Toparlak, s.34.
[236] C-311/18, bkz.;
https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, E.T.:10.07.2021.

bir üye şirket tarafından yüklenilmesi olanaklı değilse, yurtdışında bulunan üye şirket bünyesinde oluşabilecek aykırılıklarda üye şirketin bireysel sorumluluğu olduğu hükmü getirilebilir. Bu olasılığın, bilhassa merkezi yurtdışında olan grup şirketler açısından tercih edilebildiği görülmektedir[237].

B.Etkili Uygulamanın Sağlanması

Bağlayıcı şirket kurallarının geçerli olması için etkili bir şekilde uygulanması temin edilmelidir. Kurum, yayımladığı yardımcı dokümanda etkili uygulama yapılabilmesi için yararlanılabilecek metotlar öngörmüştür. Bu doküman uyarınca, veri sorumlusu bilhassa kişisel verileri aktaran veya işleyen çalışanlar için, eğitim ve farkındalık çalışmaları yapmalıdır. Bununla birlikte, istem durumunda Kurum'a verilmek üzere yapılan çalışmaların kayıtları da elde tutulmalıdır.

İlgili kişilerin haklarını etkin bir şekilde kullanabilmeleri için etkili uygulama yapılması önemlidir. Bu bağlamda bağlayıcı şirket kuralları içinde etkin bir şikâyet usulü getirilmelidir. Şikâyet yöntemi, net ve anlaşılır şekilde açıklanmalı ve şikâyetleri sonuçlandırma süreleri ile usulleri saptanmalıdır. Bahse konu başvuru sistemi oluşturulurken, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[238] ile getirilen sorumluluklar icra edilmeli ve Tebliğin de getirdiği biçimde bir başvuru sistemi teşekkül ettirilmelidir. Bu çerçevede, AB hukuku kapsamında etkin uygulama kıstası, Türk vatandaşları bakımından KVKK'ndaki hak ve olanakların, verilerin aktarımının yapıldığı üçüncü ülkelerde de benzeri şekilde kolayca kullanılabilmesi gerekmektedir.

Kurum'un etkili uygulama bakımından koyduğu bir diğer kıstas ise, bağlayıcı şirket kuralları içinde uyum ve denetim aşamalarının getirilmesidir. Grup şirket içinde bağlayıcı şirket kurallarının yerine getirildiğine dair denetimin, kimin tarafından yerine getirileceği tespit edilmelidir. Bununla birlikte denetimin hangi sürelerle ve ne tür usuller kullanılarak yapılacağı da yer almalıdır. Bu manada bağlayıcı şirket kuralları için görevli bir personel de belirlenmelidir[239].

[237] Toparlak, s.106.
[238] Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ, bkz. https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-6.htm, E.T.: 09.07.2021.
[239] Toparlak, s.106-107.

C.Kişisel Verilerin İşlenmesi ve Aktarılması Sürecinin Açıklanması

Bağlayıcı şirket kuralları çerçevesinde geçekleştirilecek veri işlemenin KVKK'na uygunluğunu temin etmek için Kurum, bazı taahhütlerin olmasını şart koşmaktadır. Öncelikle konulan kuralların kapsamı ve yapılacak aktarımlar genel olsa da tanımlanmalıdır. Kişisel verilerin işlenmesine ilişkin taahhütler yapılırken, Kurum'un aydınlatma yükümlülüğüne dair tebliğinden faydalanılabilir[240]. Kişisel verilerin özelliği, bölümleri ve veri konusu kişi grubu tespit edilmelidir. Bununla birlikte, grup şirket içinde bağlayıcı şirket kurallarına istinaden gerçekleştirilecek aktarım süreçleri de belirlenmeli ve açıklanmalıdır. Veri aktarımlarının hangi usulde, hangi aralıklarda yapılacağı ve verilerin grup şirket içinde dağılımı şeklinde bilgiler yer almalıdır.

Bağlayıcı şirket kurallarında grup şirket içinde gerçekleştirilen veri aktarımlarının üçüncü kişilere ileri aktarımı (onward transfer) kavramı da yer almalıdır. Örneğin bağlayıcı şirket kurallarının, ileri aktarımlarda da kullanılacağı ve geçerli olacağı taahhüt edilmelidir. Hatta bağlayıcı şirket kurallarının veri güvenliğine dair bölümünde sunulacak taahhütlerin, ileri aktarımlarda da geçerli olduğu hususu aranmaktadır.

Veri aktarım sürecinde şeffaflığı gösterebilmek için grup şirket yapısı açık şekilde ortaya konulmalıdır. Bu manada KVKK'ndaki grup şirketin bütününde veri sorumlusu temsilcisi görevini yerine getirebilmesi için bir irtibat kişisi belirlenmelidir. Bu irtibat kişisi, bağlayıcı şirket kurallarını taahhüt eden şirketler topluluğu üyelerinin mevcut iletişim bilgilerine sahip olmalı ve herhangi değişiklik durumunda Kurum'u ve ilgisi olan kişileri bilgilendirmelidir[241].

D.Kurum ile Koordinasyonun Sağlanması

Bağlayıcı şirket kuralları içinde Kurum ile koordinasyonun ne şekilde yapılacağı yer almalıdır.

Buna ilave olarak grup şirketin, bir hususta Kurum'un tavsiyelerini uygulamayı kabulüne dair bir yükümlülük de düzenlenmelidir. Ancak içeriği kesin ve açık olarak

[240] Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ, bkz. https://kvkk.gov.tr/ıcerik/5443/aydınlatma-yukumlulugunun-yerınegetırılmesınde-uyulacak-usul-ve-esaslar-hakkında-teblıg, E.T.: 09.07.2021.
[241] Toparlak, s.106.

tespit edilemeyen bu yükümlülük, bilhassa merkezi yabancı ülkede olan grup şirketler açısından sorun yaratabilecektir.

ABAD, *Schrems II* kararının akabinde, AB dışına veri aktarmalarında üçüncü ülkede tahmin edilemeyen devlet müdahalesini en asgari seviyeye indirmeye çabalamaktadır[242]. Örneğin verileri AB'den aktaran kişinin; veri aktarımının yapıldığı üçüncü ülkedeki kamu makamlarının denetleme yetkisine ilişkin iç hukuk incelemesi yapması zorunludur. Bu açıdan üçüncü ülkedeki kişi, bağlı olduğu iç hukuk kuralları sebebiyle standart veri koruma maddelerine uyamayacağını ifade edebilmektedir. Araştırma neticesinde, her iki tarafın standart veri koruma gereklerini ifa edemeyecekleri tespit edilirse, AB'deki veri sorumlusunun, veri aktarımını durdurması veya sözleşmeyi feshetmesi gereklidir[243].

Akit taraflar için getirilen bu yükümlülüklerin yanı sıra verinin aktarımının yapıldığı üçüncü ülkedeki veri koruma makamı açısından da yükümlülükler öngörülmelidir. Çünkü bu veri koruma makamlarının da denetim yükümlülüğü bulunmaktadır. Bu veri koruma otoriterleri, veri aktarımının denetimini yaparken üçüncü ülkede hem devlet yönetiminin erişimini, hem de başkaca bir gerekçeyle standart veri koruma hükümlerinin işlemediğini ve korumanın yapılamadığını belirlerse, veri aktarımını durdurabilir ya da yasaklayabilir. ABAD kararlarında da AB'deki veri koruma makamlarının veri aktarım sürecine katılmaları daha güçlü hale getirilmiştir. Kaldı ki, uygun güvenlik tedbiri kavramı gereğince verilen taahhütlerle ulusal düzenlemelerin birbirine aykırı olması halinde, AB hukukuna üstünlük verilmesi gerektiği belirtilmektedir[244].

Kanaatimizce, kendisi ile koordinasyonun sağlanması hususunda Kurum, Schrems II kararındaki gibi daha somut kriterler veya hükümler getirmelidir. Örneğin, grup şirket içinde veri aktarımı yapılması halinde, aktarımın yapıldığı diğer şirketin bulunduğu ülkedeki devlet yönetiminin, aktarımı yapılan bu verilere erişimini temin eden iç hukuk kuralları bulunup bulunmadığının ve hukuk sisteminin genel görünümünün Kurum'a bildirilmesi gibi bir koşul getirilmesi, Regülasyonun içeriği ile daha uyumlu olacaktır.

[242] Toparlak, s.107.
[243] C-311/18, p.134, 135, 140.
[244] C-311/18, p.107, 108, 113,114.

E.Raporlama ve Kayıt Değişikliği Mekanizmalarının Belirlenmesi

Bağlayıcı şirket kurallarının niteliklerine bakıldığında, grup şirketin gereksinimleri ve yapısındaki değişiklikler gereğince farklılaştırılabilir ve güncel hale getirilebilir kurallar olduğu görülmektedir. Gerçekleştirilecek bu değişikliklerin, gecikme yaşanmaksızın Kurum'a ve çok uluslu şirket üyelerine gönderileceği taahhüdü verilmelidir. Bu değişikliklerin Kurum'a bildirilmesine ilişkin getirilen süre, değişikliğin özelliğine göre değişmektedir. Bağlayıcı şirket kurallarının koruma düzeyine etki eden ya da başka bir sebeple esaslı kabul edilen değişiklikler, Kurum'a hemen bildirilmelidir.

Bağlayıcı şirket kurallarının uygulanmasına etki etmeyecek ve tamamen idari değişiklikler gibi durumlar dışında ilgili kişinin haklarını zarara uğratabilecek ya da veri güvenliğine önemli şekilde etki edecek değişikliklerden de daha önceden Kurum'a bilgi verilmesi zorunludur. Bağlayıcı şirket kurallarında esaslı kabul edilmeyecek başka değişikliklerin ise, yapılacak açıklamalarla beraber Kurum'a yıllık şekilde bilgi verileceği taahhüt edilmelidir. Kurumla iletişimin temin edilmesi ve bahse konu raporlamanın yapılması için yetkili bir kişi atanmalıdır[245].

Bu bağlamda grup şirketin bu çeşit değişiklikleri bildirmek ve kaydını tutmak için bağlayıcı şirket kuralları metninde grubun üyeleri açısından oluşabilecek değişikliklerden, başka grup üyelerine ve Kurum'a nasıl bildirimde bulunulacağına dair usulleri oluşturmaları gerekmektedir. Bununla birlikte, bağlayıcı şirket kuralları metni ve uygulanmasında oluşacak tüm değişiklikleri kayıt altına alacak bir sistemin kurulması gerekmektedir[246].

F.Veri Güvenliğinin Sağlanması

Kurul'un duyurusu uyarınca, bağlayıcı şirket kuralları içeriğine girebilecek kişisel veriler kısıtlanabilmektedir. Bu kurallarda taahhüt edilmesi gereken veri

[245] Veri sorumluları için bağlayıcı şirket kuralları başvuru formu, bkz: https://www.kvkk.gov.tr/ıcerik/6728/yurt-dısına-kısısel-verı-aktarımında-baglayıcı-sırket-kuralları-hakkında-duyuru, E.T.:10.7.2021.
[246] Toparlak, s.108.

koruma ilkeleri, sadece Türkiye'den gerçekleştirilen aktarımlar veya ileri aktarımları kapsayacak şekilde düzenlenebilmektedir[247].

1.Yapılacak Tüm Kişisel Veri Aktarımlarını Kapsar Biçimde Veri Koruma İlkelerine Dair Bir Açıklama

Kurul duyurusunda, bağlayıcı şirket kurallarının içeriğine girecek kişisel verilere ilişkin açıklamadaki belirsizlik sebebiyle, sınırlama imkânından elde edilecek amaç anlaşılamamaktadır. Bu kurallar, sadece ileri aktarımlara ilişkin taahhüt barındıran, pratik şekilde uygulanabilir kurallar olmayacaktır. Duyurudan görülebildiği gibi, bu kurallar çerçevesinde veri koruma ilkelerine ilişkin yapılacak taahhüt, Türkiye'den gerçekleştirilecek aktarımlarla kısıtlanabilmektedir. Fakat bu kurallar çerçevesinde korunma altında olan verilere ilişkin ileri aktarımlarda da KVKK m.9'a göre getirilen uygun ve yeterli güvenlik tedbirlerinden birinin varlığı aranmaktadır.

Veri koruma ilkeleri kapsamında sunulacak taahhütte, KVKK m. 4/2/a ila m.4/2-d arasındaki düzenlemelerde yer alan hükümler de dikkate almalıdır. Bahse konu taahhütlerin işlenme amacıyla bağlı ve sınırlı olma ilkesinin bir gereği olarak, "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik*"[248] de burada önemli görülmektedir[249]. Veri güvenliğinin sağlanması amacıyla hazırlanacak taahhütlere dair Kurum'un yayımladığı rehberden yararlanılabilir[250]. Öte yandan, hassas kişisel veriler işlenirken, KVKK'nın aradığı ek yükümlülüklerin de taahhüt edilmesi gerekmektedir[251].

---

[247] Dülger, 2019, s.405; Çekin, 2020, s.221.

[248] Yönetmelik metni için bkz. https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm, E.T.:10.07.2021.

[249] Toparlak, s.109.

[250] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesine İlişkin Rehberi, Sage Matbaacılık, Ankara, 2017, bkz: https://www.kvkk.gov.tr/yayinlar/kişisel%20verilerin%20silinmesi,%20yok%20edilmesi%20veya%20anonim%20hale%20getirilmesi%20rehberi.pdf, E.T.:10.07.2021.

[251] Kurul Kararı, 31/01/2018 tarih ve 2018/10 sayılı, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler", bkz. https://www.kvkk.gov.tr/Icerik/2051/Ozel-Nitelikli-Kisisel-Veriler, E.T.:10.7.2021.

2.Teknik ve İdari Önlemler

Bağlayıcı şirket kuralları kapsamında veri güvenliğine dair alınacak teknik ve idari önlemlere ilişkin açık şekilde taahhüt verilmelidir. Bu önlemler saptanırken, Kurum'un bu önlemlere dair yayımladığı "*Veri Güvenliği Rehberi*"nden yararlanılabilecektir. Bu önlemler çerçevesinde, grup şirketin bir üyesinin bünyesinde yapılan bir kişisel veri ihlali durumunda, ülkemizdeki merkez ya da yetkili üyenin haberdar edilmesi gerekmektedir. Yapılan kişisel veri aktarım aykırılığına dair bildirim, ilgili veri koruma birimine ve ihlalden etkilenmesi olası şahsa da iletilir. Bu bildirim yükümlülüğü, bu kurallar kapsamında grup şirketler tarafından taahhüt edilmelidir.

Bağlayıcı şirket kuralları hazırlayacak grup şirket,veri güvenliğini düzenlerken kendi ağı içinde bulunan yabancı şirketlerin, bağlı oldukları yabancı ulusal düzenlemeleri de incelenmelidir. Yabancı ulusal düzenlemelerin grup şirket üyesini bağlayıcı şirket kurallarına uymasını men ettiği hallere dair şeffaflık sağlanmalıdır. Eğer yabancı ulusal düzenlemeler, bağlayıcı şirket kurallarına uyulmasını büyük ölçüde azaltıyorsa bu düzenlemeler hakkında, Türkiye'deki merkez ya da üye şirkete bilgi sunulacağı taahhüdü verilmelidir. Ayrıca Kurum'un da bu etkilenme halinden bilgilendirileceği de düzenlenmelidir.

Buna örnek olarak AB hukukunda, Regülasyon m.47/2'ye göre yabancı ulusal düzenlemelerle çatıştığı için uygulanamayacak bağlayıcı şirket kuralları yükümlülüklerinin olması durumunda, bu durumun AB'deki ortak sorumlu üyeye veya genel merkezin uyumluluk bölümüne bildirilmesi gerektiği hüküm altına alınmıştır. Fakat bağlayıcı şirket kuralları içeriğinde olan bu husus isteğe bağlı olarak şirketler tarafından düzenlenebilecektir. Bu ilişkinin bağlayıcı şirket kurallarında yer alması isteğe bağlı olarak ifade edilse de şirket bakımından da avantajlıdır. Bu şekilde olası bir çatışma durumunda grup şirketin izleyeceği usul açık olacaktır. İlave olarak bu düzenleme, şeffaflığı ve hesap verebilirliği de arttırmaktadır[252].

[252] Toparlak, s.109-110.

G. Hesap Verebilirlik ve Şeffaflığın Sağlanması

Grup şirketin veri sorumlusu üyesi, bağlayıcı şirket kurallarına uyumu gerçekleştirmekle yükümlüdür[253]. Bu sorumluluğun icra edilebilmesi amacıyla bütün veri işleme kategorilerinin kaydı tutulmalı ve istenmesi durumunda Kurum'a sunulmalıdır.

Daha öncede ifade edildiği üzere hesap verebilirlik, KVKK içinde açık bir şekilde yer almış bir veri koruma ilkesi değildir[254]. Bu nedenle içeriği ve kapsamı Kurum duyurusu ile tespit edilen bağlayıcı şirket kurallarına dahil edilmesi gerektiği ifade edilmiştir[255].

Hesap verebilirlik, KVKK'da bağımsız bir ilke şeklinde yer almasa da hesap verebilirliğin temini için bazı araçlara atıf yapılmıştır. Hesap verebilirlik, veri sorumlularının KVKK m.12'de yer alan veri güvenliğine dair sorumlulukları yerine getirmeleri anlamına da gelmektedir. Bu nedenle hesap verebilirliğin sağlanması için öngörülecek araçların, Kurul duyurusunda hesap verilebilirlik başlığıyla gösterilmesinin Kanun'un amacına da uygun olduğu söylenebilir.

Bağlayıcı şirket kurallarının önemli yararlarından biri de KVKK m. 12 düzenlenen veri güvenliği yükümlülüklerine ilişkin hesap verebilirliği arttırması ve kanıt şeklinde kullanılabilmesidir. Bu kurallar içerisinde hesap verebilirliğin arttırılması için, veri ilgisi şahısların hak ve hürriyetleri üstünde yüksek riske sahip veri işleme eylemleri hakkında risk analizi yapılması taahhüdü verilmelidir. Yapılacak risk analizi kapsamında, riski asgari düzeye azaltmak için gereken tedbirlerin alınacağı ve yüksek risk durumunda, veri işleme eylemlerinden Kurum'un haberdar edilmesi gerektiği hükmü getirilmelidir.

KVKK m.12 haricinde, m.15/3 uyarınca Kurul'un yaptığı incelemede, veri sorumlusu, inceleme konusuna ilişkin Kurul'un istediği bilgi ve dökümanları on beş gün içerisinde Kurul'a sunmak ve gerekirse Kurul'a belgelerin bulunduğu yerde inceleme yapmasına olanak tanımak zorundadır. Bu bağlamda bu kuralların Türk hukukunda ispat kolaylığı sağladığı görülmektedir.

---

[253] Dülger, 2019, s.405 vd.
[254] Regülasyon, md. 5/2 uyarınca veri sorumluları, veri işleme ilkelerine uyulduğuna dair hesap verebilirliği sağlamakla yükümlüdürler, bkz. Dülger, 2019, s.139.
[255] Toparlak, s.110.

Öte yandan, doktrinde kişisel verilerin işlenmesinde KVKK m. 4/2-c, ilgili kişinin haklarının yer aldığı m.11 ile veri sorumlusunun aydınlatma yükümlülüğünün düzenlendiği m.10'da şeffaflık ilkesi ve buna bağlı koruma mekanizmasına yer verildiği belirtilmiştir[256]. Ancak bu maddelere bakıldığında şeffaflık ilkesinin, veri koruma ilkesi olarak dolaylı şekilde KVKK içinde yer aldığı görülmektedir. Kurumun yayınladığı duyuruda bu kuralların, grup şirketler tarafından etkili bir şekilde uygulaması olduğu ve etkili uygulamayı sağlayacak uyumluluk denetimi içinde raporlamanın şeffaf bir şekilde yapılmasının gerektiği belirtilmiştir. Bu kuralları uygulayacak grup şirketin uygulayacağı uyumluluk denetim programı hakkında, düzenli şekilde denetime tabi tutulması ve bu denetimi kimlerin gerçekleştireceği gibi konularda da açıklamaların, düzeltici faaliyetlerin gerçekleşmesini sağlayacak yöntemlerin bağlayıcı kurallar içerisinde açıklanmış olması gerekir.

Kurum duyurusunda, bir bağlayıcı şirket kuralları üyesinin uyması gereken hükümlerde, şirketin bağlayıcı şirket kurallarındaki yükümlülüklerini icra etmesini önleyen ya da bu kurallar ile getirilen hükümlerin tatbik edilmesine ciddi oranda etki eden düzenlemeler varsa, hemen grubun ülkemizde yerleşik merkezi ya da bu yoksa kişisel verilerin korunması hususunda yetkili kıldığı ve ülkemizde kurulu bir grup üyesinin bilgilendirilmesinin şeffaflık ilkesi kapsamında olduğunu kabul etmiştir.

Regülasyon m. 5/2 gereğince veri sorumluları, veri işleme ilkelerinin yerine getirildiğine ilişkin hesap verebilirliği sağlamakla sorumludurlar. Bağlayıcı şirket kurallarının önemli hedeflerinden biri, grup şirket içerisinde hesap verebilirliği sağlamak ve kanıtlayabilmektir. Bu manada bu kuralların getirdiği en önemli yararlardan biri de kanunla uyumu *(compliance)* göstermektir. Hukuk muhakemesi kurallarına göre veya idari yargılama usulünde bağlayıcı şirket kuralları, geçerli bir kanıt aracı kabul edilmektedir.

Bu hükümler; gizlilik ve veri koruması gerekliliklerine ilişkin şirket içinde anlayış ve duyarlılığı artırmaktadır. Çünkü bağlayıcı şirket kuralları, şirket içinde veri korumasını yapabilecek ayrı bir kısmın oluşturulmasını ve gizliliğin şirket değerlerinde sürekli şekilde var olması ve korunmasını gerektirmektedir[257].

[256] Çekin, 2020, s.81.
[257] Toparlak, s.46.

Bu kapsamda olası ihlaller neticesinde, veri sorumlusu aleyhinde verilebilecek idari para cezaları da azalmaktadır. Bağlayıcı şirket kuralları, ayrıntılı ve çalışır bir veri koruma değerleri veya kültürünün oluşturulması için, şirket içerisinde aşağıda gösterilenler gibi detaylı yöntemler getirmektedir:

a. Veri koruması uyum projesinin izlenmesi ve kontrolü amacıyla ayrı bir yönetim bölümünün oluşturulması,

b. Verinin hukuka uygun şekilde işlenmesini temin etmek üzere şirket içi talimatlar meydana getirilmesi,

c. Şeffaflığın sağlanması için veri ilgilisine yeterli bilginin verilmesi ve bildirimlerin gerçekleştirilmesi,

d. Uyum projesi kapsamında ve veri işleme aşamalarında risk değerlendirmesi ve yönetiminin yapılması,

e. Verileri işleyen kişilere, düzenli bilgilendirme verilmesi ve eğitimlerden geçirilmesi,

f. Yapılacak iç ve dış teftişlerle, veri koruma kurallarına uyulup uyulmadığının (compliance) denetiminin yapılması,

g. Veri sahibi kişilerin istemlerine mümkün olduğunca hızlı ve yeterli biçimde dönülmesi için gereken idari kısımların oluşturulması[258].

H. Yardımcı Bilgi ve Belgeler

Kurumca yayımlanan yardımcı rehberde bağlayıcı şirket kurallarının içerisine alınması zorunlu görülmeyen yardımcı belgeler gösterilmiştir. Rehberde, veri aktarımının gerçekleştirileceği ülkelerin taraf olduğu kişisel verilerin korunmasına dair uluslararası sözleşmelere ilişkin bilgi verilmesinin faydalı olacağı belirtilmiştir. Benzer biçimde verinin aktarılacağı ülkede, ulusal mevzuat ve veri koruma makamının bulunup bulunmadığına ilişkin bilgi verilmesi de isteğe bağlı olarak gösterilmiştir.

IV. KURUL BAŞVURUSUNA İLİŞKİN USUL VE ESASLAR

Yaptığı duyuruda Kurul, var olan yurt dışına veri aktarım yollarının birden çok ülkede faaliyet gösteren şirket toplulukları arasında gerçekleştirilecek veri aktarımları

[258] Toparlak, s.46.

açısından uygulamada yetersiz olabildiğini; bu sebeple de bağlayıcı şirket kurallarının kabul edildiğini ifade etmiştir.

A.Başvuru Yapma Yetkisi

Grup şirketin Türkiye'de kurulu merkezi varsa bu yer yetkilidir. Grup şirketin Türkiye'de kurulu merkezi yoksa Türkiye'de yerleşik bir grup üyesi kişisel verilerin korunması hususunda yetkilendirilecek üye tarafından başvuru yapılmalıdır[259]. Bu halde, grup namına başvuru yapma yetkisine bu üye sahiptir. Yetkilendirilecek kişinin Grup Şirkete bağlı bir şirket veya ortak girişimde bir karar mekanizması var olan gruptaki veri sorumlularından herhangi birisinin olması mümkündür.

B. Başvuru Yöntemi

Bağlayıcı şirket kuralları ve başvuruya dair başka bütün bilgi ve belgeler Kurul'a elden ya da posta aracılığıyla sunulmalıdır.

C.Başvuruda Sunulacak Bilgi ve Belgeler

Başvuruda verilecek bilgi ve belgeler; başvuru formu, Bağlayıcı Şirket Kuralları'nın yazılı hali ve başvuruya dair diğer bütün bilgi ve belgelerdir. Bağlayıcı şirket kuralları metninin bir asıl sureti ek yapılmalıdır. Kurum tarafından yayımlanan "Başvuru Formu"na göre; veri sorumlusu/işleyen sıfatıyla grup üyesi şirketin ismi/unvanı, genel merkezinin adresi ve genel merkezi Türkiye'de değilse Türkiye'de kurulu grup üyesinin adresinin yazılması gerekmektedir. Başvuru işlemini yapan kişi bakımından, başvurucu kişinin adı/unvanı, TC kimlik numarası, başvurucunun hukuki statüsü, irtibat kişisinin adı veya birimi, irtibat kişisinin adres, telefon numarası, elektronik posta adresi gibi bilgiler formda yer almalıdır[260].

Ayrıca başvuru formunda; veri aktarımının gerçekleştirileceği ülke ve bu kuralların dahil edildiği bütün grup üyeleri ile iletişim bilgileri yer almalıdır.

Bağlayıcı Şirket Kuralları başvuru formunda, ilk bölümdeki başvurucu bilgilerinden sonra ikinci bölümde sekiz soru başlığı altında değerlendirme kriterleri yer almaktadır. "Bağlayıcı Şirket Kurallarına Yönelik Bilgiler" başlıklı ikinci

[259] Dülger, Makale, s.6.

[260] Bağlayıcı Şirket Kuralları Hakkında Duyuru, bkz. https://www.kvkk.gov.tr/ıcerik/6728/yurt-dısınakısısel- verı-aktarımında-baglayıcı-sırket-kuralları-hakkında-duyuru, Erişim Tarihi: 10.07.2021

bölümdeki ilk sorular, hazırlanan yapının iç ve dış bağlayıcılık unsuruna dair sorulardır. Usulüne uygun bir bağlayıcı şirket kuralları başvurusu yapılabilmesi ve bu başvurunun uygun bulunabilmesi için bu kuralların ulusal düzenlemelere uygun şekilde, bütün grup şirket üyelerini bağlayıcı bir etkiye sahip olması gerektiği belirtilmiştir. "A.Bağlayıcılık Unsuru" adı verilen bu bölümde düzenlenen sorular, bahse konu bağlayıcılık unsurunun grup şirketleri, çalışanlar ve veri işleyenler bakımında bulunup bulunmadığının saptanmasını sağlamaktadır.

"B. Etkili Uygulama" başlığında düzenlenen ise bağlayıcı şirket kurallarının etkin uygulanmasına ilişkin olup, bu kuralların grup tarafından etkili şekilde uygulanması için önemli olduğu belirtilmiştir. Bu kısımda etkin bir uygulama sağlanması amacıyla grup şirket içinde ne tür sistemlerin ne şekilde kullanıldığına dair sorular bulunmaktadır. Örneğin, çalışanlara yapılan eğitim ve farkındalık çalışmaları, şikayet mekanizmaları, bu kurallara uyumluluk denetimleri ve bağlayıcı şirket kurallarının uygulanması konusunda personel görevlendirilmesine ilişkin sorular yer almıştır.

Üçüncü başlıkta ise, Kurum ile işbirliği ve iletişimin temini için kurulacak usullere dair sorular sorulmaktadır. Dördüncü soru ise, bu kuralları hazırlayan grup şirket içindeki veri aktarımına dairdir. Bu başlıkta, aktarılacak veri kategorileri, verilerin genel veya hassas kişisel veri olup olmadığı, aktarma amaçları, verileri en fazla saklama süreleri, veriye konu kişi grubu ya da grupları, veri aktarımının gerçekleştirileceği yöntemler, veri aktarımının hukuki nedenleri, aktarımı yapılacak verilerin grup içindeki dağılımı gibi konulara ilişkin sorular sorulmakta ve grup içindeki veri işleme aşamalarının net ve anlaşılır olarak tanımlanması gerekmektedir[261].

Beşinci başlıkta, bu kurallarda veri ilgilisi kişilerin haklarına zarar verebilecek veya onları etkileyecek değişikliklerin Kurum'a bildirilmesi gerektiği ifade edilmiş ve bu kuralların metni ya da grubun üyeleri açısından oluşabilecek değişikliklerden başka grup üyeleri ve Kurum'un ne şekilde bilgilendirileceği ve bunların nasıl kayıt altına alınacağı soruları yöneltilmiştir. Altıncı soruda, veri güvenliğini temin etmek için alınan bütün teknik ve idari önlemlerin ayrıntılarıyla açıklanması, genel ilkelere uyumun nasıl sağlanacağı, hassas verilerin işlenmesinde Kurulca tespit edilen alınacak

[261] Toparlak, s.122.

yeterli önlemler, veri ihlal bildirimine süreçlerinin açıklanması talep edilmektedir. Bu kurallar içinde bu konuların ne şekilde hüküm altına alındığı, destekleyici belgelerle belirtilmelidir.

"Hesap Verebilirlik Ve Diğer Esaslar/Araçlar" adını taşıyan yedinci başlık altında grup şirket üyelerinin, bu kurallara ne şekilde uyum sağlayacağı ve bundan ne şekilde sorumlu tutulacağı açıklanmaktadır. Bununla birlikte, bu başlıkta düzenlenen önemli bir konu, grup üyesi her bir veri sorumlusunca bu kurallar çerçevesinde yapılacak veri işleme eylemlerinin kaydının ne şekilde tutulacağının açıklanmasının istenmesidir. Regülasyon'da düzenlenmeyen envanter veya kayıt tutma zorunluluğunun, bağlayıcı şirket kuralları içindeki grup şirket üyeleri açısından söz konusu olup olmayacağı sorunu ortaya çıkmaktadır. Bu manada Kurum'un yayınladığı yardımcı dokümanda sadece çok uluslu şirket üyelerinin bütün veri işleme eylemlerinin yazılı olarak kaydedilmesi ve istenmesi durumunda Kurum'a vermesi zorunluluğu belirtilmektedir. Formda son kısım aktarımın gerçekleştirileceği ülkelerin onayladığı kişisel verilerin korunmasına ilişkin uluslararası sözleşmeler ile grup şirket üyelerinin ulusal kişisel verileri koruma düzenlemelerine dairdir.

Kurum'a, AB hukukuna göre düzenlenmiş bir bağlayıcı şirket kurallarını taahhüt eden Türk üyenin, iletilecek metni tercüme ederek bu doküman ile grup namına bu kurallara ilişkin başvuru gerçekleştirmesi de olanaklı olabilecektir. Bu başvuruyu yapmadan önce, tercümesi yapılan metnin Kurum'un aradığı bütün konuları taahhüt etmesi gereklidir. Bu metin istenilen şartları taşıdığı takdirde, gerek AB'den Türkiye'ye gerekse Türkiye'den AB'ye, grup şirket üyeleri arasında gerçekleştirilecek veri aktarımları hukuka uygun olmuş olacaktır. Bu şekilde KVKK da Regülasyon ile uyumlu olmuş olacaktır. Sadece bu durum dahi bu kurallar gibi düzenlemelerin, uluslararası veri koruma kuralları açısından ehemmiyetini ortaya çıkarmaktadır[262].

D.Başvurunun Sonuçlandırılması

Kurum, başvuru tarihinden başlayarak bir yıl içinde değerlendirerek başvuruları sonuca bağlar. Gerektiği takdirde bu sürenin, altı aylık müddetlerle uzatılabilmesi

[262] Toparlak, s.123.

mümkündür. Başvuruya Kurul tarafından izin verilmesi durumunda, bu hâl, Kurumca ilgili kişiye bildirilir ve gerektiği takdirde ilan edilir. Bu kurallarda getirilmesi planlanan kolaylığın sağlanması bu süreler nedeni ile şimdiden uzun kontrol süreçleri içerisinde zor gözükmektedir. Uzun onay aşamalarına bir de bağlayıcı kuralların yapılması için hazırlık süreleri de ilave edildiğinde, hedeflenen işletmelerin uzunca bir süre daha KVKK m.9'daki muğlaklıklarla karşı karşıya bırakıldığı görülebilmektedir. Dolayısı ile bir kolaylık sağlamak üzere getirilen bu kurallar için daha kısa sürelerde verilecek bir onay mekanizması, bağlayıcı şirket kurallarının getirilme amacı ile uyumlu olacaktır. Ek olarak; Kurul tarafından yayımlanan Formda yer aldığı gibi, başvurusu onaylanan Gruplar, Kurum tarafından sadece "*gerekmesi*" durumunda yayınlanacaktır. Bu nedenle AB'ndekine benzer açık bir listenin Türkiye'deki uygulamada bulunmayacağı da bu hususta ayrıca anlaşılmaktadır.

V.BAĞLAYICI ŞİRKET KURALLARI KAPSAMINDA ŞİRKETİN SORUMLULUĞU

Türk hukukunda kişisel verilerin korunmasına ilişkin düzenlemeler, KVKK'nun haricinde birçok kanunda ve diğer düzenlemelerde yer almaktadır[263]. Dolayısıyla bağlayıcı şirket kuralları uyum sürecine ilişkin sadece KVKK değil tüm mevzuata da bakılmalıdır. Bununla birlikte, bağlayıcı şirket kuralları koyma taahhüdü veren Türkiye'deki üyenin, Türkiye'deki kişilerle ilişkilerini elbette özel hukuk kuralları düzenleyecektir. Bu çerçevede ortaya çıkabilecek hak ve yükümlülükler de unutulmamalıdır. Diğer bir deyişle, AB hukukunda ortaya çıkan bağlayıcı şirket kurallarını taahhüt eden Türk şirketinin, KVKK ve diğer mevzuat hükümlerinden kaynaklanabilecek sorumluluğunun da incelenmesi gerekecektir[264]. Ek olarak belirtmek gerekir ki; Madde 29 Çalışma Grubu'na göre[265], sorumlu tutulabilme ilkesinin özü, veri sorumlusunun aşağıda belirtilen borçlarıdır:

[263] Ayrıntılı bilgi için bkz. Kaya, Bedii, Kişisel Verileri Koruma Hukuku– Mevzuat ve İçtihat, 1. Basım, On İki Levha Yayıncılık, İstanbul, 2018.
[264] Toparlak, s.84.
[265] Madde 29 Çalışma Grubu, sorumlu tutulabilme prensibi hakkında 3/2010 sayılı Görüş, WP 173, Brüksel, 13 Temmuz 2010.

- olağan koşullar altında veri işleme eylemleri çerçevesinde veri koruma kurallarına uygun davranıldığını temin edecek tedbirleri almak,
- veri sahipleri ile denetim makamlarına veri koruma kurallarına uyumu temin etmek için uygulanan tedbirlerin yazılı olduğu belgeleri hazır tutmak.

Bu sebeple genel anlamda sorumlu tutulabilme ilkesi, veri sorumlularının bir yandan aktif şekilde uyum göstermesini diğer yandan veri sahiplerinin ya da denetleyici makamların eksiklikleri göstermeyi beklememesini gerektirmektedir.

A.Hukuki Sorumluluk

Veri sorumluları ve işleyenlerin sorumluluk durumları, KVKK'nun "Suçlar ve Kabahatler" başlıklı Beşinci Bölümünde yer almıştır. Burada elbette cezai yaptırımlar ve kabahat karşılığı idari para cezası uygulanmasına dair hükümlere yer verilmiştir. Avrupa Birliği düzenlemesinden (Regülasyon m.82) farklı olarak KVKK, kişisel verilerin hukuka aykırı şekilde işlenmesinden kaynaklanacak zararlardan sorumluluk bakımından özel bir hüküm içermemektir ve bu durumda özel hukukta tazminat yaptırımı ile koruma sağlanmıştır (m. 11). Bir kamu tüzel kişisinin eylemi neticesinde gerçekleşen zarar da, tam yargı davası ile talep edebilecektir[266]. Hukuka aykırı şekilde veri işlendiğini ileri süren ilgili kişilerin KVKK'nın yaptığı atıf ile maddi ve manevi tazminat ile önleme, durdurma ve tespit davalarından yararlanması olanaklıdır. Yani KVKK m.14/3 gereği, "*kişilik hakları ihlâl edilenlerin, genel hükümlere göre tazminat hakkı saklı*" olduğundan bahsi geçen TMK m. 24. ve 25. ile TBK m. 53, 54, 56 ve 58. hükümlerine göre tazminat hakkı ilgili kişi yönüyle mevcuttur.

Öte yandan, Regülasyon, veri sorumluları ve işleyenler arasında sorumluluk ilişkisinin olduğunu belirtse de, bu ilişkinin KVKK'nda açık olmadığı görülmektedir. Bağlayıcı şirket kurallarının KVKK'da açıkça düzenlenmediği gözetildiğinde aslında bu kurallar karşılığında bir cezai sorumluluk yüklenmesi hukuka aykırı olarak değerlendirilebilecek bir husustur. KVKK, idari para cezaları verilmesi hususunda neredeyse tüm sorumluluğu veri sorumlusuna vermiştir. Bir başkasının dahil

[266]Akgül, 2013, s:34; Kağıtçıoğlu, Mutlu, Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bakış, İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi, 1(2), 2016, s.80.

olabileceği müteselsil sorumluluk durumunda ise, veri sorumlusu ve işleyen arasındaki ilişkinin özelliği ve koşullarına dair bir düzenleme bulunmamaktadır[267].

1.Tazminat Sorumluluğu

Hukuka aykırı olarak kişisel verilerinin işlenmesi nedeniyle zarar gören ilgili kişi, "Haklar ve yükümlülükler" başlığını taşıyan KVKK m.11/1/ğ gereğince veri sorumlusuna müracaat ederek zararın tazminini isteme hakkına sahiptir. Bu maddeye ilave olarak KVKK m.14/3'te, kişilik hakkı zarara uğrayanların, genel hükümler uyarınca tazminat haklarının bulunduğu belirtilmiştir[268].

Mutlak ve herkese yönelik öne sürülebilen şahsa sıkı sıkıya bağlı[269] bir hak olan kişilik hakkı olarak kişisel verilere yönelen hukuka aykırı bir tecavüz TMK gereği haksız fiil olacaktır[270]. KVKK m.14/3'ün yönlendirmesi ile TMK'da yer alan m.24 hükmü uyarınca *"...kişilik haklarına yapılan her saldırı hukuka aykırıdır"*. Kişilik haklarına ayrılık hallerinde TMK m.24 ve devamı maddeleri ile, haksız fiilin gerçekleşmesi durumunda ise TBK m.49 ve devamı maddelerinin uygulanması[271] gerekecektir. Doktrinde, genel hükümler uyarınca kişisel verilerin hukuka aykırı işlenmesi ve aktarılması durumunda Türkiye'deki veri sorumlusuna yöneltilebilecek tazminat hakkının bulunduğu belirtilmiş[272], parasal sonuçların kişilik hakkına yapılan ihlal nedeniyle meydana gelen dolaylı sonuçları olup bunların, kişilik hakkının şahıs varlığı niteliğini değiştirmediği ileri sürülmüştür[273].

Grup içinde bağlayıcı şirket kuralları maddelerine aykırı davranılmasından doğan zararın, Grubun ülkemizde kurulu merkezi ya da kişisel verilerin korunmasında yetki kılınmış ülkemizde yerleşik bir Grup üyesince tazmin edilmesi gerekir. Bu çerçevede, yetkili Grup üyesi ve alınan mali teminatlar belirtilmelidir.

---

[267] Çekin, 2020, s.172.
[268] Ayözger Öngün, s.217.
[269] Zevkliler/Havutçu/Gürpınar, s.112.
[270] Kahraman, s.482; Haksız fiillerin kişilik hakkı, ayni hak ve fikri hak gibi mutlak hakların ihlalinden oluşacağı hk. bkz. Serozan, Rona, İfa, İfa Engelleri, Haksız Zenginleşme, Borçlar Hukuku Genel Bölüm Cilt 3, Filiz, İstanbul, 2009, s.286.
[271] Akman, Sermet, Burcuoğlu, Haluk, Altop, Atilla, Tekinay Borçlar Hukuku Genel Hükümler, İstanbul 1993, s.475; Nomer, Haluk N., Borçlar Hukuku Genel Hükümler, 15. Bası, Beta Yayınevi, İstanbul 2017, s.138.
[272] Toparlak, s.85; Ayözger Öngün, s.217.
[273] Serdar, İlknur, Radyo ve Televizyon Yoluyla Kişilik Hakkının İhlali ve Kişiliğin Korunması, Ankara, Seçkin Yayınevi, 1999, s.28.

a.Haksız Fiil

Haksız fiil esasen zarara yol açan ile zarar gören arasında bir borç ilişkisi doğurmakta[274] olup haksız fiil sorumluluğunun yaptırımı, bu fiil neticesinde gerçekleşen zararın tazmini şeklindedir.

Genel hükümler kapsamında talep edilebilecek tazminat isteminin ilk koşulu haksız bir eylemin bulunmasıdır. Hukuka uygunluk nedeni olmadıkça, hukuk düzenince korunan bir hakkın ihlali, hukuka aykırı kabul edilir[275]. Başka bir deyişle örneğin, tıbbi müdahaleye gösterilen rıza ile bu müdahale hukuka uygun olacaktır[276]. Bu çerçevede özel kanun niteliğindeki KVKK'nda yer alan sorumluluk hükümleri ile hukuka uygunluk sebepleri de göz önüne alınacaktır. Çünkü hukuka uygun veri işleme faaliyetinden söz edilebilmesi için yukarıda belirttiğimiz KVKK m.4'de gösterilen işleme ilkelerine uyulması gerekmektedir. Bununla birlikte, KVKK m. 5'de yer alan açık rızanın bulunması veya kanunda açıkça öngörülmesi, sözleşmenin taraflarının kişisel verilerinin işlenmesinin gerekmesi, veri sorumlusunun hukuki yükümlülüklerini icra edebilmesi için zorunlu olması veya veri ilgilisi şahsın veriyi alenileştirmiş olması gibi işleme koşullarından birinin bulunması gerekmektedir[277].

b. Nedensellik Bağı

Tazminat sorumluluğunun doğabilmesi için, fiilin haksız veya hukuka aykırı olması yanında bu fiilin hayatın olağan akışında, kişinin zarar görmesine elverişli olması şartı da aranmaktadır[278]. Bu çerçevede veri sorumlusunun hukuka aykırı veri işleme veya aktarma eyleminin, ilgili kişide zarar oluşturmaya elverişli olması beklenir.

Öte yandan, veri ilgilisi kişinin zararı, zararı tek başına gerçekleştirmeye elverişli bulunmayan birden fazla hukuka aykırı işleminin sonucu oluşmuş olabilir. Örneğin bağlayıcı şirket kuralları ile kişisel verinin AB'deki üye şirkete, KVKK m.9 yükümlülüklere uyulmaksızın aktarılması ve AB'deki işletmenin veri saklama alanlarında yeterli önlemleri almaması ve bir siber saldırıya uğraması nedeniyle, ilgili

[274] Serozan, 2009, s.286; Reisoğlu, Safa, Türk Borçlar Hukuku Genel Hükümler, 23. Bası, Beta, İstanbul 2012. s.162.
[275] Oğuzman Kemal, Öz, Turgut, Borçlar Hukuku Genel Hükümler Cilt – II, 14. Bası, Vedat Kitapçılık, İstanbul, Türkiye 2018, s.15.
[276] Kahraman, s.484.
[277] Toparlak, s.85.
[278] Oğuzman/ Öz, s.45; Ayözger Öngün, s.272.

kişinin zararı gerçekleşmiş olabilir. Bu halde ortak illiyet bağı kavramı gündeme gelecektir[279].

c. Kusur

Kusur, hukuk düzeni tarafından hoş görülmeyen ve kınanabilir davranıştır[280]. KVKK m.11/1/ğ ve m.14/3'teki düzenlemelerde açık şekilde belirtilmediği için tazminat talebinde kusur sorumluluğu mu yoksa sebep sorumluluğunun mu benimseneceği tartışmalı olan bir konudur. Bu konu ele alınırken, KVKK m.12 gereğince veri sorumlusu ve işleyen için veri güvenliğine ilişkin getirilen yükümlülükler de göz önüne alınmalıdır[281]. KVKK m. 12 gereğince, veri sorumlusu tüm tedbirleri değil, gereken tedbirleri almakla yükümlü kılınmıştır. Bu kapsamda yasa koyucunun KVKK'da sonuca bağlı bir sorumluluk getirmediği söylenebilir[282].

Dijital şekilde pekçok sayıda veriyi toplama, saklama, inceleme imkânı olan veri sorumlularının, verileri uygun biçimde koruyamama tehlikesini de yüklenmiş sayıldıklarının hakkaniyet prensibinin bir gereği olduğu belirtilmiştir[283]. Bu sebeple, bu noktada bir tehlike sorumluluğunun bulunduğunun kabulü ve zarardan sorumlu tutulacak veri sorumlusunun kusurunun aranmamasının doğru olabileceği, ancak KVKK'da buna ilişkin bir hüküm olmadığı belirtilmiştir. Bu noktada TBK "tehlike sorumluluğu ve denkleştirme" başlıklı madde 71'in uygulanıp uygulanamayacağı tartışılmıştır. TBK m.71 uyarınca, ciddi şekilde tehlike oluşturan bir işletmenin faaliyetinden zararın oluşması halinde, bu zarardan işletme sahibi ve işleten müteselsilen sorumludur. Bir işletmenin, niteliği ya da faaliyet yaparken kullandığı araçlar veya ekipmanlar göz önüne alındığında, bu işlerde uzman bir şahıstan umulan bütün özen gösterilse bile ağır zararlar meydana getirmeye elverişli olduğu neticesine ulaşılırsa, bu işletmenin ciddi ölçüde tehlike oluşturan bir işletme olduğu varsayılır. Veri sorumlularının faaliyetlerinin bu madde kapsamındaki bir tehlike olarak tanımlanıp tanımlanmayacağı bu maddenin uygulanması açısından önem arz edecektir.

[279] Oğuzman/ Öz, s.51.
[280] Ayözger Öngün, s.267; Oğuzman/ Öz, s.55.
[281] Çekin, 2020, s.172.
[282] Çekin, 2020, s.173.
[283] Gürpınar, s.691.

Öte yandan, bu alanda tehlike sorumluluğu, üçüncü kişinin ağır kusuru halinde veri sorumlusunu sorumluluktan kurtulabilecek ve çoğunlukla zarar gören ilgili kişinin menfaatine bir netice doğurmayacaktır. Çünkü bu durum verileri bilhassa da elektronik ortamda depolayan veri sorumlularının, aldıkları bütün tedbirlere karşın örneğin bir bilgisayar korsanının sistemlerine sızması durumunda, üçüncü şahsın ağır kusurunun kendi sorumluluğunu kaldıracağına ilişkin savunma yapmasına neden olur ve bu tehlike sorunluluğunu kabul etmenin pratikte ilgili kişiye bir faydası olmaz. Bu sebeple, veri aktarımı alanında veri sorumluları için tehlike sorumluluğu getirilse bile, üçüncü şahsın ağır kusurunun nedensellik bağını kesemeyeceğine dair özel bir düzenleme yapılması gerekmektedir[284].

Bununla birlikte, KVKK m.12'de yer alan yükümlülükleri icra eden veri sorumlusunun buna rağmen sorumlu tutulması, bu maddenin amacı ve uygulamadaki işlerliğini önleyecektir[285]. Öte yandan KVKK m.12'de veri güvenliğine dair getirilen yükümlülükler arasında, veri sorumlusunun özen borcu belirtilmektedir. Zararın oluşması, özensiz hareket edildiğini gösterse de, özen düzeyinin tespitinde ise veri işleme eylemlerinin içerdiği tehlike göz önüne alınmalıdır. Veri işleme eylemi ne ölçüde risk taşıyorsa, veri sorumlusunun göstereceği özen de o ölçüde fazla olmalıdır[286].

Bağlayıcı şirket kuralları, gösterilmesi gereken özen derecesinin öngörülmesi bakımından da faydalı olacaktır. Çünkü bu kurallar düzenlenirken, risk analizi ile veri koruması yönünde etki değerlendirmesi yapılması gerekmektedir. Bu şekilde şirketin veri işleme eylemlerinde oluşabilecek tehlike ve bu çerçevede gösterilmesi gereken özen seviyesi açığa çıkacaktır[287].

Özen yükümlülüğünü icra etmeyen veri sorumlusunun tazminat yükümlülüğünün, sebep sorumluluğu niteliğini taşıdığı ileri sürülmüştür[288]. Bu nedenle, kural olarak, zarar gerçekleştiğinde veri sorumlusunun veri güvenliğine dair yükümlülüklerini icra etmediği var sayılmalıdır. Bu görüş, ilgili kişinin lehine olsa da

[284] Gürpınar, s.691.
[285] Toparlak, s.86.
[286] Çekin, 2020, s.172.
[287] Toparlak, s.87.
[288] Çekin, Mesut Serdar, '6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanununun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 74, S. 2, 2016, s.638.

veri sorumlusu, özellikle KVKK m.10 ve 12'de yer alan tüm koşulları yerine getirdiğini kanıtlarsa kendisine sorumluluktan kurtuluş olanağı (kurtuluş beyyinesi) verilmelidir[289]. Bu açıdan bağlayıcı şirket kurallarının da önemli olduğu görülmektedir. Çünkü bağlayıcı şirket kuralları, KVKK m.12 sorumluluklarının icra edildiğine ilişkin kanıt aracı şeklinde kullanılabilir. Kaldı ki, AB hukukunda Regülasyon m.82/3'te, zararın meydana gelmesinde sorumlu olmadıklarını ispatlamaları halinde denetleyici ya da veri işleyenin sorumluluktan kurtulabileceği hükmü yer almıştır[290]. AB hukukuna paralel olan bu görüş, ilgili kişiye ispat açısından kolaylık sağlayacak ve KVKK'nın da amacıyla uyumlu olacaktır. Çünkü kusur sorumluluğunda veri sorumlusunun kusurunu, zarar gören kanıtlamalıdır. Sebep sorumluluğunun kabul edilmesi halinde ise hukuka aykırı eylemin ve zararın kanıtlanması yeterli olacaktır[291].

Bununla birlikte, KVKK m.11 gereğince veri sorumlusuna başvurarak bilgi talep eden ilgili kişinin, verilen bilginin güvenilirliğini kontrol etmesi olanaklı değildir. Bu durum anılan korumanın zayıf yanını da oluşturmaktadır. Örnek olarak ilgili kişinin verisi, veri sorumlusu tarafından yurtdışına aktarıldığında ve bu hususta ilgili kişiye bilgi verilmediğinde, ilgili kişinin bu verinin ne olduğunu belirlemesi veya zararını belirlemesi güç olacaktır[292]. Bu durum, ilgili kişinin Anayasa m.20/3'de anayasal bir hak olarak düzenlenen, kişisel verilerine ilişkin bilgilendirilme, bunlara erişme, bunların düzeltilmesi ya da silinmesini isteme hakkını kullanmasını neredeyse imkânsız hale getirmektedir. Bu tartışmalara bakıldığında, bağlayıcı şirket kurallarının ilgili kişilerin kişisel verileri aktarılmış olsa bile onları koruyabileceği ve uygulamada da verinin denetimini ve ispat kolaylığını sağlayabileceği görülmektedir[293].

Bağlayıcı şirket kuralları, KVKK m.12 yükümlülüklerini gerek veri sorumlusu şirket gerekse verilerin aktarımının yapıldığı üçüncü şahıslar açısından bağlayıcı bir şekilde hüküm altına almaktadır. Buna ilave olarak m.12'de düzenlenen veri sorumlusu şirket içinde bir yapı da getirilmiştir. Ancak tüm bu hüküm ve kuralların bu sistemin hala Türk mevzuatında açıkça bir kanunda yer almamasından ötürü ne derece geçerli ve uygulanabilir olacağı şüphelidir. Yani bağlayıcı şirket kurallarının

[289] Çekin, 2016, s.638.
[290] Ayözger Öngün, s.267.
[291] Çekin, 2020, s.174.
[292] Çekin, 2016, s.638.
[293] Toparlak, s.87.

bağlayıcılığının uygulamada nasıl sağlanacağı usul ve esaslarının hala kanunda öngörülmemiş olmasından ötürü net değildir.

Hesap verebilirliği ve şeffaflığı arttıran[294] bu düzenleme, veri ilgilisi şahıslara verilecek bilgilerin güvenilirliğini arttıracak ve doğruluğunu taahhüt edecektir. Bununla birlikte, Kurul'un da bağlayıcı şirket kurallarının bulunduğu bu şirketi kontrol ve denetim aşamaları, daha işler olacaktır. Bu sebeple bağlayıcı şirket kurallarının, KVKK yükümlülüklerinin icra edildiğine ilişkin ispat vasıtası şeklinde kullanılması da kolay hale gelecektir. Bu durum, ilgili kişilerle birlikte veri sorumlusu şirketlere de rahatlık sağlayacaktır[295].

d.Maddi ve Manevi Zarar

Kişilik hakları ihlal edilen kişilerin genel hükümler uyarınca tazminat hakkı KVKK m.14/3'de saklı tutulmuştur. Bu maddede sözü edilen genel hükümler, TMK m.24. ve 25 ile TBK m.53, 54, 56 ve m.58'dir. TMK m.24 uyarınca, hukuka aykırı şekilde kişilik hakkı ihlal edilen kişi, hâkimden, saldırıyı yapanlara karşı korunma talep edebilir ve bu koruma davayla istenebilir. Kişilik hakkına saldırı durumunda maddî ve manevî tazminat davalarının açılması da mümkündür (TMK m.25)[296].

TMK m. 25 uyarınca davacı, anılan tazminat taleplerinin yanı sıra hukuka aykırı tecavüz sebebiyle kazanılan gelirin vekâletsiz iş görme düzenlemeleri çerçevesinde kendisine verilmesini de isteyebilecektir.

İhlal durumunda oluşabilecek maddi zarar dikkate alındığında ele alınması gerekli olan ilk konu, kişisel verilerin ekonomik değeridir. TMK m.23 düzenlemesi, kişinin hak ve fiil ehliyetlerinden kısmi şekilde de olsa vazgeçemeyeceği ya da onları hukuka veyahut ahlaka aykırı şekilde kısıtlayamayacağı hükmünü içermektedir. Bu şekilde, kişiyi kendisinden de korumak hedeflenmekte ve özel hayatın da herhangi bir ticarete konu olamayacağı belirtilmektedir[297]. Buna karşın, kişisel verilerle işleyen günümüz dijital dünyası ve veri ekonomisinde, kişisel verilerin meta halinde geldiği

[294] Dülger, 2019, s.152.
[295] Toparlak, s.88.
[296] Gürpınar, s.689.
[297] Serozan, 2011, s.412; Ayözger Öngün, s.280-281.

ve önemli bir miktarda ekonomik değere sahip olduğu bir gerçektir[298]. Bu kapsamda değişken olsa da veri işleyen veri sorumlusunun bir kazanç elde ettiği bilinmektedir.

İlgili kişinin, kişisel verilerinin hukuka aykırı işlenmesi veya aktarılmasından ötürü görebileceği somut bir zarara örnek olarak; banka tarafından ilgili kişiye kredi verilmemesi ya da kişinin işe alınmaması gibi durumlar gösterilebilecektir[299].

Ortaya çıkabilecek bir başka zarar olan kişilik hakkının ihlali sebebiyle ilgili kişinin duyduğu acı ve elemin giderilmesi ya da azaltılması için manevi tazminat davaları da önemlidir[300]. Bu çerçevede, hukuka aykırı şekilde kişisel verilerin işlenmesi sebebiyle manevi zarar gören ilgili kişi, veri sorumlusunun sorumluluğuna gidebilecektir. Örneğin, işyerinde yeterli korumasının olmaması sebebiyle yetkisiz kişilerin, veri ilgilisi şahsın sağlık verilerine ulaşıp bunu kullanması durumunda, veri sahibi ilgili kişi, işverenin sorumluluğuna gidebilecektir.

Ayrıca TMK m.25 çerçevesinde ilgili kişi olan davacı, kişilik haklarını korunmak için kendi ikamet yeri ya da davalının ikamet yerinde dava açabilecektir. Bu maddeye göre bağlayıcı şirket kurallarını taahhüt eden üye Türk şirketinin, AB'deki şirkete ilgili şahsın verisini KVKK'yı ihlal eder biçimde aktarması ve AB'de bir zararın gerçekleşmesi durumunda, veri ilgilisi şahıs ikamet yeri adresinde de dava açabilir[301].

e. Türkiye'de Şube Ya da İrtibat Bürosu Olan Grup Şirket Veya Teşebbüslerin Sorumluluğu

Daha önce belirttiğimiz gibi, bağlayıcı şirket kuralları düzenleyebilecek yapılar; grup şirket veya ekonomik iş birliği pozisyonuna sahip teşebbüslerdir. Bu yapının içine girebilmek için üye teşebbüsün, gerçek veya tüzel kişiliğinin bulunması gerekmemektedir. Hatta bağlayıcı şirket kurallarını hazırlayan kurum; üçüncü bir ülkede irtibat bürosu veya bir ofis şeklinde de faaliyet yapıyor olabilir. Bağlayıcı şirket kurallarının yapısının, ülkemizdeki üyesinin hukuki bir kişiliği bulunmamasının

[298] Lieshout, Marc, 'the Value of Personal Data', IFIP Advances in Information and Communication Technology, C. 457, S. 5, 2015, s.26-38.
[299] Çekin, 2020, s.174.
[300] Oğuzman/Öz, s.259.
[301] Toparlak, s.89.

KVKK açısından incelenmesi gerekmektedir. Çünkü KVKK, sorumluluğu belirlerken gerçek veya tüzel bir hukuki kişiliğin bulunmasını şart koşmaktadır.

Regülasyon'da yer alan veri işleme faaliyetinin mutlaka AB içinde yapılmasını aramayan kuruluş ilkesi gereğince, hukuki bir kişilik olmasa da fiziki bir yapı altında gerçekleştirilen faaliyetler de Regülasyon kapsamına girmektedir. Bununla birlikte *Google Spain* kararı (C –131/12) ile AB haricinde yerleşik şirketlerin AB içerisindeki üye şirketlerle arasındaki bağlantıya ilişkin ilkeler getirmiştir. AB içerisindeki şirketin faaliyeti, AB haricindeki ana şirketten ayrı olamıyorsa, ana şirketin faaliyetleri de Regülasyonun uygulama kapsamına girecektir. KVKK'da ise Regülasyon'daki düzenlemeye benzer bir düzenleme yoktur. Bu nedenle Türkiye'de tüzel kişiliğe sahip olamadan veri işleyen yabancı şirketlerin sorumlulukları sorun oluşturabilir.

Bu soruna çözüm bulmak için irtibat büroları ve şubeler yönünden Türk Ticaret Kanunu'ndaki (TTK) düzenlemeye bakılmalıdır. TTK m.40/4'e göre, merkezleri Türkiye sınırları haricinde olan ticari teşebbüslerin ülkemizdeki şubeleri, yerli ticari teşebbüsler gibi tescil olurlar. Bu şubeler açısından ikamet yeri ülkemizde olan tam yetkili bir ticari temsilci atanması hükmü getirilmiştir. Türk hukukunda bir yerin şube kabul edilebilmesi için merkeze bağımlı olma, dış ilişkilerinde bağımsızlık, yer ve idare ayrılığı gibi kıstasların bulunup bulunmadığına da bakmak gerekir[302]. Şubeler, iç işlerinde merkeze bağlı olsalar da, dışişlerinde bağımsız olduklarından, merkezin veri işleme faaliyeti gibi işlemlerini üçüncü kişilerle kendi başlarına yapabilmektedirler[303].

Tüm bu açıklamalardan görüleceği üzere, gerçek veya özel hukuk tüzel kişiliği olmasa da, veri işleme faaliyeti yapan ve ticari gelir temin eden şubelerin veri sorumlusu olarak kabul edilmesi, yasanın amacı ile uyumlu olacaktır. Ancak, bu bağlamda KVKK'nun veri sorumlusunu gerçek veya tüzel kişi olarak kabul etmesi sorun oluşturmaktadır. KVKK m. 18/2 gereğince, Kurul tarafından düzenlenecek idari para cezaları, yalnızca gerçek kişiler ve özel hukuk tüzel kişileri aleyhine uygulanabilecektir[304].

[302] Arkan, Sabih, Ticari İşletme Hukuku, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, Ankara, Türkiye 2014, s.37.
[303] Arkan, s.38.
[304] Toparlak, s.93.

KVKK'daki bu düzenlemeye rağmen Kurul, bu konuda verdiği bir kararında[305], veri sorumlusu kavramını isabetli bir şekilde AB hukukundaki kuruluş ilkesine gönderme yaparak ele almıştır. Kararda, VERBİS'e kaydolmak için veri sorumlusu olunması ve tüzel veya gerçek kişiliğin var olması gerektiği belirtilmiştir. Yine kararda, yurtdışında kurulu tüzel kişilerin Türkiye'deki şubelerinin ayrı bir tüzel kişilikleri olmasa da, TTK m.40 uyarınca şubelerin yerli ticari işletmeler gibi tescil edilmesi gerektiği belirtilmiştir. Bunun yanında Kurul, Regülasyon m.4'e gönderme yaparak AB'deki veri sorumlusu olma kıstası olarak, "tüzel kişi" olma şartının bulunmadığını dikkate almıştır. Bu sebeple, veri işleme süreçleri açısından merkezden bağımsız olarak Türkiye'de veri sorumlusu kıstaslarına uygun şekilde faaliyet gösteren bu şubelerin, veri sorumlusu kabul edileceğini belirtmiştir. Bu çerçevede KVKK'nda değişiklik yapılması halinde veri sorumlusunun hukuki bir kişiliğinin bulunması şartı değiştirilmelidir. Bağlayıcı şirket kurallarını taahhüt eden çok uluslu şirketin Türkiye'deki üyesinin şube şeklinde örgütlenmesi durumu, KVKK'ndan kaynaklanan yükümlülükleri ortadan kaldırmamaktadır. Türkiye'de bulunan şube de, diğer veri sorumluları gibi KVKK'ndan kaynaklanan yükümlülükleri yerine getirmekle sorumludur[306].

Öte yandan, Türkiye'de açılan irtibat büroları bakımından yapılacak değerlendirme, şubeler için yapılanlardan farklı olacaktır. İrtibat bürolarını düzenleyen "*4875 sayılı Doğrudan Yabancı Yatırımlar Kanunu (DYYK)*" m.3'e göre bu bürolar, kendine ait hukuki kişilikleri bulunmayan, yurt dışında bulunan merkez ofis namına çalışan ve doğrudan ticari faaliyette bulunmayan bürolardır[307].Bu büroların birçoğu, yıllardır Türkiye'de yerleşik bir yapısı olan ve pek çok çalışana sahip bürolardır. Bu bürolar, işleyiş ve nitelikleri gereği, birçok gerçek ve tüzel kişinin verisini elde etmekte, muhafaza etmekte ve yurtdışındaki merkez şirkete aktarmaktadırlar. Bu işleyiş ve nitelikleri gereği, veri sorumlusu sıfatına sahip olduğu tespitinin KVKK'nın amacına uygun düştüğü ifade edilebilir. Dolayısıyla Türkiye'de kendine ait hukuki bir

[305] Kişisel Verileri Koruma Kurulu, Yurtdışında Yerleşik Tüzel Kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili 23/07/2019 tarih ve 2019/225 sayılı Karar, bkz. https://www.kvkk.gov.tr/Icerik/5545/2019-225, E.T.:11.07.2021.
[306] Toparlak, s.93.
[307] Kara, Hacı, 'Türk Hukukunda İrtibat Bürosu ve Özellikleri', İzmir Barosu Dergisi, C. 83, S.3, 2019, s.167-168.

kişiliği bulunmadan yapılanan ve faaliyet gösteren bu büroların yükümlülükleri de ayrı bir sorun oluşturabilmektedir.

Kurul, bu soruna ilişkin bir kararında[308], AB hukukundaki kuruluş ilkesini dikkate alarak değerlendirme yapmıştır. Anılan kararda Kurul, DYYK'daki koşulları tekrarlayarak, ülkemizde irtibat bürosu kurulabilmesi için, şirket tüzelkişiliklerinin yabancı ülke yasaları uyarınca kurulması ve irtibat bürolarının Türkiye'de ticari faaliyette bulunmaması gerektiğini belirtmiştir. Ayrıca bu büroların, ticari faaliyet haricinde haberleşme, araştırma yapma, sosyal ve kültürel alanlarda çalışmalar yapma, şirket birleşmeleri ve devirleri için hazırlık yapma, reklam ve tanıtım, yatırım ve iş imkânlarını yakından izleme ve bu hususlara dair merkez firmaya bilgi verme amacına sahip bürolar oldukları ifade edilmiştir. Bu kapsamda Kurul, irtibat büroları, şube özelliğine sahip olmadığından VERBİS sistemine kayıt edilme yükümlülüklerinin olmadığına karar vermiştir[309].

Türk hukukunda irtibat bürolarının düzenlenmesi amacı ele alındığında, bu büroların, ticari risk almayı seçmeyen yabancı yatırımcılar için ülkemizde yatırım ve iş olanaklarına ilişkin gereken bilgileri ilk elden edinmesi ve piyasanın izlenmesi için kullanıldığı görülmektedir. Kaldı ki, DYYK m.3/h uyarınca sadece yabancı şirketlere, ülkemizde ticarî faaliyet yapmamak şartıyla irtibat bürosu açma izni verilmektedir[310]. Bu çerçevede Kurul'un, irtibat bürolarını VERBİS yükümlülüğünün haricinde tutması makul görünmektedir.

B.İhlal Durumunda Kurula Başvuru ve İdari Para Cezaları

KVKK, kural olarak, ülkemiz sınırları içinde uygulanmaktadır. Ülkemiz sınırları içerisinde olmamakla birlikte, Türkiye'de veri işleme faaliyetleri yapan Google, Facebook gibi şirketlere doğrudan uygulanabilirliğinin bulunmadığı görüşü belirtilmiştir[311]. Ancak KVKK'nın kapsamını düzenleyen m.2'de bu Kanun

[308] Yurtdışında yerleşik Tüzel kişilerin Türkiye'deki Şubeleri ile İrtibat Bürolarının Sicile Kayıt Yükümlülüğü Hakkındaki Görüş Talebi ile ilgili Kişisel Verileri Koruma Kurulunun 23/07/2019 tarih ve 2019/225 sayılı Kararı, bkz. https://www.kvkk.gov.tr/Icerik/5545/2019-225, E.T.: 12.07.2021.
[309] Toparlak, s.94.
[310] Kara, s.194.
[311] Toparlak, s.89.

hükümlerinin, kişisel verileri elle veya otomatik olarak işlenen gerçek ve tüzel kişiler hakkında uygulanacağı belirtildiğinden, kanaatimizce ülkemizde gerçek ve tüzel kişilerin verilerini işleyen ve faaliyet gösteren merkezi yabancı ülkede bulunan gerçek ve tüzel kişilere ilişkin de uygulanabilecektir. Tekrar belirtmek gerekir ki; bağlayıcı şirket kuralları açıkça Türk mevzuatında kanunla öngörülmemiştir. Bu nedenle bu kurallara kanundan kaynaklı bir aykırılık aslında dolaylıdır denebilir.

KVKK'ya göre yükümlülük yöneltilen şahıslar olan veri sorumlusu ve veri işleyen gerçek ya da tüzel kişi olabilecektir. Veri sorumluları ve işleyenler açısından Regülasyon'daki hükmün aksine, KVKK'nın lafzı mutlaka bir hukuki kişilik aramaktadır. KVKK, veri sorumluları ve işleyenleri, gerçek ya da tüzel kişiliklerle sınırlamaktadır. Kurul, hukuki kişiliğin yanı sıra kimliğin tespit edilebilir olması gerektiğine de değinmiştir[312]. Kurul bir kararında, internetteki bir kullanıcı adıyla gerçekleştirilen hukuka aykırı kişisel veri işleme eylemi bulunsa da, bu kullanıcı adının şahsın kimliğini tespite yeterli gelmediğini ve bu kişi belirsiz olduğundan, bir işlem yapılamayacağına karar vermiştir. Kararda Kurumca yapılacak işlem bulunmadığına karar verilmiş olsa dahi, KVKK'nın 17/1 maddesi gereği, kişisel veri suçları açısından TCK m.135 ila m.140 arasındaki hükümlerin uygulanacağının vurgulanmış olması ile hukuka aykırılığın KVKK ile olmasa bile diğer mevzuat gereği sonuçsuz kalamayacağı isabetli şekilde belirtilmiştir. Aksi bir durum, hukuka aykırılığın yaptırımsız kalması olurdu. Ek olarak, kanaatimizce TCK gereği yürütülen soruşturma neticesinde kimliğin belirli hale gelmesi söz konusu olur ise Kurum'un 'işlem yapabilir' olması da gerekir.

KVKK'nun beşinci bölümünde yer alan suçlar ve kabahatlerin tatbik edilebilmesi için, ülkemizde yerleşik ve belirlenebilir bir hukuki kişilik bulunmalıdır. İdari para cezaları, veri sorumlusu gerçek kişiler ve özel hukuk tüzelkişileri aleyhinde uygulanmaktadır (m.18/2)[313]. KVKK m.18'de veri sorumlularına yönelik düzenlenmiş ve farklı kabahatler sonucu 13.391,00TL'den 2.678.863,00 TL'ye kadar idari para cezaları getirilmiştir. KVKK m.18/2'nin lafzına bakıldığında, idari para cezalarının, sadece Türkiye'deki yapının yani Türkiye'de bulunan gerçek ve tüzel kişinin

[312]13/09/2018 Tarihli ve 2018/106 Sayılı Karar, bkz. https://kvkk.gov.tr/Icerik/5421/2018-106, E.T:11.07.2021.
[313] Dülger, 2019, s.373.

Türkiye'deki faaliyetlerine ilişkin verilebileceği ileri sürülmüştür[314]. Ancak gerek KVKK m.2 gerekse m.18/2'de Türk hukukuna göre gerçek kişi veya tüzel kişiden bahsedilmemektedir. Bu sorunla karşılaşan kanun koyucu, sadece sosyal ağ sağlayıcılara ilişkin olarak KVKK'da değil, "*5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*"da değişiklik yapmış ve 29/7/2020 tarih ve 7253 sayılı Kanun m.6 ile 5651 sayılı Kanun'a ek 4. maddeyi eklemiştir. Bu maddeyle, ülkemizden günlük bir milyondan fazla erişime sahip olan ve kaynağı yurt dışında bulunan sosyal ağ sağlayıcılarının Türk vatandaşı olan yetkili en az bir kişiyi Türkiye'de temsilci şeklinde belirleme ve Kurum'a bildirme yükümlülüğü getirilmiştir. Kaldı ki bu bağlamda Kurul'un Facebook şirketine yönelik 2019 yılında verdiği iki kararda anılan şirkete idari para cezası verildiği görülmektedir.

Kurul, Türkiye'de yerleşik kurulu bir tüzel kişiliği olmayan ve ABD'de yerleşik şirket olan Facebook'a üzerinde gerçekleşen ve Türkiye'deki ilgili şahısların kişisel verilerine etki eden hukuka aykırılık nedeniyle, bu şirket aleyhinde KVKK m. 12/1 ve 12/5'e göre idari para cezası vermiştir[315]. Yine Kurul, Facebook'ta meydana gelen ve Türkiye'deki veri ilgilisi şahısların kişisel verilerine etki eden bir başka hukuka aykırılık nedeniyle 18 Eylül 2019 tarihinde anılan şirket aleyhinde KVKK m. 12/1 ve 12/5'e göre idari para cezası verilmesine karar vermiştir[316].

Bununla birlikte KVKK m.10 gereğince aydınlatma yükümlülüğünü icra etmeyen veri sorumlularına ilişkin olarak bu madde kapsamında 13.391,00TL'den 267.883,00 TL'ye kadar idari para cezası yer almaktadır. Veri güvenliğine dair yükümlülükleri veri sorumlusu ve veri işleyenin icra etmemesi durumunda ise, 40.179,00 TL'den 2.678.863,00 TL'ye kadar idari para cezasına karar verilebilecek olup, bu para cezasına ilişkin müşterek sorumluluk getirilmiştir (m.12)[317]. Ayrıca, veri sorumluları, KVKK m.15 gereğince Kurul'un inceleme yaptığı konuya dair istediği bilgi ve dokümanları on beş gün içerisinde sunmalıdırlar ve gerekirse Kurul'a belgelerin bulunduğu yerde inceleme yapma olanağı sağlarlar.

---

[314] Toparlak, s.90.

[315] Facebook Hakkında Kişisel Verileri Koruma Kurulu'nun 11.04.2019 tarih ve 2019/104 sayılı Karar Özeti, bkz. https://www.kvkk.gov.tr/Icerik/5450/2019-104, E.T.:11.07.2021.

[316] Facebook hakkında Kişisel Verileri Koruma Kurulu'nun 18.09.2019 tarih ve 2019/269 sayılı Karar Özeti, bkz. https://kvkk.gov.tr/Icerik/5534/2019-269, E.T.:11.07.2021.

[317] Çekin, 2020, s.228.

Kurul, şikâyet sonucu veya kendiliğinden yaptığı inceleme neticesinde bir aykırılığı belirlemesi durumunda, bu aykırılığın giderilmesi kararı vermektedir (KVKK m.15). Bahse konu kararı otuz gün içinde icra etmeyen veri sorumlularına 66.965,00 TL ila 2.678.863,00 TL arasında idari para cezası verilebilmektedir. Bununla birlikte, VERBİS'e kayıt ve bildirim yükümlülüğünü icra etmeyen veri sorumlularına da idari para cezası verilebilmektedir (KVKK m.16).

Bağlayıcı şirket kuralları taahhüdünde bulunan Türkiye'deki üyenin KVKK'ndan kaynaklanacak sorumluluğunun, esasta kendi faaliyetleri nedeniyle oluşabilecek hukuka aykırılıkları kapsadığı ileri sürülmüştür[318].

İdari para cezaları bakımından esas olarak göz önüne alınan konular; aydınlatma yükümlülüğü, veri güvenliğine dair yükümlülükler, Kurul'un verdiği kararların icrası ile VERBİS'e bildirim ve kayıt yükümlülüğüdür. Bu manada bağlayıcı şirket kuralları taahhütlerinin, bilhassa bu yükümlülükleri ihlal etmemesine önem verilmelidir. Kurul, VERBİS'e kayıtlı tüm veri sorumlularınca kişisel veri işleme envanteri düzenlenmesini önermektedir[319]. Bu nedenle bağlayıcı şirket kurallarını kullanacak şirketlerin envanterinin bulunması ve Kurul'a sunulması önem arz etmektedir.

Ayrıca idari para cezalarında alt ve üst sınırlar arasındaki sınır çok geniştir. Sınırın geniş olması uygulamada da tutarsızlıklara yol açacağı gerekçesiyle eleştirilmiştir[320]. Buna ilave olarak ilgili maddenin altında, belirlenecek idari para cezası miktarının hangi usul ve ilkeler kapsamında tayin edileceğinin belirtilmemesi de sorun oluşturabilecektir. Regülasyon kapsamında verilecek idari para cezalarının tayin edilme usul ve ilkeleri, Regülasyon m.83'de detaylı şekilde yer almaktadır.

KVKK'nın gerekçesinde, idari para cezalarının alt ve üst sınırı arasındaki açıklığın bilinçli biçimde geniş bırakıldığı ve veri sorumlusunun ekonomik gücüne bakılarak idari para cezasının verileceği ifade edilmiştir. Fakat Kanunda idari para cezasının belirlenme kriterine ilişkin hüküm bulunmamaktadır. İlave şekilde idari para cezasının fiil baz alınarak mı ya da ilgili şahıs esas alınarak mı belirleneceği de açıkça

[318] Toparlak, s.91.
[319] Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, bkz.; https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf, s.15, E.T:15.10.2021.
[320] Toparlak, s.91.

düzenlenmemiştir. Bu kriterlerin yer almamasının, hukuki belirlilik ilkesine zarar verebileceği, tutarsız uygulamalara yol açabileceği belirtilmiştir[321]. Ayrıca doktrinde, kabahatler hukuku açısından zincirleme suç hükümleri mevzuatta düzenlenmediğinden her bir veri sızıntısı veya hukuka aykırı aktarım halinde, ihlal sayısı kadar idari para cezası verileceğinden, bu durumun veri sorumluları açısından önemli sorunlara yol açacağı belirtilmiştir[322].

C.Cezai Sorumluluk

İlgili kişiye ait kişisel verilerin ceza hukuku alanında ne anlama geldiği hususunda açık bir düzenleme bulunmamasının "suç ve cezanın kanuniliği" ilkesine aykırı olup olmadığı konusunda tartışma varsa da[323], KVKK m.17'de öngörüldüğü gibi kişisel verilere ilişkin suçlar açısından TCK m. 135 ila 140 hükümleri uygulanacaktır [324]. Bu kapsamda bu suçlar kısaca ele alınacaktır. Öncelikle, TCK m. 135 gereğince hukuka aykırı şekilde şahısların kişisel verilerini kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği düzenlenmiştir. KVKK m. 5'te yer alan ilgili kişinin rızası, kanunlarda açıkça öngörülmesi, bedensel bütünlüğün korunması için zorunlu olması, ilgili şahsın veriyi alenileştirmiş olması gibi hususlar hukuka uygunluk sebebi oluşturacaktır[325]. Bu nedenle Türk şirketin taahhüt edeceği bağlayıcı şirket kurallarında yer alan hukuka uygunluk nedenlerinin, KVKK m. 5 ile uyumlu olması gerekmektedir.

Kişisel verilerin korunmasına dair bir başka hüküm olan TCK m. 136'da ise, bu verileri hukuka aykırı şekilde bir başka şahsa veren, yayan ya da elde eden şahıslar hakkında hapis cezası verileceği öngörülmüştür. Bu madde kapsamında kişisel verilerin aktarılmasından söz edildiğinden, bu aktarımlarda KVKK m. 8 ve m. 9'a uygun davranılması gerekmektedir. Aksi takdirde, cezai sorumluluk yanında KVKK yükümlülüğüne aykırılık hali de oluşacaktır. Türkiye'den AB'deki üyelere aktarılacak

[321] Küzeci, 2019, s.376.
[322] Dülger, 2019, s.374.
[323] Başalp, 2008, s.296; Şener, Gülnihal Emine, Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, Adalet Dergisi, 2011, s.74.
[324] Dülger, 2019, s.309 vd.; Çekin, 2020, s.225; Ayözger Öngün, s.97.
[325] Dülger, 2019, s.323 vd.

verilerle ilgili KVKK m.9'daki yurt dışına veri aktarım yükümlülüklerine uyulmalıdır[326].

KVKK m.17/2'de, m.7'de yer alan kişisel verilerin silinmesi, yok edilmesi ya da anonimleştirilmesini düzenleyen hükmün ihlal edilmesi durumunda, TCK m. 138 gereğince hapis cezasına hükmedileceği öngörülmüştür. KVKK m.17/2, TCK m.138'de düzenlendiği gibi, kanunda öngörülen sürelerin sona ermiş olmasına rağmen verilerin yok edilmemesi durumunu düzenlemektedir. Bu manada Türk hukukunda, yasal yükümlülük olarak getirilen çeşitli saklama süreleri de değerlendirilmelidir[327]. Bu kapsamda "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesine İlişkin Yönetmelik*" m.5/1 gereğince veri sorumluları; kişisel verilerin silinmesi ve imha kuralları oluşturmakla yükümlüdürler. Yine bu Yönetmelik'te yer alan m.6'da ise, saklama ve imha politikasının asgari olarak hangi tür verilerin ne kadar süreyle saklanacağının gösterilmesi öngörülmüştür[328]. Bu çerçevede bağlayıcı şirket kurallarını taahhüt eden Türk şirketinin, Türk kanunlarında yer alan saklama sürelerini aşmaması gerekir. Diğer bir deyişle, bağlayıcı şirket kurallarında yer alan saklama süreleri iç hukukla karşılaştırılmalı ve iç hukuka aykırı olmaması temin edilmelidir. Oluşturulacak kişisel verileri silme ve imha kurallarında Türk mevzuatındaki saklama sürelerinin belirtilmesi gerekir. Son olarak, yukarıda yer alan suçların tüzel kişilerin organları tarafından işlenmesi durumunda, TCK m.140 gereğince bunlara özgü güvenlik tedbirleri uygulanacaktır[329].

D.Bağlayıcıyı Şirket Kurallarının İhlalinde İspat Yükü

Kurum'un yayınladığı bağlayıcı şirket kuralları başvuru formunda, bağlayıcılık unsuru olarak, bu kuralların ihlali iddiasına ilişkin ispat yükünün, grubun ülkemizde kurulu merkezinde ya da grubun merkezi Türkiye'de değil ise veri korunmasında yetkili kılınmış ülkemizde kurulu grup üyesinde bulunması gerekmektedir.

[326] Toparlak, s.96; Ayözger Öngün, s.98.
[327] Dülger, 2019, s.370-371; Çekin, 2020, s.225.
[328] Kurul'un kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin rehberi bkz. https://www.kvkk.gov.tr/yayinlar/kişisel%20verilerin%20silinmesi, %20yok%20edilmesi%20veya%20anonim%20hale%20getirilmesi%20rehberi.pdf, E.T.: 12.07.2021.
[329] Toparlak, s.97.

Yine Kurum'un yayınladığı "Veri Sorumluları İçin Bağlayıcı Şirket Kurallarında Bulunması Gereken Temel Hususlara İlişkin Yardımcı Doküman"da "Uygunluk Kriterleri" başlığı altında ispat yükünün bireysel değil şirket üzerinde olması gerektiği belirtilmiştir. Yine bu dokümana göre, gruptaki tüm üyeler için hukuki anlamda geçerli ve kanıtlanabilir bir ya da daha çok usul ile bağlayıcı şirket kurallarının bağlayıcılığı temin edilmelidir. Bu sistemin hala Türk mevzuatında açıkça bir kanunda yer almamasından ötürü bu kuralların ne derece geçerli ve uygulanabilir olacağı şüphelidir. Yani bağlayıcı şirket kurallarının bu yönü ile bağlayıcılığının uygulamada nasıl sağlanacağı usul ve esaslarının hala kanunda öngörülmemiş olmasından ötürü net değildir.

E.Veri Sahibinin Hakları

KVKK m.11'in ilgili kişilere tanıdığı haklar, bağlayıcı şirket kuralları içinde de kapsamlı şekilde taahhüt edilmelidir. Bu madde uyarınca ilgili şahıs, istediği zaman veri sorumlusuna başvurarak kendisiyle alakalı verilerinin işlenip işlenmediğini öğrenme, kişisel verileri işlenmişse bunları isteme, bu verilerin işlenme amacı ve bu bilgilerin bu amaca uygun şekilde kullanılıp kullanılmadığı veya aktarılıp aktarılmadığını öğrenme hakkı bulunmaktadır. Veri ilgilisi şahsın bilgi edinme hakkı; kişisel verilerin korunmasına dair haklarının da çekirdeğini meydana getirmektedir. Çünkü şahsın kişisel verileri üzerindeki faaliyetlere ilişkin bilgilendirilmemesi durumunda bunlara ilişkin haklarını kullanması olanaklı olmayacaktır. Bu sebeple veri ilgilisi şahsın bilgi edinme hakkının, veri sorumlusunun aydınlatma yükümlülüğüyle çok yakın bir ilişkisi bulunmaktadır[330].

Bununla birlikte ilgili kişi; kişisel verilerin eksik ya da hatalı işlenmesi halinde, düzeltilmesini talep etme (m.11), bu verilerin silinmesi veya yok edilmesini talep etme (m.7) hakkına sahiptir.

Öte yandan, KVKK m.11'de veri ilgilisi şahsın, işlenmiş olan verilerinin otomatik olarak analiz edilerek, şahsın aleyhine bir neticesinin meydana çıkması durumunda bu neticeye itiraz etme hakkı yer almıştır. Yine bu madde uyarınca, kişisel

[330] Şimşek, s.90.

verilerin yasaya aykırı olarak işlenmesi nedeniyle zarar görmesi durumunda, şahsın zararın tazminini isteme hakkı bulunmaktadır[331]. Grup şirketin Türkiye'de kurulu merkezi, veri korunmasında yetkili kılınmış Türkiye'de kurulu bir Grup üyesi ya da aktarım yapan veri sorumlusunun bağlayıcı şirket kurallarından doğan tazminatın ödenmesi ve ihlallerin ortadan kaldırılması hususundaki yükümlülüğünü kabulü ve bunu taahhüt etmesi gereklidir. Bu taahhüde ek olarak, Grup şirket açısından, bilhassa Türkiye haricindeki bir kural ihlali halinde, Türkiye haricinde yerleşik bir grup üyesi tarafından yapılabilecek bütün ihlaller açısından her bir üyenin sorumlu olması da temin edilebilir. Elbette bağlayıcı kuralları ile bağlı Türkiye dışında yerleşik fiilleri açısından sorumluluğu kabul eden bütün üyelerin, bağlayıcı şirket kurallarının ihlal edilmesinden doğan zararların giderilmesi için yeterli varlığa sahip olduğuna ilişkin başvuru formunda bir taahhüt ve bilgi yer almalıdır.

Bağlayıcı şirket kurallarında ilgili kişinin haklarını kullanılabilmesi için taahhüt edilen usuller de gösterilmelidir. Örneğin veri koruma makamlarına şikâyet veya üye devletlerin yetkili ve görevli mahkemelerinde dava açma yöntemleri belirtilmelidir[332].

VI. BAĞLAYICI ŞİRKET KURALLARINA İLİŞKİN AB HUKUKU İLE TÜRK HUKUKUNUN KARŞILAŞTIRILMASI

Türk hukukunda Kurul; Regülasyon, ABAD kararları ve AB uygulamasını dikkate alarak bağlayıcı şirket kurallarını yayınlamış olup bu duyuru, büyük oranda Regülasyon ile uyumludur. Bununla birlikte, anılan duyuruda düzenlenmeyen noktalar ve iki hukuk sistemindeki farklılıklar ele alınmaya çalışılacaktır.

Öncelikle Regülasyon'un aksine KVKK, rıza ve açık rıza ayrımı yapmakta ve veri işleme sebebini hukuka uygun hale getiren olarak açık rızayı esas almaktadır[333]. Bu çerçevede bağlayıcı şirket kurallarını taahhütte bulunan ülkemizdeki üye şirket, açık rızayı hukuka uygunluk nedeni şeklinde ileri sürüyorsa, KVKK m.5/1'e uygun biçimde rızanın alınmasını sağlamalıdır[334].

Regülasyon, üçüncü ülkelere veri aktarılması amacıyla farklı uygun güvenlik tedbirleri belirlemiştir. Regülasyon m.40'da, davranış kuralları (code of conduct)

[331] Çabuk, s.113-114.
[332] Toparlak, s.55.
[333] Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP 187, 13 Temmuz 2011, s.21.
[334] Toparlak, s.78.

adıyla, veri sorumlusu veya işleyen üyeleri temsile yetkili olan sektör ya da ticari birliklerinin, o sektörün gereksinimlerini dikkate alarak düzenledikleri ve onaylanmış araçlardan söz edilmiştir. Bu araçlarla üçüncü ülkelere veri aktarımında ilgili alanın ihtiyaçlarını dikkate alarak bağlayıcı şirket kuralları oluşturulabilecektir. Yine son zamanlarda çok yaygın bir uygulama olmasa da AB hukukunda veri sorumlusu ya da işleyenin yaptığı faaliyetlerin Regülasyon'a uyumlu olduğunu gösteren sertifikalar (Regülasyon m.42/5, 43, 46/2-f, 63) da bağlayıcı şirket kuralları hazırlanırken dikkate alınmaktadır. Türk hukukunda gerek davranış kuralları gerekse sertifikalara ilişkin düzenleme bulunmadığı görülmektedir. Elbette Kurul yapacağı ek bir duyuru ile davranış kuralları ve sertifika kullanımına ilişkin kurallar oluşturabilir ve bu sayede de bağlayıcı şirket kuralları kapsamında yeterli korumaya tabi aktarım yapılabilir[335].

Öte yandan, Türkiye'de yerleşik fakat AB'de üyeleri olan küresel bir grup şirketin kendi bağlayıcı şirket kurallarını hazırlaması ve uygulaması da olanaklıdır. Bu durumda bu kurallar, Türk hukuku bakımından küresel şirket içerisinde veri akışını serbest şekilde temin edecektir. Bu kuralların, AB'de akredite bir kuruluştan Regülasyon m.46/2/f gereğince sertifika alması da akla gelebilir. Bu halde Türkiye'de düzenlenen bu kurallar, AB'de gerçekleştirilecek veri transferleri için de Regülasyon'a göre uygun güvenlik tedbiri özelliğine sahip olacaktır.

Çok uluslu bir AB şirketinin bağlayıcı şirket kurallarını taahhüt eden Türkiye'deki şirketi, onaylanmış bu kurallara uygun hareket etmelidir. Bilhassa veri işleme koşulları, hukuka uygunluk sebepleri ve veri ilgilisi şahıslardan alınacak rızalar, Regülasyon'a ve bağlayıcı şirket kurallarına uymalıdır. Bununla birlikte Türkiye'deki şirket, bağlayıcı şirket kuralları kapsamında kendisine aktarımı yapılan verileri, üçüncü bir kişiye aktarırken de Regülasyon'da yer alan veri aktarımı yükümlülükleri ile bağlıdır.

Özellikle Regülasyon m.47/2/f uyarınca, AB'deki müşterek sorumlu üye şirket, hukuka aykırılığın kendisi ile hiçbir ilgisinin bulunmadığını kanıtlarsa sorumluluktan kurtulabilmektedir. Türk hukukunda da KVKK'da bağlayıcı şirket kuralları kapsamında, sorumluluğun kime ait olduğunun ve kurtuluş kanıtı getirilip getirilmeyeceğinin yasa ile düzenlenmesi gerekmektedir.

[335] Toparlak, s.42.

Regülasyon m.47/2-k uyarınca grup şirkette, bağlayıcı şirket kurallarının değişmesi halinde bunun raporlanması ve veri koruma kuruluna bildirilmesi gerekmektedir. Veri koruma kuruluna bu bildirimi yapacak şirket içindeki görevliler belirlenmeli ve daha önemlisi, bu değişiklik bağlayıcı şirket kurallarını esastan etkiliyorsa yetkili veri koruma makamına başvurulmalı ve yeni bir onay safhasının gerekip gerekmediğine ilişkin görüş alınmalıdır. Kurul duyurusunda bu değişikliklerin raporlama mekanizmasına yer verilmişse de, bağlayıcı şirket kurallarının esasını etkileyecek değişikliklerde Kurul'dan onay alınmasına ilişkin düzenleme yer almamaktadır.

Grup şirketin üçüncü ülkedeki üyeleri, bağlayıcı şirket kurallarında verilen taahhütlere bakmalı ve bağlı oldukları ulusal mevzuatla karşılaştırma yapmalıdırlar. Üçüncü ülkedeki veri koruma yasalarına ilişkin bu karşılaştırma, grup şirketin uyumluluk departmanı ve veri koruma görevlisiyle paylaşılmalıdır (Regülasyon m.47/2-m). Buna dair Kurul duyurusunda hüküm bulunsa da, bunun işlerliğinin nasıl denetleneceğine dair düzenleme yapılmamıştır. Bağlayıcı şirket kurallarında verilen taahhütlere aykırı hükümlerin tespit edilmesi halinde Kurul'un haberdar edilmesi gerekir. Bununla birlikte, bağlayıcı şirket kurallarının uygulanması açısından geçerli olan yasal düzenlemenin KVKK olduğu açık şekilde yazılmalı ve Kurul, yetkili makam şeklinde ifade edilmelidir.

Bağlayıcı şirket kurallarında, üçüncü ülkelerin iç mevzuatından kaynaklanabilecek idari denetim otoritelerinin denetim yetkisine ilişkin bir istisna yer almaktadır. Bahse konu istisna "her halükârda demokratik bir devlet düzenlemesinin gereklerini aşmayacak şekilde" ibaresiyle, belirsiz bir şekilde belirtilmiştir.

Bağlayıcı şirket kurallarına ilişkin şirketlerin irtibatlı oldukları veri koruma kurulları ilgili ülkenin veri koruma kurulu olmaktadır. Regülasyon kapsamında (m.70) Avrupa Veri Koruma Kurulu'nun Regülasyonun düzenli uygulanmasını sağlamak ve Avrupa Birliği Komisyonu'na; veri sorumluları, veri işleyenler ve denetim kurumları arasındaki veri aktarımlarına dair bağlayıcı şirket kurallarının şekli ve usullerine dair tavsiyelerde bulunmak gibi denetim görevleri bulunmaktadır. İlgili ülkelerdeki veri koruma kurullarının ülkemizdeki Kurul'un görevini yerine getirdiği söylenebilse de, bu durumda denetim organı olabilecek bir üst kurulun ülkemizde bulunmadığı ifade edilebilir.

Regülasyon m.45 gereğince, Avrupa Birliği Komisyonu bazı ülkelerde kişisel veri aktarımında Regülasyon'a eşdeğer bir korumanın bulunduğuna dair karar verebilmektedir[336].Türk hukukunda Kurul'un veri aktarımı yapılacak güvenli ülkeleri belirlememesi de bir sorun oluşturmaktadır.

Kanaatimizce başka ülkelere kişisel veri aktarımının yapıldığı önemli bir aktarım yolu olan bağlayıcı şirket kurallarına ilişkin hüküm ve düzenlemelerin Kurul duyurusu ile değil, Regülasyon'da olduğu gibi kanuni bir düzenleme ile yapılması gerekmektedir.

[336] Yörük, s.108.

DÖRDÜNCÜ BÖLÜM

AB HUKUKUNDA KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI VE BAĞLAYICI ŞİRKET KURALLARI

I. AB HUKUKUNDA ULUSLARARASI VERİ AKTARIM YÖNTEMLERİ

AB dışına veri aktarımı, sınır ötesi veri aktarımı olarak ta adlandırılmakta olup[337] bu veri aktarımı, daha önce 95/46 sayılı Direktif m.25 ve 26'da düzenlenmiş olupyeterli koruma temin etmeyen üçüncü ülkelere, kural olarak, veri aktarımı yasaklanmıştır. Ancak bu hükümler, esnek olmayan bir yapıya sahip olmaları ve uygulanmada zorluklar çıkarması sebebiyle doktrinde eleştirilmiştir[338]. Bilhassa AB ile ABD arasında yapılan veri aktarımının her iki taraftaki ticari faaliyetlere menfi etkisi nedeniyle Avrupa Komisyonu "*Güvenli Liman Gizlilik İlkeleri*"ni[339] kabul etmiştir. Bu İlkeler, bunları kabul eden ve bu ilkeler kapsamında faaliyet yürüten ABD şirketleri ile AB arasında yeterli korumanın sağlandığını göstermekte olup bu şekilde veri aktarımının yapılmasına olanak tanımıştır[340]. Ancak ABAD, Ekim 2015 tarihli Schrems kararı[341] ile Güvenli Liman Anlaşmasını geçersiz hale getirmiştir.

AB haricine kişisel veri aktarımı, yani üçüncü ülkeler ile uluslararası örgütlere gerçekleştirilecek aktarımlar Regülasyon m.40 ila 50 arasında yer almıştır. Regülasyon da, Direktif'te olduğu gibi, yeterli koruma düzeyi sağlayan üçüncü ülkelere kişisel veri aktarımına izin vermektedir (Regülasyon m.45). Bunun yanında, Komisyon'un

[337] Lambert, Paul, Understanding the New European Data Protection Rules, Taylor & Francis, 2017, s.341.
[338] Küzeci, 2019, s.175; Moerel, s.118.
[339] Commission Decision of 26 July 2000, 2000/520/EC.
[340] Küzeci, 2019, s.180.
[341] Maximilian Schrems v Data Protection Commissioner, C-362/14, karara ilişkin ayrıntılı bilgi için bkz. Marques, João, "And they built a crooked harbour" – the Schrems ruling and what it means for the future of data transfers between the EU and US", UNIO - EU Law Journal, C. 2, S. 2, June 2016, s.54-70.

yeterlilik kararı bulunmadığı durumlarda bile, m.46 gereğince veri sorumlusunun veya veri işleyenin uygun güvenlik tedbirlerini alması ve verilerin aktarımının yapılacağı ülkede, veri özneleri açısından hakların ve etkili hukuk yollarının getirilmiş olması şartıyla aktarım olanaklıdır. Bunların haricinde m.47'de, anılan uygun güvenlik tedbirlerinden biri olarak bağlayıcı şirket kurallarına dair ilkeler düzenlenmiş, m.48 ve 49'da ise AB hukukunda izin verilmeyecek veri aktarımları ve istisnai durumlar düzenlenmiştir.

A. AB Hukukunda Açık Rıza Kavramı

Regülasyon'da rıza; kişinin özgür iradesi ile, belli bir konuda, bilgisi kapsamında ve yoruma açık olmayacak biçimde, verilerinin işlenmesine ilişkin izni anlamına gelen bir hareket şeklinde ifade edilmiştir (m.4/11)[342]. Regülasyon'da rıza ve açık rıza kavramları için bir ayrım bulunmamaktadır. Şahsın, verilerinin işlenip işlenmemesi ve işleniyorsa hangi durumlarda işleneceğine ilişkin rızasını vermesi gerekmektedir. Açık rızanın, olağan rızadan farkı, yazılı, sözlü ya da elektronik yolla iletilmiş açık bir beyan içermesidir[343]. İlgili kişi rıza beyanını, açık şekilde kabul ettiğini gösteren bir hareketi ile verebilmektedir. Açık rızada ise mutlak surette, onay ve rızanın kelimelerle ifade edilmesi gerekmektedir[344].

ABAD da Planet kararında hukuka uygun bir rıza için aktif bir eylem aramaktadır[345].Günümüzde rıza bir kutucuğa tıklama suretiyle de verilebilmektedir. Ancak önceden işaretlenmiş kutucuklar kişinin rızası şeklinde kabul edilemez.

Rıza, Regülasyon m.6 gereğince kişisel verilerin işlenmesinde hukuka uygunluk nedenleri arasında önemli bir role sahiptir. Kaldı ki rıza, şahsın verisinin işlenmesine ilişkin özgür iradesiyle vereceği, belli, bilgilendirmeye dayalı ve kesin şekilde hüküm altına alınan bir hukuka uygunluk nedenidir. Açık rıza koşulu ise sadece Regülasyon m.9/2/a kapsamında yer alan hassas kişisel verilerin işlenmesi için aranmaktadır. Bununla birlikte Regülasyon m. 22/2/c gereğince veri ilgilisi şahıs, otomatik şekilde veri işlenmesi için de açık rızasını göstermelidir.

---

[342] Yörük, s.61; Turan, s.177.
[343] Çekin, 2020, s.79; Başalp, s.39.
[344] Toparlak, s.77.
[345] C - 673/17, para.62.

Regülasyon m.7'de rızanın geçerliliği için birçok şart getirilmiştir. Bu şartlar, rızanın şekli veya içeriği ile ilgili olmayıp, rızanın varlığının hangi koşullar altında mümkün olabileceğini belirler. Bu manada öncelikle, kişisel verilerin işlenmesi rızaya dayanıyorsa, veri sorumlusunun, ilgili kişinin bu işleme faaliyetine rıza verdiğini gösterebilmesi gerekir (m.7/1). Ayrıca rızanın bir hizmetten yararlanma bakımından ön şart olarak düzenlenmesi durumunda, özgür iradenin sakatlanacağı ve rızanın geçersiz kabul edileceği de ifade edilmiştir[346]. Bu bağlamda Kurul'un Amazon Türkiye'ye ilişkin yeni kararında, ilgiliden elde edilen açık rızanın hizmet verilmesine önşart şeklinde düzenlendiğinden söz edilmiş ve özgür iradenin sakatlandığına karar verilmiştir. Kurul, Bahse konu gerekçe ve Kanun'a diğer aykırılıklar nedeniyle anılan şirket hakkında idari para cezası uygulanmasına karar vermiştir[347].

Farklı konuları içerecek şekilde yazılı bir beyan içinde rıza, açıklanacaksa rıza talebi, başkaca konulardan açık şekilde ayırt edilebilecek biçimde, kolay, anlaşılır ve erişilebilir şekilde yazılmalı, sade ve açık bir dil tercih edilmelidir. Rıza beyanında, Regülasyon'a aykırı bulunan bölümler varsa, bu bölümler bağlayıcı değildir (Regülasyon m.7/2).

Rıza istenildiğinde daima geri alınabilir. Fakat rızanın geri alınması geriye değil, ileriye etkilidir. Rıza geri alınmadan önce, bu rızaya istinaden gerçekleştirilen işleme faaliyetleri hukuka uygun olacak ve geri almadan etkilenmeyecektir. İlgili kişiler, rıza vermeden evvel bu konuda bilgilendirilmiş olmalıdır[348]. Regülasyon'a göre, rızadan feragat veya geri alma da rızanın beyan edilmesi kadar kolay olmalıdır (m.7/3). Rızanın geri alınabilmesi, ilgili kişilerin verilerinin geleceğini tayin etme hakkının doğal bir neticesidir.

Rızanın özgür şekilde beyan edilip edilmediğinin tespitinde, başka konuların yanı sıra, bir sözleşmenin yerine getirilmesinin, ifa için gerekmeyen kişisel verilerin işlenmesinin rızasına bağlanıp bağlanmadığı önemlidir (Regülasyon m.7/4)[349]. Veri sorumlusu, sözleşmenin ifası açısından gereken ve işleme eylemleri kapsamında verilmiş rızayı, bu amaçların dışında bir işlem yapacak biçimde genişletemez.

---

[346] Regülasyon, Gerekçe, m.42.
[347] Kişisel Verileri Koruma Kurulu, Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili 27/02/2020 Tarihli ve 2020/173 Sayılı Karar, bkz.; https://www.kvkk.gov.tr/Icerik/6739/2020-173, E. T.: 13.07.2021.
[348] Çekin, 2020, s.84.
[349] Çekin, 2020, s.84.

Görüldüğü üzere, Regülasyon'un aksine KVKK, rıza ve açık rıza ayrımı yapmakta ve açık rızayı veri işleme sebebini hukuka uygun hale getiren rıza olarak esas almaktadır[350]. Bu çerçevede, bağlayıcı şirket kuralları taahhüdünde bulunan ülkemizdeki üye şirket, hukuka uygunluk nedeni olarak açık rızayı ileri sürüyorsa, m. 5/1'e uygun biçimde rızanın alınmasını sağlamalıdır[351].

B.Avrupa Birliği Komisyonu'nun Uygunluk/Yeterlilik Kararı Çerçevesinde Aktarım

Regülasyon'un uluslararası veri aktarımına ilişkin hedefi, Regülasyon'da veri ilgilisi şahıslara verilen koruma düzeyinin verilerin aktarımının yapıldığı ülkede de korunmasıdır. Bu kapsamda öncelikle verinin aktarılacağı üçüncü ülkede Regülasyon kuralları çerçevesinde karşılıklı/yeterli bir korumanın bulunup bulunmadığı değerlendirilmektedir. Yeterli veri koruma seviyesi bulunan üçüncü ülkelere verilerin serbestçe aktarımı Regülasyon m.45 hükmünde düzenlenmiş olup, AAD de "yeterli koruma düzeyi" terimini, üçüncü ülkenin hak ve özgürlüklere AB hukukunun sağladığı teminatlarla eşit seviyede korumanın vaat edilmesi manasına geldiğini ifade etmiştir. Bahse konu koruma düzeyini temin etmede izlediği yolun AB'de uygulananlardan farklı olabileceği üçüncü bir ülkenin yeterlilik standardı, AB düzenlemelerinin tamamen aynı şekilde izlenmesini gerektirmemektedir.[352]

Regülasyon m.45 gereğince, Avrupa Birliği Komisyonu bazı ülkelerde kişisel veri aktarımında Regülasyon'a eşdeğer bir korumanın bulunduğuna dair karar verebilmektedir[353]. Anılan Regülasyon maddesi, Direktif m.25'de geliştirilmiştir ve bu madde, Komisyonun veri aktarımı yapılacak ülkede yeterli koruma olup olmadığı incelemesi yaparken, dikkate alacağı kriterleri içermektedir. Bu karar, üçüncü ülkeler bakımından 'AB ile uyum göstergesi' şeklinde görülmektedir. Ayrıca AB haricinden alınacak veri işleme hizmetleri için tercih sebebi olmaktadır[354].

---

[350] Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP 187, 13 Temmuz 2011, s.8, 21.
[351] Toparlak, s.78.
[352] Avrupa Komisyonu (2017), Komisyon'dan Avrupa Parlamentosu ve Konsey'e İleti "Küresel Dünyada Kişisel Verilerin Alışverişi ve Korunması" COM (2017)7 final 10 Ocak 2017, s.6, bkz: https://ec.europa.eu, E.T.:14.08.2022.
[353] Yörük, s.108.
[354] Toparlak, s.28.

Üçüncü ülkede yeterli korumanın olduğuna dair yani yeterlilik kararı için göz önüne alınacak kıstaslar Regülasyon m.45/2'de gösterilmiştir. Bu kriterler sayma şeklinde tespit edilmemiştir ve AB Komisyonu yaptığı somut değerlendirmede ilave olarak diğer noktaları da dikkate alabilmektedir. Regülasyon m.45/2'de üç değerlendirme kıstası gösterilmiştir. İlki, üçüncü ülke ya da uluslararası kuruluş veya örgütün iç hukukundaki veri koruma düzenlemelerini ele almaktadır. İkincisi, bağımsız bir yetkili veri koruma idaresinin (data protection authority) var olup olmadığının ve uygulamada veri koruma hukukunun etkinliğinin incelenmesidir. Son kriter olarak, üçüncü ülkenin veri koruması mevzuatı ve uygulamasının uluslararası düzenlemelerle uyumlu olup olmadığı değerlendirilmektedir[355].

Yeterlilik kararı Regülasyon gereğince sadece belli bir bölgeyle ya da üçüncü ülkedeki belli bir sektörle kısıtlanabilmektedir. Bu kapsamda örneğin Avrupa Birliği ile ABD arasında yapılan *Safe Harbor* ve *Privacy Shield* anlaşmaları önemli örnekler olmuşlardır.

Komisyon, yaptığı inceleme neticesinde yeterlilik kararı verirse, bu karar, üçüncü ülkedeki veya uluslararası kuruluştaki tüm gelişmeleri göz önüne alınarak, dört yılda bir yeniden değerlendirilecektir (Regülasyon m.45/3,4). Komisyon değerlendirme neticesinde üçüncü ülke veya uluslararası kuruluşun temin ettiği korumanın yetersizleştiği kanısına ulaşırsa, kararını gerektiği ölçüde geri alabilir, değişiklik yapabilir veya askıya alabilir. Ancak bu kararı, geriye etkili olmayacaktır (Regülasyon m.45/5). 95/46 sayılı Direktif'in geçerli olduğu sürede verilmiş yeterlilik kararları da Komisyon tarafından Regülasyon ilke ve düzenlemelerine göre değişiklik yapılmadıkça veya kaldırılmadıkça geçerlidir (Regülasyon, m.45/9).

Regülasyon m.45/8'e göre Komisyon, AB Resmi Gazetesi'nde ve internet sayfasında, yeterli veri koruma temin eden üçüncü ülkelerin, bu ülkelerin sektörleri veya uluslararası örgütlerinin bir listesini yayınlar. 2018 yılında Andorra, Arjantin, ticari işletmeler açısından Kanada, Guernsey, Faroe Adaları, Man Adaları, İsrail, Yeni Zelanda Uruguay ve İsviçre'ye ilişkin geçerli yeterlilik kararı vardır [356].

[355] AB Komisyonu üçüncü ülkelere veri aktarımında yeterlilik kararı, bkz.; https://ec.europa.eu/info/law/lawtopic/data-protection/international-dimension-data-protection/adequacy-decisions_en, E. T:13.07.2021.

[356] European Union Agency For Fundamental Rights, Handbook on European Data Protection Law, Luxembourg, 2018, s.255, bkz. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, E.T.:13.07.2021

C.Yeterli Korumaya Tabi Aktarımlar

1. İdari Düzenlemeler

Veri aktarımının yapılacağı üçüncü ülkede, yeterli korumanın olduğu tespit edilememişse, tarafların uygun güvenlik tedbirlerinden birini temin etmeleri gerekmektedir. Regülasyon m.46'da bulunan bu tedbirler, aslında AB içindeki hak ve yükümlülüklerin veri aktarımının yapıldığı ülkede de korunacağı garantisini getirmektedir. Bununla birlikte bu tedbirler, bu aktarım sürecinin AB üyesi ülkelerdeki yetkili veri koruma makamlarınca takip edilmesi ve denetlenmesini de gerektirmektedir. Regülasyon'da getirilen yedi güvenlik tedbiri, iki ana başlığa ayrılmaktadır. Birinci grupta, AB'deki veri koruma makamlarının iznine bağlı olan tedbirler bulunmaktadır. Bu tedbirler, veri aktarımının yapıldığı üçüncü ülkedeki veri sorumlusu veya işleyen ile akdedilecek sözleşme hükümleri (Regülasyon m. 46/3/a) ve idari makamlarca veri sahiplerinin haklarının dahil edildiği maddelerdir (Regülasyon m. 46/3/b). Bu gruptaki tedbirler, daha külfetli ve alınması yavaş olduğundan, pratikte çok uygulanmamaktadır. İkinci gruptaki önlemler ise Regülasyon m. 46/2'ye göre, kamu makamları arasında hukuki bağlayıcılığı olan araçlar ile Avrupa Birliği Komisyonu'nca kararlaştırılan veya ülkelerin veri koruma makamlarınca tespit edilip Komisyon tarafından onaylanan standart veri koruma maddeleridir[357]. Bu iki önlem haricindeki önlemler; bağlayıcı şirket kuralları, davranış kuralları ve sertifikalardır.

2.Standart Veri Koruma Hükümleri

Standart veri koruma hükümleri Regülasyon m. 46/2/c'de üçüncü ülkelerde bulunan kişi ve şirketlere veri aktarımı amacıyla uygun bir güvenlik tedbiri olarak kabul edilmektedir[358]. Bu hükümler, başka sözleşmesel yükümlülüklerden daha önce uygulanır ve üçüncü ülkelerde de Regülasyon kapsamına göre verilerin korumasını sağlamaktadır. Bu tedbir için Komisyon tarafından yapılmış sözleşmeler veya üçüncü kişiler tarafından önerilerek Komisyonca onaylanan sözleşmeler kullanılabilir. Doktrinde Komisyonca düzenlenen 'standart sözleşme maddeleri' ismiyle hazırlanmış

[357] Toparlak, s.36.
[358] Çekin, 2020, s.177 vd.; Turan, s.403 vd.

üç sözleşmenin bulunduğu belirtilmiştir[359]. Bu üç sözleşme, çeşitli veri işleme faaliyetleri için yapılmış ve Regülasyon m.46/2/c gereğince uygun güvenlik tedbiri önlemi kabul edilmektedir[360].

Direktif'in yürürlükte olduğu dönemde de var olan bu sözleşmeler, veri aktarımının hukuka uygun yapıldığının yetkili merciler tarafından denetlendiğini göstermektedir. Standart veri koruma hükümleri, hızlı uygulanabildiği ve idari süreçlerin belirsizliğini de ortadan kaldırdığından taraflara da yüksek bir koruma temin etmektedir.

Komisyon tarafından hazırlanan standart sözleşme maddeleri güncellenirken, halen yerleşik veri aktarımı sistemleri ve gizlilik kuralları olan, büyük çaptaki küresel kuruluşların gereksinimlerine cevap verememektedir. Ayrıca bu sözleşmeler, bulut bilişim sistemleri gibi teknolojik yenilikler noktasında eksiktir. Bununla birlikte, standart sözleşmelerin tek bir amaç taşıması, çeşitli amaçlarla gerçekleştirilen veri aktarımlarında birden çok sözleşme yapılmasına neden olmakta ve şirketlerin gerekenden daha fazla taahhüt vermesine neden olmaktadır. Bu hallerde, şirketlerin kendi kurallarına uygun olarak düzenlenebilen ve hemen hemen her türlü veri aktarımı sürecini taahhüt eden başka alternatif yöntemler daha avantajlıdır. Bağlayıcı şirket kuralları da belli durumlarda daha zorlu bir metot kabul edilebilecek standart veri koruma maddelerine seçenek oluşturabilmektedir[361].

ABAD'ın 16 Temmuz 2020 tarihli *Schrems II* kararında, standart sözleşme hükümlerinin uygulamasına ilişkin önemli açıklamalar bulunmaktadır. Bu kararın akabinde standart sözleşme hükümleri içeren sözleşmeleri imzalayan taraflara, üçüncü ülkelerdeki veri koruma kurallarını araştırma sorumluluğu yüklenmiştir. Ayrıca üçüncü ülkedeki kamu makamlarının aktarılan veriler üstündeki denetim yetkisini de araştırmakla taraflar yükümlü kılınmıştır. Yapılan inceleme neticesinde standart sözleşme hükümlerinin ifa edilemeyeceği tespit edilirse, sözleşme feshedilmeli ve/veya aktarım durdurulmalıdır[362]. Bu karar ayrıca, AB'deki veri koruma

[359] Toparlak, s.38.
[360] European Commissions (EC), Standard Contractual Clauses, bkz. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en#:~:text =On%204%20June%202021%2C%20the,subject%20to%20the%20GDPR)%3A, E.T.: 13.07.2021.
[361] Bowman, Gufflet, s. 257-261; Moerel, s.26.
[362] C-311/18, para. 140.

makamlarının da denetim yetkisini kuvvetlendirmektedir. AB veri koruma makamları, üçüncü ülkede standart sözleşme hükümlerinin korunmadığını belirlerlerse veri aktarımını durdurabilir ya da yasaklayabilir[363].

3.Davranış Kuralları

Davranış kuralları (codes of conduct) sektörel bir düzenleme olup AB hukukunda Regülasyon m.40'da düzenlenmiştir. Bu kurallar; veri sorumlusu veya işleyen üyeleri temsil eden sektör ya da ticari birliklerinin, o sektörün gereksinimlerini dikkate alarak düzenledikleri ve onaydan geçmiş araçlardır[364]. Bu kuralları hazırlayan Birliğe üye olan veri sorumluları ya da işleyenler isterlerse, bunlara uymayı tam olarak taahhüt edip, kendileri açısından bu kurallara hukuki bağlayıcılık kazandırabilirler. Bu özelliği nedeniyle davranış kuralları, hesap verebilirliği arttıran isteğe bağlı uyum araçlarıdır. Davranış kuralları, veri aktarmayı da kapsayacak şekilde, bütün veri işleme süreçlerini içerecek biçimde hazırlandığından, Regülasyon m.46/2/e'de üçüncü ülkelere aktarımda uygun bir güvenlik tedbiri şeklinde kabul edilmektedir. Bir davranış kuralının Regülasyon'a göre uygun güvenlik tedbiri olarak kabul edilebilmesi için üç koşula sahip olması gerekir. Bu koşullar; Regülasyon m.40'da yer alan veri koruma ilkelerini taahhüt etmesi; Regülasyon m.55 gereğince yetkili veri koruma makamı ya da AB Komisyonunca onaylanması ile hukuki bağlayıcılığının bulunmasıdır.

Davranış kuralları, sadece belli bir ülkede uygulanacaksa o üye ülkenin veri koruma otoritesine başvuru yeterlidir. Ancak o davranış kuralları AB içinde geçerli olacaksa, üye ülke yetkili makamı, kendisine verilen davranış kurallarını Regülasyon m.63 kapsamında düzenlenen uyum mekanizması çerçevesinde AB Veri Koruma Kurulu'na sunar[365].

Davranış Kuralları, meslek odaları ya da birlikler gibi kurumlar tarafından sektör gözetilerek düzenlendiğinden, ilgili sektörün gereksinimleri kapsamında geliştirilirler. Bununla birlikte davranış kuralları, oluşturuldukları ticari birlikteliğin üyeleri, veri sorumluları veya işleyenleri açısından çabuk ve göreceli olarak hesaplı

[363] C-311/18, para.113, 114.
[364] Çekin, 2020, s.179.
[365] Çekin, 2020, s.179-180.

bir uyum yöntemidir. Öte yandan, yetkili veri koruma otoritesi tarafından onaya tabi tutulduklarından, bu kurallara uymayı vaat eden veri sorumluları ya da işleyenler, yetkili makam gözünde güvenilir olarak kabul edilmektedir[366]. Bu manada davranış kuralları, şeffaflık ve hesap verebilirlik ilkelerinin de gerçekleşmesine katkıda bulunmaktadır.

Davranış kuralları, veri sorumlusu ya da işleyenin üye olduğu meslek odaları veya birlikler tarafından hazırlamışsa, bunun veri sorumlusu şirket tarafından taahhüt edilmesi birçok bakımdan yararlıdır. Fakat veri sorumlusu veya işleyenin bilhassa sürdürmeyi istediği yerleşik kuralları ya da özel bir teşkilatlanması varsa, veri aktarımı amacıyla farklı uygun güvenlik tedbirleri dikkate alınabilir.

4.Sertifikasyon Mekanizması

Sertifikalar (certification), veri sorumlusu ya da işleyenin yaptığı faaliyetlerin Regülasyon'a uyumlu olduğunu gösteren damga/mühürlerdir. Sertifikalar, Regülasyon m.42/5 gereğince AB üyesi devletlerin veri koruma makamları ya da Regülasyon m.43 gereğince yetkili sertifika kuruluşlarınca tarafından verilmektedirler[367]. Yukarıda belirtildiği gibi Regülasyon m.63 gereğince AB Veri Koruma Kurulu tarafından da sertifika verilebilmektedir[368]. Üçüncü ülkelerdeki veri sorumlusu ya da işleyenlerin bu sertifikaları alması durumunda, sertifika, AB'den bu ülkeye gerçekleştirilecek veri aktarımlarında Regülasyon m.46/2/f uyarınca uygun güvenlik önlemi niteliğindedir[369].

Sertifika almayı talep eden üçüncü ülkelerdeki veri sorumluları ya da işleyenlerin yerine getirmeleri gereken dört yükümlülük bulunmaktadır[370]. Sertifika kıstasları, AB Komisyonunca onaylandığı biçimde tespit edilen veri koruma ilkelerini kapsamalıdır. Sertifika, Regülasyon'un yetkili kıldığı bir kurum ya da AB Veri

[366]Information Commissioner's Office, Guide to Codes of Conduct, bkz. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-thegeneral-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/, E.T.: 14.07.2021.
[367] Dove, Edward, The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era, The Journal of Law, Medicine & Ethics, 46, 2018, s.1025.
[368]European Data Protection Seal, bkz. https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en, E.T.:14.7.2021.
[369]Çekin, 2020, s.181.
[370]Toparlak, s.41-42.

Koruma Kurulunca verilmelidir. Üçüncü ülkedeki veri sorumlusu veya işleyen, Regülasyon'un getirdiği yükümlülüklere dair taahhüt vermelidir. Son olarak sertifika kıstaslarının, üçüncü ülkede bulunan veri sorumlusu ya da işleyenler açısından hukuki bağlayıcılığının bulunması koşulu aranmaktadır.

Sertifikanın AB'de kurulu bir veri sorumlusu ya da işleyen için getirdiği en önemli fayda, olası denetim giderlerinin azalmasıdır. Bununla birlikte veri sahiplerinde oluşturulan güven, bir pazarlama yararı da oluşturabilir[371]. Üçüncü ülkelerde bulunan veri sorumluları ya da işleyenleri açısından getirdiği fayda daha büyüktür. Çünkü AB'den o üçüncü ülkeye gerçekleştirilecek veri aktarımları amacıyla uygun bir güvenlik tedbirinin bulunması, üçüncü ülkedeki sorumluları tercih edilebilir bir alternatif durumuna sokacaktır. Hatta, veri işleme süreçlerinde maliyetleri düşürmek için dıştan hizmet alındığı (outsource) hallerde, üçüncü ülkelerdeki sorumlular açısından sertifikaların ticari önemi bulunmaktadır.

Regülasyon öncesi dönemde de sertifikalar, AB hukukunda geniş bir şekilde kullanılmıştır. Hatta AB içinde 2013 yılına kadar verilmiş veri koruma sertifikaları incelendiğinde, altı farklı ülke tarafından verilmiş yaklaşık beş yüz sertifika olduğu anlaşılmaktadır[372]. Bu sertifikanın en yaygın olanı, Almanya tarafından verilen gizlilik mührü sertifikasıdır. Ancak doktrinde, bu yöntemin Regülasyon içinde tek bir şekilde düzenlemesi ve uygulanabilirliği bakımından eleştiriler yapılmaktadır[373].

Regülasyon, üçüncü ülkelere veri aktarılması amacıyla farklı uygun güvenlik tedbirleri belirlemiştir. Şirketler kendi özel durumları kapsamında değerlendirme yapmalı ve kendi ihtiyaçlarını karşılayanı seçilmelidir. Türkiye'deki şirketler açısından uygun güvenlik tedbirlerine göz atıldığında, bağlayıcı şirket kurallarının birçok açıdan önemli olduğu görülmektedir. Örneğin küresel ve çok uluslu bir grup şirketin Türkiye'deki üyesi veri sorumlusu ya da işleyene uygun güvenlik tedbiri özelliğindeki bağlayıcı şirket kuralları gönderilip, buna uygun hareket etmesi beklenecektir. Bu durumda Türkiye'deki üye şirket açısından bağlayıcı hale gelecek bağlayıcı şirket kurallarına bir uyum süreci başlatılacaktır. Diğer bir deyişle,

[371]GDPR Certification, bkz. https://www.eugdpr.institute/gdpr-certification/, E.T.:14.07.2021.
[372]Data Protection Schemes Active in Europe, bkz. https://www.researchgate.net/figure/Data-protectioncertification-schemes-active-in-Europe-in-2016_tbl1_305821630, E.T.: 14.07.2021.
[373]Lachaud, Eric, "Why the Certification Process Defined in the GDPR Cannot Be Successful", Computer Law & Security Review, C. 32, 2016, s.814–826.

Türkiye'deki üye şirket hem Türk hukukuna hem de bağlayıcı şirket kuralları yükümlülüklerine uygun hareket etmelidir[374].

Öte yandan, Türkiye'de yerleşik fakat AB'de üyeleri olan çok uluslu şirketin kendi bağlayıcı şirket kurallarını hazırlaması ve uygulaması da olanaklıdır. Bu durumda düzenlenecek bu kurallar, Türk hukuku bakımından küresel şirket içerisinde serbest veri akışını temin edecektir. Düzenlenen bu kuralların, AB'de yetkili bir kuruluştan Regülasyon m.46/2/f gereğince sertifikalı hale getirilmesi de akla gelebilir. Bu halde Türkiye'de düzenlenen bu kurallar, AB'den gerçekleştirilecek veri aktarımlarında da Regülasyon kapsamındaki uygun güvenlik tedbiri özelliği kazanacaktır.

II. BAĞLAYICI ŞİRKET KURALLARI

Bağlayıcı şirket kuralları, küresel grup şirketlerin kendi içindeki veri faaliyetleri ve aktarımlarında, yeterli ve eşit seviyede koruma vaat eden metinlerdir. Bu kurallar, grup şirket bünyesindeki tüm üyeler açısından bağlayıcı kabul edilir ve üyelerin bütün veri işleme eylemlerine uygulanır. Bağlayıcı şirket kurallarını kabul eden grup şirketin, veri işleme sürecini ve ihtiyaçlarını dikkate alması ve bunların yetkili veri otoritesi tarafından onaylanması gerekmektedir. Bu nedenle Regülasyon'a uygun ve eşit seviyede veri koruma vaat eden bu kurallar, grup şirket içinde serbestçe veri dolaşımını temin etmektedir[375]. Grup şirkette veri korumasını vaat eden bu kurallar, sadece AB hukukunda değil, başka hukuk sistemlerinde de bulunmaktadır[376].

A.Bağlayıcı Şirket Kurallarının Amaçları ve Yararları

Bağlayıcı şirket kuralları, grup şirketin veri aktarımında kendi ihtiyaçlarını karşılamak üzere hazırladığı kurallardır. Küresel grup şirketin içinde bulunan bütün şirket ve kuruluşlar açısından bağlayıcı şekilde hazırlanan kurallar metni, üyelerin her

[374]Toparlak, s.42.
[375]Masoch, Daniela Fábián "Why Should Companies Invest in Binding Corporate Rules?', The International Comparative Legal Guide to: Data Protection, 2019, bkz: https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, E.T.: 14.7.2021.
[376]Sullivan, Claire, 'EU GDPR Or APEC CBPR? A Comparative Analysis of The Approach of The EU And APEC To Cross Border Data Transfers And Protection of Personal Data İn The Iot Era', Computer Law and Security Review, C.35, 2019, s.382.

birinin Regülasyon'a uymasını sağlamaktadır. Regülasyon'da yer alan düzenlemelere bağlı şekilde hazırlanıp onaylatılmış bağlayıcı şirket kuralları, grup şirket içindeki veri aktarım faaliyetlerinde uygun bir güvenlik tedbiri kabul edilmektedir. Bu nedenle grup şirket yapısında bulunan bütün şirketler arasında serbest veri akışını sağlamaktadır[377]. Grup şirket içerisinde küresel çapta Regülasyon ile uyum içinde olan aynı veri koruma düzeyinin sağlanmasının, daha basit ve işleyen bir süreç oluşturduğu ifade edilmiştir[378]. Hatta, uyum süreci, çalışanlar tarafından daha kolay idare edilebilir ve ilgili kişiler tarafından daha rahat anlaşılabilir bir duruma gelir.

Getirdiği faydaları ile bağlayıcı şirket kuralları, uluslararası veri aktarımında uygun bir güvenlik tedbirinden daha fazlası haline gelmiştir. Şirkete özgü şekilde düzenlenip küresel çapta aynı koruma düzeyini taahhüt eden bağlayıcı şirket kuralları, çok uluslu şirketin tümünde saydam bir veri işleme uyum aşamasının da esasını oluşturabilir[379]. Grup şirketin tek amacı sadece şirket içerisinde serbest veri akışı yapmak ise daha küçük çaplı ve daha az maliyetli seçeneklere başvurabilir. Ancak bağlayıcı şirket kuralları, grup şirket içindeki tüm üye şirketlerin bütün veri işleme ve aktarım faaliyetlerini düzenleyen geniş bir uyum süreci gerektirmektedir.

Regülasyon m. 5/2 gereğince veri sorumluları, faaliyetlerinde veri işleme ilkelerinin gözetildiğine ilişkin hesap verebilirliği sağlamak yükümlüğünü üstlenmişlerdir[380]. Bu çerçevede, bağlayıcı şirket kurallarının amaçlarından biri de, grup şirket içinde verilerin işlenmesi ve aktarılması başta olmak üzere hesap verebilirliği sağlamakta ve bunu kanıtlamaktadır. Bu kapsamda bağlayıcı şirket kurallarının getirdiği en önemli yararlardan biri de mevzuat ile uyumu (compliance) göstermektir. Hatta hukuk yargılamalarında bağlayıcı şirket kurallarının geçerli bir ispat aracı olarak kabul edileceği belirtilmiştir[381].

Bağlayıcı şirket kuralları, veri gizliliği ve veri koruması gerekliliklerine ilişkin şirket içindeki bilinç, anlayış ve farkındalığı arttırmaktadır. Çünkü bağlayıcı şirket kuralları, şirket içinde veri koruması üzerinde yoğunlaşacak bir birimin

[377] Moerel, s.100.
[378] Toparlak, s.45.
[379] Bowman, Gufflet, s. 257-261.
[380] Moerel, s.33.
[381] Toparlak, s.46.

oluşturulmasına ve veri gizliliğinin şirket kültürü sayılmasına yol açabilmektedir[382]. Hatta, olası hukuka aykırılıkları önleyeceğinden, sonucunda ihlalden sorumlu olacak veri sorumlusu hakkındaki idari inceleme ve yaptırım kararları da azalacaktır[383].

Bağlayıcı şirket kuralları, grup şirketin veri idaresi kuralları ve ilkelerinin resmi hale getirilip yayınlanmasıdır. Bu kurallar, ilgili ülke veya uluslararası kurumların denetim otoriteleri, iş ortakları ve müşteriler önünde hesap verebilirliği sağlamaktadır[384]. Başka bir deyişle, bağlayıcı şirket kuralları olan şirketler, buna sahip olmayan rakipleri üzerinde ciddi bir rekabet avantajına sahiptir.

Bağlayıcı şirket kuralları, taahhütleri şirkete özel düzenlenerek onaylandıklarından ve yeni yapılanmalara ihtiyaç duyulduğundan nispeten masraflı ve uzun bir süreçtir. Fakat bu süreç sonucunda şirkete getirdiği yararlar ve şirketin ihtiyaçları değerlendirilerek, bu kuralların düzenlemesine gerek bulunup bulunmadığına karar verilmelidir[385].

B. Bağlayıcı Şirket Kurallarının Tarihsel Gelişimi

Günümüzde veri aktarımları, dijitalleşmenin etkisi ile internet üzerinden veya özel bilgisayar ağlarından yapılmaktadır. Dijital alandaki bu gelişmeler, küresel şirketlerin veri yönetim süreçlerini de etkilemiştir. Küresel grup şirketleri, maliyetten tasarruf veya pratik gerekçelerle, yapılandıkları her ülkede yerel bilgi işlem sistemleri kurmamaktadırlar. Bununla birlikte, grup şirket bünyesindeki üye şirketler arasında internet ya da özel bir ağ üzerinden sürekli bir veri akışı bulunmaktadır.

Öte yandan, dinamik yönlendirme ve bulut bilişim sistemlerinin yaygın hale gelmesiyle veri aktarımı konusundaki sorunlar artmıştır. Bulut bilişim sistemlerinde veriler, bu sistemin niteliği gereği bir 'bulutta' işlenmekte ve statik bir biçimde belli bir yerde tutulmamaktadırlar. Dinamik yönlendirme sistemi ise, verilerin önceden konulmuş bir yörünge üstünde kalan ağ içinde işlendiği statik yönlendirmenin zıttı özelliğini taşımaktadır. Yani, dinamik yönlendirme sonucu verilerin çevrimiçi nereye

[382]Masoch, Daniela Fábián "Why Should Companies Invest in Binding Corporate Rules?', The International Comparative Legal Guide to: Data Protection, 2019, bkz: https://iclg.com/firms/fabian-privacy-legal/daniela-fabian-masoch, E.T.:14.7.2021.
[383]Toparlak, s.46.
[384]Moerel, s.175.
[385]Kulezsa, Joanna, 'Transboundary data protection and international business compliance', International Data Privacy Law, C. 4, S. 4, 2014, s. 298 – 306; Moerel, s.108.

gönderildiği öngörülememektedir[386]. Bu nedenlerle, bu sistemlerdeki verilerin internet üstünden yönlendirilerek aktarıldığı ve depo edildiği ülkeler tahmin edilemeyebilir. Değişik ulusal mevzuatlara bağlı olan küresel şirketlerin veri aktarımının, şeffaf ve tek uygulamaya yapılacak şekilde yapılması önem arz etmektedir. Direktif döneminde küresel çaplı grup şirketlerin veri aktarımlarındaki sorunlara çözüm bulmak amacıyla, bağlayıcı şirket kurallarının AB hukuku içinde gelişimi başlamıştır.

Bağlayıcı şirket kuralları, Direktif'in yürürlükte olduğu dönemde m.29 Çalışma Grubu kararlarıyla ortaya çıkmıştır. Direktif m.26 ve m.29 kapsamında md. 29 Çalışma Grubu kararlarıyla oluşturulan bağlayıcı şirket kuralları, Direktif'te bu adıyla yer almamıştır. Fakat bu dönemde gerek doktrin gerekse uygulamada bağlayıcı şirket kuralları adıyla adlandırılmıştır[387]. Direktif döneminde m. 29 Çalışma Grubunca bağlayıcı şirket kurallarına ilişkin kataloglar ve kılavuzlar yayınlanmış ve sonra Daimler Crysler şirketinin taahhütleri ilk bağlayıcı şirket kuralları olarak onaylanmıştır.

Direktif içinde yazılı şekilde yer almayan bağlayıcı şirket kuralları, yukarıda söz edilen davranış kurallarından geliştirilmiş ve ilk kez Regülasyon içinde yasal bir düzenlemeye kavuşmuştur. Regülasyon'da grup şirketlerin veya ekonomik işbirliği durumundaki teşebbüslerin bağlayıcı şirket kuralları düzenlemelerinden faydalanabileceği yer almış ve m.47 ile geçerlilik hüküm ve koşulları tespit edilmiştir. Direktif döneminde onaylanmış bağlayıcı şirket kuralları, Regülasyonun yürürlüğe girmesinden sonra da geçerli kabul edilmiştir[388].

C. Bağlayıcı Şirket Kurallarının Konu Bakımından Uygulanması

Bağlayıcı şirket kuralları, niteliğine bakıldığında üçüncü ülkelere veri aktarımı amacıyla uygun güvenlik tedbirlerinin sıralandığı Regülasyon m.46 kapsamına girmektedir. Bu hüküm, AB'den ve AEA'ndan üçüncü ülkelere aktarımı yapılan kişisel verileri hüküm altına almaktadır. Bu sebeple bağlayıcı şirket kuralları da esas olarak AB ve AEA'dan üçüncü ülkelere aktarılan kişisel verilere uygulanmaktadır. Başka bir deyişle şirketler, hazırlayıp onaylattıkları bağlayıcı şirket kurallarının

[386]Toparlak, s.47.
[387]Toparlak, s.48.
[388]Direktif döneminde hazırlanıp onaylanan bağlayıcı şirket kuralları listesi için bkz. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841, E.T.:14.07.2021.

konusu olan kişisel verileri, sadece AB ve AEA'dan aktarılan kişisel verilerle kısıtlayabilirler.

Bağlayıcı şirket kuralları, müşteri verileri gibi sadece belli bir kişisel veri kategorisiyle de sınırlanabilmektedir. Bu halde standart veri koruma maddeleri gibi başka veri grupları açısından diğer koruma veya uygun güvenlik tedbirleri getirilmelidir. Çünkü bağlayıcı şirket kuralları, üçüncü ülkelere veri aktarılırken başvurulacak uygun bir emniyet tedbirinden çok daha ötedir. Bu kurallar, kapsamlı taahhütler barındırmakta ve uzun süreli uyum projelerinin uygulanmasına ihtiyaç göstermektedirler. Bu çerçevede konu açısından sınırlama getirilmesi talep edilebilmektedir[389].

D. Bağlayıcı Şirket Kurallarının Kişi Bakımından Uygulanması

Regülasyon'da tanımların yer aldığı m.4'e göre, grup şirketler veya ekonomik işbirliği içindeki teşebbüsler, bağlayıcı şirket kuralları düzenleyebilirler. Regülasyon m.4/20'deki bağlayıcı şirket kuralları tanımında veri sorumlusu ve veri işleyen şeklinde ayrım da yapılmamıştır. Gerek veri sorumlusu gerekse veri işleyen için de bağlayıcı şirket kuralları düzenlemek olanaklıdır ve bu durum şirketin kararına bırakılmıştır[390].

Regülasyon'a göre bağlayıcı şirket kuralları düzenleyebilecek ilk yapı türü, grup şirketlerdir ve bu kavram belirsiz değildir. Fakat ikinci tür olan 'ortak ekonomik faaliyet/iş birliği içerisindeki teşebbüsler' kavramı içine hangi yapıların gireceği inceleme konusu yapılabilir. Metne bakıldığında, bağlayıcı şirket kuralları düzenleyebilmek için hukuki manada bir grup şirket yapısının gerekmediği görülmektedir. Hatta menfaat ve kâr için ortak ekonomik faaliyet yapan, örneğin ortak girişim, şubeler, bağlı kuruluşlar gibi yapılar da bağlayıcı şirket kuralları düzenleyebilecektir. Ayrıca, maddede yer alan "teşebbüs" terimi de yapının hukuki kişiliğine ilişkin bir mecburiyet bulunmadığını göstermektedir. Teşebbüs kavramının seçilmesinin nedeni bu kavramın, küçük ve orta büyüklükte işletmeleri kapsadığı anlamına gelmesidir.[391].

[389] Toparlak, s.61.
[390] Çekin, 2020, s. 118.
[391] Toparlak, s.61.

E. Bağlayıcı Şirket Kuralları İçinde Verilecek Taahhütler

Bağlayıcı şirket kurallarında, oluşturulduğu dönemden başlayarak kişisel verilerin kim tarafından hangi amaçla işlendiğinin açık olmasını sağlayan [392]şeffaflık ilkesine önem verilmiştir. Regülasyon içinde bağlayıcı şirket kurallarında olması gereken unsurları sayan madde, şeffaflığı temin etmek için 14 fıkra olarak yazılmıştır. Maddenin ayrıntılı şekilde düzenlenmesi, uyumluluk sürecinin AB içinde tutarlı olmasını ve kolay yönetimini sağlamaktadır. Çünkü bağlayıcı şirket kurallarının onay süreçleri yürüten şirketin yerleşik olduğu üye devlete göre, farklı veri koruma kurumları tarafından yürütülmektedir.

Bağlayıcı şirket kuralları, birazdan söz edilecek on dört fıkranın yanı sıra çok uluslu şirketin Regülasyon'dan kaynaklanan bütün yükümlülüklerini kapsamak durumundadır. Örneğin Regülasyon m.47/2-d'de yer alan veri işleme ilkeleri, Regülasyon m. 5'deki genel düzenlemeden ayrılmamalıdır. Yine örneğin m.28 gereğince bağlayıcı şirket kurallarının içinde veri işleyenler de düzenlenmiş ise, m. 28 yükümlülükleri de ifa edilmeli; bu kurallar yanında veri işleme için gereken sözleşmeler yapılmalıdır[393]. Genel yükümlülükler dışında Regülasyon'un bağlayıcı şirket kurallarında bulunmasını belirttiği unsurlar aşağıda gösterilmiştir.

1. Bağlayıcı Şirket Kurallarını Koyan Şirketin Yapısı ve İletişim Bilgileri

Regülasyon m. 47/2/a, AB yasa koyucusunun önem verdiği veri sahiplerine yönelik şeffaflığı sağlamak için getirilmiştir. Bu madde, aynı zamanda Regülasyon'un şirketlere yönelik getirdiği yükümlülüklerin kolayca tatbik edilebilmesini sağlamaktadır. Bu düzenleme ile şirket aleyhine tazminat talebinin bulunması durumunda, sorumlular daha hızlı ve kolay şekilde belirlenmektedir. Bu sebeple bağlayıcı şirket kurallarını hazırlayan grup şirket ya da ekonomik iş birliği içindeki teşebbüsün yapısı sunulmalı ve şirketlerin ne şekilde gruplandığı belirlenmelidir. Bununla birlikte bütün üyelerin irtibat bilgileri ile üçüncü ülkelerde yer alan üyelerden sorumlu AB şirketleri de gösterilmelidir.

---

[392] Bainbridge, s.59; Develioğlu, s.44.
[393] *Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 18/EN WP 257 rev.01 .

2. Veri Aktarımları ve İşlenen Veriler

Direktif'in yürürlükte olduğu dönemde üçüncü ülkelere veri aktarımı, aktarıldığı AB üyesindeki veri koruma makamının onaylamasına bağlı idi. Bu onay süreci, verilerin aktarımının yapıldığı ülkeye ilişkin gerekli bütün bilgilerin elde edildiği kabulüne dayanmaktaydı. Regülasyon yürürlüğe girdikten sonra getirilen bağlayıcı şirket kuralları ile bu veri aktarımı amacıyla bağımsız bir onay sürecine ihtiyaç bulunmamaktadır. Bu sebeple, veri aktarımına ilişkin sürecin bağlayıcı şirket kuralları içinde ayrıntılı şekilde yazılması hükmü getirilmiştir (Regülasyon m. 47/2/b)[394]. Bu kapsamda verilerin işlenme metot ve usulleri, verilerin grupları, veri işleme sürecinin amacı, veri sahiplerinin grubu ve üçüncü ülkede veri aktarımının yapıldığı kişi veya taraflar gibi bilgilerin gösterilmesi gerekmektedir[395].

3. İç ve Dış Bağlayıcılık

Regülasyon'da, iç ve dış bağlayıcılık kavramları açıklanmamış veya tanımı yapılmamıştır. İç ve dış bağlayıcılık kıstasları için AB Veri Kurulu'nun görüşlerinden faydalanılmaktadır. Bu görüşler uyarınca iç bağlayıcılık, bu kuralları hazırlayan ekonomik işbirliği içerisindeki teşebbüsler veya grup şirketin bütün üyelerine ve bunların işçilerine verilecek açık talimatlarla temin edilmektedir. Bu sistemin ne şekilde kurulacağı hususunda şirket serbest bırakılmıştır (Regülasyon m.47/2-c)[396]. İç bağlayıcılık amacıyla oluşturulan yapı bağlayıcı şirket kuralları içinde yer almalıdır.

Dış bağlayıcılığın yapılabilmesi içinse, bütün üçüncü kişilerin hakları ve bunların ne şekilde kullanılacağının net ve öngörülebilir şekilde yazılması gerekir. Bu manada verisi aktarılan veya işlenen ilgili kişiler de üçüncü kişi kabul edilmektedir. AB'de kurulu bir üye şirketin, üçüncü ülkelerde oluşabilecek hukuki ihlallerde hukuki sorumluluğu üstlenmesi, dış bağlayıcılığın getirdiği önemli yükümlülüklerden biridir. Üçüncü ülkelerin sorumluluğunu üstlenen bu üye şirket, bağlayıcı şirket kuralları içinde ifade edilmelidir[397]. Bu bağlamda üçüncü kişiler, bağlayıcı şirket kurallarında yazılan haklarını kullanabilmektedirler.

---

[394] *Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256.
[395] Toparlak, s.54.
[396] *Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 18/EN WP 257 rev.01.
[397] *Working Document,* Md.29 Çalışma Grubu (WP), 11639/02/EN WP 74, 108, 152.

4. Veri İşleme İlkeleri

Regülasyon'da bağlayıcı şirket kuralları içinde taahhüt verilecek veri işleme ilkelerine ilişkin sınırlı bulunmayan bir liste getirilmiştir (Regülasyon m. 47/2/d). Ancak bu veri işleme ilkelerinin vaat edilmesi, tek başına yeterli değildir. Bağlayıcı şirket kuralları içinde, bu ilkelerde, çok uluslu şirket veya ortak girişimde verilerin ne şekilde işlendiği somut biçimde yazılmalı ve örnek verilerek açıklanmalıdır[398].

5. İlgili Kişilerin Hakları

Regülasyon'da ilgili kişilere tanınan tüm haklar, bağlayıcı şirket kuralları içinde de ayrıntılı şekilde taahhüt edilmelidir. Bu manada aşağıda sayılanları kapsayacak fakat sayma yoluyla sınırlı olmayacak biçimde; veri işleme ilkeleri, Regülasyon m.15'de yer alan veri ilgilisi şahsın hakları, m.16 gereğince verilerin düzeltilmesi hakkı, m.17 gereğince unutulma hakkı, m.18'de yer alan biçimiyle veri işlenmesini sınırlama hakkı, m. 21 itiraz ve m.22 gereğince verilerin otomatik karar alma sürecinin kapsamına katılmasına itiraz hakkı ve m.82 gereğince tazminat imkanları taahhüt edilmelidir (Regülasyon m.47/2/e). Bununla birlikte şayet ilgili kişinin bağlı olduğu yerel veri koruma yasalarının Regülasyon'dan üstün koruma sağlaması halinde, bu haklar da bağlayıcı şirket kuralları kapsamına alınmalıdır.

Bağlayıcı şirket kurallarında yer alan hakların kullanımı için usuller de yer almalıdır. Hatta veri koruma makamları bünyesinde şikâyet veya üye devletlerin mahkemelerinde açılacak dava yolları da açıklanmalıdır.

Ayrıca seçim hakkı veri ilgilisi şahısta olacak biçimde, verileri üçüncü ülkelere aktaran AB ülkesindeki mahkemeler ve çok uluslu şirket merkezinin bulunduğu AB ülkesindeki mahkemeler yetkili olacaktır[399]. İlave olarak Regülasyon m.79/2 gereğince ilgili kişinin yerleşik olduğu yerdeki bir mahkemede de dava açılabilmektedir.

6. AB'deki Kuruluşların Sorumluluğu

Bağlayıcı şirket kurallarında verilerin aktarımının yapıldığı üçüncü ülkedeki olası ihlaller için, AB'deki sorumlu üye şirket açık şekilde ifade edilmelidir. Bu

[398] Toparlak, s.55.
[399] *Working Document,* Md.29 Çalışma Grubu (WP), 17/EN WP 256.

yükümlülük, şeffaflık ilkesinin gerçekleşmesine yardımcı olmaktadır. Bağlayıcı şirket kurallarında çok uluslu şirketin üçüncü ülkelerde bulunan üyeleri açısından da ortak sorumluluk getirilmelidir[400]. Bu durum yasal bir yükümlülük olmadığından, bağlayıcı şirket kuralları içerisinde bağlayıcılığı mutlak surette belirtilmelidir. AB'deki müşterek sorumlu üye şirket, hukuka aykırılığın kendisi ile hiçbir ilgisinin bulunmadığını kanıtlarsa sorumluluktan kurtulabilmektedir (Regülasyon m.47/2/f).

Çalışma Grubu dokümanlarında kullanılan bu ifadenin kurtuluş beyyinesi[401] olduğu söylenebilir. Bağlayıcı şirket kurallarında, üçüncü ülkedeki üye şirketler açısından getirilmiş yükümlülükler, gösterilmesi gereken özeni belirtmektedir. Üçüncü ülkedeki üye şirketin bağlı olduğu ulusal hukuk incelemesi gerçekleştirilmeli ve bağlayıcı şirket kuralları yükümlülüklerini ihlal eden durumlar tespit edilmelidir. Gereken durumlarda AB'deki yetkili veri koruma makamından görüş alınmalıdır. Bağlayıcı şirket kurallarında yer alan teknik ve idari önlemler, üçüncü ülkedeki üye şirket açısından da bağlayıcı biçimde uygulanmalıdır. Gereken denetim ve raporlama faaliyetleri gerçekleştirilmelidir. Bu nedenle AB'deki müşterek sorumlu şirketin gereken özeni gösterdiğini kanıtlaması durumunda kendisine kurtuluş olanağı verilmesi, bağlayıcı şirket kurallarının amaçları ve getiriliş mantığı ile uyumludur. Elbette ispat külfeti AB'deki üye şirkete aittir. Bağlayıcı şirket kuralları taahhütlerine uygun davranılmaması, özen yükümlülüğüne de aykırı olacaktır[402].

Üçüncü ülkedeki üye şirketin yapabileceği hukuka aykırılıklar açısından AB'deki hangi üye şirketin müşterek sorumlu olacağı Regülasyon m.47'de yer almamaktadır. Grup şirketler, bağlayıcı şirket kuralları yayınlarken kendi yapıları gereğince, AB'deki bir üye şirketi müşterek sorumlu olarak belirleyebilmektedir. Bu durumda genellikle, üçüncü ülkelere verilerin aktarımının yapıldığı şirket ya da AB'deki ana merkez seçilmektedir[403].

7. İlgili Kişilere İletilecek Bilgiler

Veri ilgilisi şahıslara iletilmesi gerekli bilgiler, Regülasyon m.13 ve m. 14'de yer almıştır. Bağlayıcı şirket kuralları içinde bu bilgilerin hangi usulle veya ne şekilde

[400]Moerel, s.219.
[401]Oğuzman/Öz, s. 148 vd; Çekin, 2016, s.638.
[402]*Working Document,* Md. 29 Çalışma Grubu (WP), 18/EN WP 257 rev.01.
[403]Toparlak, s.56.

verileceği hususu da belirtilmelidir (Regülasyon m.47/2/g).Bahse konu yükümlülük, internet ya da özel ağ üzerinden yapılacak bilgilendirmeyle ifa edilebilmektedir. Bu kapsamda ilgili kişilere, bütün haklarını kolay şekilde kullanabilmeleri amacıyla gerekli tüm bilgiler net ve anlaşılır biçimde iletilmelidir[404].

8. Çalışanların Görevleri ve Uyumluluk (Compliance)

Bağlayıcı şirket kuralları gereğince grup şirkette bir veri koruma görevlisi saptanmalıdır. Bununla birlikte uyumluluk (compliance) sağlanması amacıyla şirket içinde ayrı bir bölümün oluşturulması gerekmektedir. Grup şirket içerindeki tüm çalışanlar uyumluluk sürecine ilişkin bilgilendirilmelidir (Regülasyon m.47/2/h)[405]. Oluşturulacak bölümün yapısı, görev ve yetkileri bağlayıcı şirket kuralları içinde yer almalıdır. Bununla birlikte grup şirket üyesi her bir şirket veya teşebbüsün görevleri tespit edilmeli ve bir kontrol zinciri oluşturulmalıdır[406]. Bu nedenle uyumluluk için grup şirketin tüm bölümlerinin raporlama faaliyeti gerçekleştireceği üst bölüm belirli olmalı ve bu bölümün talimatlarına uyulmalıdır.

9. İtiraz ve Şikâyet Süreci

Regülasyon m.47/2-i gereğince bağlayıcı şirket kurallarında iç şikâyet aşamaları tanımlanmalıdır. Veri ilgilisi kişiler, şikâyetlerini çok uluslu şirket içinde iletecekleri birimi bilebilmelidirler. Örnek olarak ilgili kişiler, şikâyet ve itiraz haklarını kendilerine gönderilen formları doldurarak iletebilirler. İletilen formda şikâyetin anlaşılabilmesi için talep edilen bilgilerin verilmesi önemlidir. Ayrıca şikâyetlerin gönderilmesi için şirketin internet sitesinde özel bir bölüme yer verilebilir. Bağlayıcı şirket kurallarında bu süreç açık şekilde yazılmalı ve iç şikâyetin iletilmesi için oluşturulan yöntem belirtilmelidir. Grup şirkete iletilen iç şikâyet, bir ila üç ay içinde araştırılarak cevaplanmalıdır[407].

---

[404]Toparlak, s.57.
[405]Cunningham, McKay, Complying with International Data Protection Law, University of Cincinnati Law Review, S.84 (2), 2018, s.439.
[406]*Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 18/EN WP 257 rev.01.
[407]*Working Document,* Md. 29 Çalışma Grubu (WP), 268, 257, 74, 108.

10. Uyumluluğun (Compliance) Devamı Amacıyla Kontrol Süreçleri

Bağlayıcı şirket kurallarının amacı, veri korumasını ve veri gizliliğini şirket kültürüne katmaktır. Bu kapsamda sürekli bir uyumluluk süreci oluşturulması amaçlanmaktadır. Bu nedenle bağlayıcı şirket kurallarının onaylanmasından sonra da uyumluluk sürdürülmeli ve denetimi sağlanmalıdır (Regülasyon m.47/2-j). Şirket bünyesinde oluşturulan uyumluluk bölümü, belirli aralıklarla testler yapmalıdır. Veri koruma yükümlülüklerine ve bağlayıcı şirket kurallarına uyumun kontrol edildiği bu denetimler, veri koruma görevlisi ve şirketin yönetim kuruluna sunulmalıdır. Gerçekleştirilen kontrollerin neticesi, istem üzerine veri koruma makamına gönderilmelidir. Bahse konusu test ve kontroller, akredite denetim kuruluşları gibi iç veya dış denetim kuruluşları vasıtasıyla gerçekleştirilebilmektedir[408]. Bağlayıcı şirket kuralları içinde şirket üyelerinin bu kontrolleri yaptıracağı süreler ve neticelerin paylaşılacağı kişiler yazılmalıdır. Ayrıca bu denetimler, bir ihlal durumunda ispat vasıtası da olabilecektir[409].

11. Bağlayıcı Şirket Kurallarının Güncellenmesi ve Yetkili Veri Koruma Makamına Bildirilmesi

Grup şirkette, bunun yapısı ve veri işleme aşamaları devamlı surette gelişmektedir. Bu sebeple hazırlanan bağlayıcı şirket kurallarını, durağan kurallar şeklinde görmemek gerekir. Tüm yeni değişikliklerde yeni bir bağlayıcı şirket kurallarının düzenlenip onaylanması gerekmez (Regülasyon m.47/2-k). Fakat değişiklik, mevcut bağlayıcı şirket kurallarına esastan etki ediyorsa, bağlayıcı şirket kurallarının baştan düzenlenip onaylanması söz konusu olabilecektir. Değişikliğin bağlayıcı şirket kurallarını esastan etkileyip etkilemediği belirlenemiyorsa, veri koruma makamına başvurulmalı ve yeni bir onay sürecinin gerekip gerekmediğine ilişkin görüşüne başvurulmalıdır.

Veri işleme sürecindeki değişikliklere ilişkin m. 29 Çalışma Grubu aşağıdaki esasları ifade etmiştir[410];

[408] *Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 18/EN WP 257 rev.01.
[409] Toparlak, s.58.
[410] *Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 18/EN WP 257 rev.01, 204 rev01.

• Grup şirket içinde, veri işleme süreçlerindeki değişiklikler izlenmeli ve ele alınmalı ve bağlayıcı şirket kurallarında değişiklik yapılıp yapılmaması gerektiği tespit edilmelidir. Bu hedef ile yetkili veri koruma makamları ile işbirliği gerçekleştirecek bir kişi veya statü oluşturulmalıdır.

• Grup şirkete yeni bir kuruluşun katılması durumunda, kuruluşta düzenlenen bağlayıcı şirket kurallarını taahhüt etmeli ve uyumluluk temin edilmelidir.

• Yıllık periyotta değişiklikler, yetkili veri koruma makamına bildirilmeli, şayet değişikliklerden biri temelden değişiklik şeklinde değerlendirilirse takip edilecek usul, yetkili veri koruma makamı ile birlikte belirlenmelidir.

• Bağlayıcı şirket kurallarında gerçekleştirilen tüm değişiklikler, bu şirket ile sözleşmeye istinaden veri işleyenlere bildirilmeli ve uyumluluk temin edilmelidir.

12. Veri Koruma Makamıyla İşbirliği

Bağlayıcı şirket kurallarını hazırlayan grup şirket, yetkili veri koruma makamı ile işbirliği yapmakla yükümlüdür (Regülasyon m.47/2-l). Bu işbirliği süreci, bağlayıcı şirket kurallarında tanımlanmış olmalıdır. Bu yükümlülüğün icra edilmesi için Regülasyon m. 47/2/f gereğince yapılan uyumluluk denetimlerinin neticeleri, Regülasyon m. 47/2/k gereğince gerçekleştirilecek güncellemeler veya Regülasyon m. 47/2/m gereğince verilen ulusal vaatler de, veri koruma makamlarıyla paylaşılmalıdır[411].

13. Üçüncü Ülkelerdeki Bağlayıcı Şirket Kurallarına Aykırı Kanuni Yükümlülüklere İlişkin Bildirim

Grup şirketin üçüncü ülkedeki üyeleri, bağlayıcı şirket kurallarında verilen taahhütlere bakmalı ve bağlı oldukları ulusal mevzuatla karşılaştırma yapmalıdırlar. Üçüncü ülkedeki veri koruma yasalarına ilişkin bu karşılaştırma, bu şirketin uyumluluk departmanı ve veri koruma görevlisiyle paylaşılmalıdır (Regülasyon m.47/2-m). Ulusal kanunlarla çatıştığı için uygulanamayacak bağlayıcı şirket kuralları yükümlülükleri varsa, bu durum AB'deki müşterek sorumlu üyeye ya da genel

[411]Toparlak, s.58.

merkezin uyumluluk birimine bildirilmelidir. Bağlayıcı şirket kuralları ile çelişen ulusal mevzuat düzenlemeleri, yetkili veri koruma makamı ile de paylaşılmalıdır.

Ulusal düzenlemeler ile bağlayıcı şirket kurallarının çeliştiği durumda, Regülasyon m. 23 gereğince bir karşılaştırma yapılmalıdır. Belirtmek gerekir ki, *Safe Harbor* kararı[412] bu karşılaştırma açısından önemlidir. Bu kararda, AB hukuku ile üçüncü ülkelerin düzenlemelerinin çeliştiği durumlarda uygulanacak ilkeler detaylı şekilde belirlenmiştir. Bu ilkeler, bağlayıcı şirket kuralları ile üçüncü ülke yasalarının çeliştiği yerlerde de uygulanabilir özelliktedir.

Son olarak, bağlayıcı şirket kurallarını kabul eden grup şirket içindeki tüm şirketler, çalışanlarına belirli aralıklarla eğitim vermekle yükümlüdürler. Eğitimlerin özelliği bağlayıcı şirket kurallarında yer almalıdır ve hatta bu eğitim programları için örneklerin bile gösterilmesi öngörülmüştür[413].

F.Onay Süreci

Bağlayıcı şirket kuralları, değişik ülkelerdeki farklı ulusal mevzuata bağlı şirketler açısından bağlayıcı şekilde hazırlanmaktadır. Bu sebeple veri koruma makamlarının iş birliği ve karşılıklı taahhütlerinin olması gerekmektedir. Regülasyon m. 47'ye uygun şekilde hazırlanmış bağlayıcı şirket kuralları, m. 63'de yer alan AB'nin bütünü için getirilmiş tutarlılık mekanizmalarına da bağlıdır. Regülasyon, üye devletlerde tutarlı bir biçimde kuralların tatbik edilmesini temin etmek amacıyla bir tutarlılık sistemi oluşturmuş olup, bu şekilde denetim makamları birbirleriyle ve gerekmesi halinde Komisyonla koordinasyon yapmaktadır. Tutarlılık sistemi, öncelikle Avrupa Veri Koruma Kurulu'nun görüşleri ile ilgilidir. İkinci olarak; tek makama bağlı olunduğu hallerde yetkilileri kontrol etmek ve denetim makamının Avrupa Veri Koruma Kurulu'ndan görüş istemediği ya da bu görüşün takip edilmediği hallerde Avrupa Veri Koruma Kurulu'nun bağlayıcı kararlarıyla ilgilidir.

Grup şirket merkezinin olduğu AB ülkesindeki yetkili veri koruma makamı, bağlayıcı şirket kuralları hazırlanırken bu tutarlılık mekanizmalarını gözlemektedir. Hatta bu veri koruma makamı, m.56 gereğince bağlayıcı şirket kurallarına "baş yetkili makam" sıfatıyla onay vermektedir. Fakat, bu şirketin AB ülkelerinde yerleşik başka

[412]C-362/14 (Maximilian Schrems v Data Protection Commissioner)
[413]*Working Document,* Md. 29 Çalışma Grubu (WP), 17/EN WP 256, 153.

üyelerinin bulunduğu yerdeki veri koruma makamları da onay sürecine dahil olmaktadırlar. Grup şirketin AB'de sadece bir adet kuruluşu bulunması durumunda bu tutarlılık sürecine gerek bulunmamaktadır. Ayrıca Regülasyon m. 57/1 ve m.58/3/j'de yer aldığı gibi veri koruma makamlarının kendi yetki alanında hazırlanan bağlayıcı şirket kurallarını onaylama yetkisi vardır[414].

G.AB İçindeki Ana Şirketin Sorumluluk Halleri

Regülasyon'un sekizinci bölümünde hukuki çözümler, sorumluluk ve cezalar yer almıştır. Bu bölüm m.82'de maddi ve manevi tazminat ile m.84'de ceza sorumluluğu halleri ile yer almaktadır. Bunlar yanında asıl etkili olan AB içinde yeknesak şekilde uygulanan idari para cezalarıdır. Bu idari para cezaları getirilirken amaçlardan biri, Google, Facebook gibi büyük çapta veri işleyenlerin faaliyetlerinde AB içinde tutarlı bir uygulamanın yerleştirilmesidir.

Regülasyon m.83'de getirilen bir yenilik, yüksek miktardaki idari para cezalarıdır[415]. Regülasyon m.8, 11, m. 25-39, m. 42 ve m. 43'de yer alan yükümlülükleri veri sorumlusu ve veri işleyenin ihlal etmesi durumunda, yetkili veri koruma makamınca 10.000.000 Avroya kadar, eğer bir ticari işletme varsa bu işletmenin global cirosunun 2 %'sine kadar hükmedilebilecek idari para cezası hükümleri getirilmiştir. Yine Regülasyon'un veri işleme ilkeleri, hukuka uygunluk sebepleri ve veri ilgilisinden alınacak rızaya ilişkin getirilen yükümlülüklerin ve özel nitelikli kişisel verilere ilişkin hükümlerin bulunduğu m. 5, m. 6, m. 7 ve m. 9'un ve veri ilgisi kişilerin haklarının yer aldığı Regülasyon m. 12 ila 22. hükmüne aykırılık halinde ise, yine veri koruma makamı tarafından belirlenmek üzere 20.000.000 Avroya kadar, eğer bir ticari işletme varsa küresel cironun 4 %'üne kadar idari para cezası verileceği hükmü getirilmiştir. Kaldı ki veri sorumlusu, ilgili kişiden alınan rızanın Regülasyon'a uygun biçimde alındığını da kanıtlamakla yükümlüdür.

Regülasyon m. 44 ila m. 49 uyarınca, bağlayıcı şirket kuralları dahil olmak üzere fakat bununla kısıtlı olmayacak biçimde, üçüncü ülkelere veri aktarımı amacıyla

[414]Toparlak, s.62.
[415]Art. 83, GDPR, bkz. https://gdpr-info.eu/art-83-gdpr/, E.T.:17.7.2021.

getirilen sorumlulukların ihlali halinde de 20.000.000 Avroya kadar, bir ticari işletme varsa global cironun 4 %'üne kadar idari para cezasına hükmedilebilmektedir[416].

Bu hükümlerden anlaşılacağı üzere bağlayıcı şirket kurallarını taahhüt eden Türkiye'deki şirket, onaylanmış bu kurallara uygun hareket etmelidir. Bilhassa veri işleme ilkeleri, hukuka uygunluk sebepleri ve ilgili kişilerden alınacak rızalara Regülasyon'un öngördüğü ve bağlayıcı şirket kurallarında yazıldığı şekilde uymalıdır. Ayrıca Türkiye'deki şirket bağlayıcı şirket kuralları kapsamında kendisine aktarımı yapılan verileri, üçüncü bir kişiye aktarırken de Regülasyon'da yer alan veri aktarımı yükümlülükleri ile bağlıdır. Bu yükümlülüklerin yerine getirilmemesi durumunda AB'deki merkez yapı hakkında, bağlayıcı şirket kurallarını taahhüt eden grup şirketin cirosunun 4 %'üne kadar idari para cezası verilebilir.

Veri koruma makamları Regülasyon m.83'de hüküm altına alınan idari para cezalarının miktarını belirlerken bazı noktaları göz önüne alırlar. Öncelikle veri sorumlusu ya da işleyen tarafından veri ilgisi kişilerin zararını gidermek veya azaltmak amacıyla yapılanlar dikkate alınmaktadır. Ayrıca Regülasyon m. 25 ve 32. gereğince getirilen teknik ve idari önlemler de değerlendirilmektedir. Zararı düşürmek için veri koruma makamları iş birliği ölçüsü yapıldığını da göz önüne almaktadır. Bir diğer kıstas olarak ise Regülasyon m. 58/2 gereğince veri koruma makamlarının önceden yaptıkları ikazlara uygun hareket edilip edilmediği incelenmektedir[417].

Veri koruma makamınca onaylanmış olan bağlayıcı şirket kurallarının bulunması, bu değerlendirmelerin yapılması bakımından önemlidir. Çünkü bağlayıcı şirket kuralları teknik ve idari önlemlerin alındığını göstermekte ve zarar tehlikesini azaltmaktadır. Bununla birlikte, veri koruma makamlarıyla koordinasyonu da güçlendirmekte ve bu şirketlerin güvenilirliğinin artmasına yol açmaktadır. Bu nedenle bağlayıcı şirket kuralları, idari para cezaları bakımından önem taşımaktadır.

Şirkete idari para cezası uygulanmasını önleyebilecek olan bağlayıcı şirket kurallarına uyulmaması, özen borcuna aykırılık oluşturabilecektir.

[416]Houser, Kimberly, Voss, Gregory, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? Richmond Journal of Law & Technology, 2018, s.63; Toparlak, s.62.
[417]Toparlak, s.64.

H. Denetim Mekanizmaları

Direktif'te kişisel verilerinin işlenmesinde korunmanın zorunlu bir unsuru, üye devletler açısından, kişisel verilerin korunmasına dair kuralların uygulanmasını denetlemek için bağımsız bir denetim biriminin görevlendirilmesiydi. Bağımsız denetim kurumlarına dair detaylı hükümlerin Direktif'te bulunduğu görülmektedir[418]. Regülasyon ise, aynı anlayışla, çok daha geniş kapsamlı düzenlemeler getirmektedir[419]. Denetim kurumlarının kuruluşu, görevleri, yetkileri, üyelerinin atanması, işbirliği ve istikrar mekanizmalarının yanında, tüzel kişiliğe sahip olan bir AB organı olan Avrupa Veri Koruma Kurulu'nun kuruluşu ve işleyişine dair esaslar Regülasyon m.51ila m.76 arasında detaylı şekilde düzenlenmiştir.

Regülasyon m.51. gereği, her üye devlet, gerçek şahısların hak ve hürriyetlerinin korunması ile AB içinde veri akışının kolay hale getirilmesi için, Regülasyon'un uygulanmasını denetlemek üzere bir ya da birden çok bağımsız denetim kurumu tayin etmek zorundadır. AB'de Regülasyon'un istikrarlı bir biçimde uygulanmasını temin etmek üzere, denetim kurumlarının birbirleriyle ve Komisyon ile işbirliği yapmaları da düzenlenmiştir.

1.Avrupa Komisyonu ve Avrupa Veri Koruma Kurulu

Avrupa Veri Koruma Kurulu, Regülasyon m.68 kapsamında kurulan, görevleri ve işleyişine dair esasları Regülasyon ile tespit edilen, bağımsız ve tüzel kişiliğe sahip bir AB organıdır. Söz konusu madde gereğince Kurul Başkanı, Kurul'u temsil eder ve Kurul üye devletlerin veri koruma kurumlarının başkanları ile Avrupa Veri Koruma Denetçisi ya da bunların temsilcilerinden oluşur. Komisyon, Kurul'un toplantı ve faaliyetlerine katılabilir, fakat oy kullanma hakkı yoktur. Kurul, görevlerini ve yetkilerini icra ederken bağımsız şekilde faaliyette bulunur, hiçbir organdan talimat almaz ve isteyemez (Regülasyon m.69). Regülasyon'un yürürlüğe girmesi ile Madde 29 Çalışma Grubu'nun faaliyeti sona ermiş ve Kurul, bu Çalışma Grubu'nun yerini almıştır[420].

[418] Küzeci, 2019, s.272.
[419] Regülasyon, Gerekçe 117.
[420] Küzeci, 2019, s.161.

Kurul'un en esaslı görevi, Regülasyonun etkili ve istikrarlı bir biçimde uygulanmasını temin etmektir. Bu kapsamda Regülasyon m.70/1'de Kurul re'sen veya Komisyon istemi doğrultusunda bilhassa icra etmesi gereken görevleri ayrıntılı şekilde saymıştır. Bu maddeye göre, bu görevler sınırlı sayıda değildir ve tüm görevlerinin Regülasyon'un istikrarlı ve uyumlu bir biçimde uygulanması amacını taşıdığı görülmektedir.

Kurul'un ilk görevi, istikrar mekanizması kapsamında Regülasyon'un doğru biçimde uygulanmasını sağlamak ve denetlemek (Regülasyon m.70/1-a) ile Regülasyon'da değişiklik teklifleri dahil olarak, Komisyon'a kişisel verilerin korunmasına dair tavsiyelerde bulunmaktır (Regülasyon m70/1-b). Ayrıca Kurul, Komisyon'a; veri sorumluları, veri işleyenler ve veri koruma kurumları arasındaki veri aktarımlarına dair bağlayıcı şirket kurallarının şekli ve usullerine dair tavsiyelerde bulunmakta (Regülasyon m.70/1-c), unutulma hakkı çerçevesinde kamuya duyurulan verilerin bağlantılarının ve kopyalarının silinmesi için en iyi uygulamalar ve usullerin neler olduğuna dair rehber ve tavsiyeler yayımlamaktır (Regülasyon m.70/1-d). Kurul'un faaliyetleri; re'sen ya da istem üzerine Regülasyon'un istikrarlı bir biçimde tatbik edilmesine yönelik olarak Regülasyon'un farklı hükümlerinin uygulamaya geçirilmesine dair yöntemler ve usullere dair rehberler ve tavsiyeler yayımlamak (Regülasyon m.70/1-e - m); davranış kuralları, sertifikasyon, veri koruma mührü gibi uygulamaların benimsenmesini desteklemek ve bunlara dair Komisyon'a görüş bildirmek (Regülasyon m.70/1-n - q), istikrar mekanizması kapsamında denetim kurumlarının taslak kararlarına dair görüş bildirmek ve acil durum prosedürü çerçevesindeki durumlar da dahil olmak üzere, uyuşmazlık çözüm makamı sıfatıyla bağlayıcı kararlar vermek (Regülasyon m.70/1-t)[421], denetim kurumları arasında işbirliğini ve ikili veya çok taraflı bilgi paylaşımını desteklemek (Regülasyon m. 70/1-u), denetim kurumları arasında ortak eğitim programları yapılmasını desteklemek ve personel değişimini kolay hale getirmek (Regülasyon m.70/1-v); küresel çaptaki denetim kurumları ile verilerin korunması düzenlemeleri ve uygulamalarına dair bilgi alışverişi yapmayı desteklemek (Regülasyon m.70/1-w), veri sorumluları veya veri işleyenlerin düzenledikleri davranış kurallarına ilişkin görüş vermek (Regülasyon m.70/1-x), istikrar mekanizması çerçevesinde oluşan sorunlarda, denetim kurumları

[421]Yörük, s.124-125.

veya mahkemelerin verdiği kararları kamunun erişimine açık, elektronik bir kayıt şeklinde tutmaktır (Regülasyon m.70/1-y).

Komisyon'un tavsiye talep ettiği bazı durumlarda, olayın acil olması halinde bir süre sınırı verilebilir (Regülasyon m70/2). Kurul; görüş, rehber ve tavsiyelerini Komisyon'a ve Regülasyon gereğince Komisyon'a yardım eden komiteye bildirir ve bunları kamusal erişime açar (Regülasyon m.70/3). Bununla birlikte Kurul, görevlerini icra ederken olanaklı durumlarda ilgili taraflara da danışmalı ve uygun bir süre içinde görüş vermelerine olanak tanımalıdır (Regülasyon m. 70/4). Son olarak Kurul, rehberleri ve tavsiyelerinin tatbik edilmesine dair denetim neticelerinin yanında istikrar mekanizması kapsamında, gerçek kişilerin kişisel verilerinin işlenmesi karşısında korunmasına dair bir rapor hazırlayarak, bunu Komisyon'un yanında Avrupa Parlamentosu ile AB Konseyi'ne iletir (Regülasyon m. 71)[422].

[422]Yörük, s.125.

SONUÇ

Uluslararası ticaretin gelişmesiyle kişisel verilerin uluslararası aktarımlarının yapıldığı alanlar da çoğalmış ve bunun sonucunda AB'de kişisel verilerin korunması amacıyla ilk olarak 95/46 sayılı Direktif uygulanmış, daha sonra bu Direktif kaldırılarak AB'de 2016 yılında Regülasyon yürürlüğe girmiştir. Bu Regülasyon, kişisel verilere ilişkin olarak şirketlere hesap verme yükümlülüğünü getirmiş ve bu yükümlülük kişisel veriler ile kişilerin mahremiyetinin korunmasını sağlayan önemli ilkeler arasında yer almıştır. Hesap verebilirlik, yürürlükteki veri koruma mevzuatının kanun ve kurallarının şirket tarafından uygulanması ve bu uygulamanın ispatlanabilir olmasıdır. Bu çerçevede hesap verebilirliği temin etmek için Regülasyon'da idari ve teknik tedbirler, risk analizleri gibi yükümlülükler de yer almıştır. Bağlayıcı şirket kuralları, şirketlerin alması gereken bu teknik ve idari tedbirleri açık şekilde düzenlemiş, taahhüt etmiş ve bu kapsamda şirketlerin hesap verebilirliğini de arttırmıştır.

Bağlayıcı şirket kurallarının amacı, bu kuralları düzenleyip taahhüt eden küresel grup şirket içinde serbestçe veri aktarımının yapılmasıdır. Bu nedenle bağlayıcı şirket kuralları, üçüncü ülkelere veri aktarımı amacıyla Regülasyon içinde getirilen uygun güvenlik tedbirleri altında yer almıştır. Ayrıca bağlayıcı şirket kuralları, veri koruması hukuku açısından uyumun esasını meydana getirebilecek yükümlülüklerin icra edilmesini ve kanıtlanmasını sağlayabilecektir.

AB hukukunda grup şirketler ya da ekonomik iş birliği şeklinde örgütlenmiş teşebbüsler bağlayıcı şirket kuralları düzenleyebilir. Bu kurallara ilişkin metinler, grup şirketlerin kendi gereksinimleri doğrultusunda düzenlenmekte ve Regülasyon'un getirdiği yükümlülükleri taahhüt etmektedir. Bağlayıcı şirket kurallarının geçerlilik kazanabilmesi için, grup şirketlerde ya da ekonomik işbirliği içindeki teşebbüste yer alan üyelerinin tümünün bu kuralları taahhüt etmeleri gerekmektedir. Veri koruma makamı tarafından da uygun görülen bağlayıcı şirket kuralları, çok uluslu şirket içindeki veri aktarımları bakımından uygun güvenlik tedbiri özelliğine sahip olmaktadır. Diğer bir deyişle, grup şirketin üçüncü ülkelerdeki üyelerine veya üye şirketine, başka bir tedbir alınmasına gerek kalmaksızın veri aktarımı mümkün olabilmektedir. Fakat verilerin bu aktarılan üçüncü ülkeden ileri aktarımları için başka

türlü güvenlik tedbirlerinin alınmasına ihtiyaç duyulacaktır. Bağlayıcı şirket kuralları, sadece AB hukukuna uyum sağlandığını göstermekte ve Regülasyon gereğince uygun güvenlik tedbiri oluşturmaktadır. Bu nedenle üçüncü ülkedeki üye şirketten AB'deki üyelere yönelik veri aktarımında, üçüncü ülkedeki iç hukukta yer alan veri aktarım ilke ve kurallarına uygun hareket edilmesi gerekmektedir. Regülasyon'da ayrıntılı şekilde düzenlenen hükümler ve AB'deki uygulamalar, uluslararası standartların hazırlanması açısından da önemli bir yol gösterici olacaktır.

Kişisel verilerin işlenmesi faaliyetleri, ülkemizin ve hatta kıtaların sınırlarını aşmaktadır. Bu kapsamda grup şirket tarafından sunulacak benzeri bir taahhüdün, Türk veri koruma hukukuna temin edebileceği faydaların da bulunduğu görülmüş ve Kurum, 10.04.2020 tarihli duyurusunda Türkiye'de kurulu veri sorumluları tarafından bağlayıcı şirket kurallarının hazırlanabileceğini belirtmiştir. İlk olarak Regülasyon'da düzenlenmiş olan bağlayıcı şirket kuralları, KVKK gereğince Kurumca meydana getirilen seçenek uygun güvenlik tedbiri anlamına gelmektedir.

Türk hukukunda kişisel verilerin yurt dışına aktarılması kriterleri KVKK'da yer almıştır. Açık rıza, belirli bir konuya dair, bilgilendirmeye dayanan ve şahsın özgür iradesi ile açıklandığı rızadır. KVKK m.3'de ilgili kişinin aydınlatmaya dayanan (m.10), belli bir konuda ve özgür iradeyle açıkladığı açık rızası ile yurt dışına veri aktarılması mümkündür.

Açık rıza, sözlü veya yazılı olarak verilebilir. İlgili kişi, KVKK m.5/2-d'de düzenlenen istisnalar dışında açık rıza beyanını istediğinde geri alabilecektir. Yine KVKK m.9 uyarınca yeterli korumanın olduğu ülkelere veri aktarımında, aktarımı yapılacak verinin özel nitelikli veri olup olmamasına göre, KVKK'nın m.5/2 veya m.6/3'da düzenlenen işleme şartlarının bulunması gerekmektedir. Bununla birlikte, yeterli veri koruması olmayan ülkelere veri aktarımı durumunda, KVKK m.9/2-b ve 12/2 uyarınca Türkiye'de kurulu veri sorumlusunca bu ülkelere veri aktarımı için düzenlenecek sözleşmelerde mutlaka veri aktaran veri sorumlusunun yükümlülükleri, veri alıcısı ya da işleyenin yükümlülükleri ve ortak hükümlerin yer alması zorunludur. Bu hükümler çerçevesinde veri aktarımı, veri sorumlularından veri sorumlularına veya veri sorumlularından veri işleyenlere yapılmaktadır. KVKK'da açık şekilde düzenlenmese de yabancı ülkelere veri aktarımında kullanılabilecek diğer bir düzenleme, bağlayıcı şirket kurallarıdır.

Türk hukukunda bağlayıcı şirket kuralları, KVKK dahil, yasal bir düzenlemede yer almamış ve Kurum'un 10.04.2020 tarihli "bağlayıcı şirket kuralları"na dair duyurusu ile Türk hukukuna girmiştir. Bağlayıcı şirket kurallarına ilişkin anılan duyuru Regülasyon kapsamında hazırlanmıştır. Kurul duyurusuna göre bağlayıcı şirket kurallarında bulunması gereken hususlar; bağlayıcılık unsurunun sağlanması, bu kuralların etkili uygulanmasının sağlanması, kişisel verilerin işlenmesi ve aktarılması sürecinin açıklanması, Kurum ile koordinasyonun sağlanması, raporlama ve kayıt değişikliği mekanizmalarının belirlenmesi ve veri güvenliğinin sağlanmasıdır. Ayrıca, yapılacak tüm kişisel veri aktarımlarını kapsayacak biçimde veri koruma ilkelerine dair bir açıklama ile teknik ve idari önlemler de alınmalıdır. Ayrıca KVKK m.12 ve m.15/3 çerçevesinde şirketlerin veri işleme ve aktarmada hesap verebilirliği ve şeffaflığı da sağlanmalıdır. Bağlayıcı şirket kuralları çerçevesinde veri sorumluları ve veri işleyenlerin tazminat, idari ve cezai sorumluluğu bulunmaktadır. Örneğin kişisel verilerinin hukuka aykırı şekilde işlenmesi nedeniyle zarar gören veri ilgilisi şahsın, KVKK m.11/1/ğ gereğince veri sorumlusuna başvuru yaparak zararın tazminini isteme hakkı bulunmaktadır. Bir kişilik hakkı olan kişisel verilerin hukuka aykırı işlenmesi hallerinde KVKK'nın atfıyla TMK m.24 ve devamı maddeleri ile haksız filin gerçekleşmesi durumunda ise TBK m.49 ve devamı maddelerinin uygulanması gerekecektir. Elbette sorumluluk için, haksız fiil, nedensellik bağı ve zararın oluşması şartlarının bulunması gerekmektedir. Bağlayıcı şirket kurallarının ihlalinde ispat yükü ve KVKK m.11 kapsamında veri sahibinin hakları da çalışmada ele alınmıştır.

Bağlayıcı şirket kuralları getiren şirketlerin teorik olarak, AB ilke ve kurallarına uygun bir yapı kurması gerektiği görülmektedir. Türk mevzuatında Kurul'un diğer üye şirketler nezdindeki denetim ve kontrol yetkisi dahil bir çok husus henüz belirsizdir. *Schrems I* ve *II* kararları da gözetilerek üçüncü ülkedeki veri koruma makamının denetim yetkisine ilişkin belirlenen ilkelere uyum sağlanmalıdır.

Kurum, bağlayıcı şirket kuralları hazırlayabilecek grup şirketlerini, merkezi Türkiye'de olan şirketlerle sınırlamamıştır. Kurum'un duyurusuna göre, merkezi yabancı ülkede bulunan bir grup şirketin, Türkiye'deki üyesinin yetkili kılınması durumunda bu kuralları hazırlaması ve uygulaması olanaklıdır. Bu sayede bağlayıcı şirket kuralları düzenlemiş bulunan, merkezi yabancı ülkede bulunan grup şirketler için bahse konu taahhütlerin, incelenerek ve gerekirse ilaveler yapılarak, Kurum

tarafından kabul gören bağlayıcı şirket kuralları şeklinde taahhüt edilmesi mümkündür. Bu şekilde grup şirket içindeki veri aktarımları Regülasyon ve KVKK çerçevesinde hukuka uygun olacaktır. Bu durum, bağlayıcı şirket kurallarının uluslararası veri koruması alanındaki önemini de ortaya koymaktadır. Öte yandan Türkiye'de şube ya da irtibat bürosu olan grup şirket veya teşebbüslerin sorumluluğu, TTK m.40/4'de düzenlenmiştir. Bu maddeye göre, şubelerin tek başlarına gerçek veya özel hukuk tüzel kişiliği olmasa da veri işleme faaliyeti yapan ve ticari gelir temin eden şubelerin veri sorumlusu şeklinde kabul edilmesi, yasanın amacı ile uyumlu olacaktır.

Birden fazla yerde şirkete sahip bir AB şirketinin bağlayıcı şirket kurallarını taahhüt eden Türkiye'deki şirketi, bu kurallara uygun davranmalıdır. AB hukukunda veri işleme koşulları, hukuka uygunluk sebepleri ve ilgili şahıslardan alınacak rızalar, Regülasyon'a ve bağlayıcı şirket kurallarına uymalıdır. Bununla birlikte bu şirketin Türkiye'deki yerleşik şirketi, bağlayıcı şirket kuralları kapsamında kendisine aktarımı yapılan verileri, üçüncü bir kişiye aktarırken de Regülasyon'da yer alan veri aktarımı yükümlülükleri ile bağlıdır.

AB'deki müşterek sorumlu üye şirket, hukuka aykırılığın kendisi ile hiçbir ilgisinin bulunmadığını kanıtlarsa sorumluluktan kurtulabilmektedir (Regülasyon m.47/2-f). Türk hukukunda da sorumluluk hukuku ve KVKK'daki bağlayıcı şirket kuralları kapsamında, bu durumda, sorumluluğun kimde olduğunun ve kurtuluş kanıtı sunulup sunulamayacağının yoruma bırakılmadan kanunla düzenlenmesi gerekmektedir. Sorumluluk konusunda özel hüküm öngörülmemiş olması, veri sorumlularının hukuki sorumluluğunun çok genel olarak hükme bağlanmış olması kanuni bir eksikliktir.

AB hukuku uyarınca grup şirkette, bağlayıcı şirket kurallarının değişmesi halinde bunun raporlanması ve veri koruma kuruluna bildirilmesi gerekmektedir (Regülasyon m.47/2-k). Veri koruma kuruluna bu bildirimi yapacak şirket içindeki görevliler belirlenmeli ve daha önemlisi, bu değişiklik bağlayıcı şirket kurallarını esastan etkiliyorsa veri koruma makamına başvurulmalı ve yeni bir onay sürecinin gerekip gerekmediğine ilişkin görüş alınmalıdır. Türk hukukunda Kurul duyurusunda bu değişikliklerin raporlama mekanizmasına yer verilmişse de, bağlayıcı şirket kurallarının esasını etkileyecek değişikliklerde Kurul'dan onay alınmasına ilişkin bir düzenleme yapılması uygun olacaktır.

Grup şirketin üçüncü ülkedeki üyeleri, bağlayıcı şirket kurallarında verilen taahhütlere bakmalı ve bağlı oldukları ulusal mevzuatla karşılaştırma yapmalıdırlar. Üçüncü ülkedeki veri koruma yasalarına ilişkin bu karşılaştırma, şirketin uyumluluk bölümü ve veri koruma görevlisine iletilmelidir (Regülasyon m.47/2-m). Buna ilişkin Kurul duyurusunda düzenleme olsa da, bunun işler hale gelip gelmediğinin nasıl denetleneceğine dair yasal düzenleme bulunmamaktadır. Bağlayıcı şirket kurallarında verilen taahhütlere aykırı hükümlerin tespit edilmesi halinde Kurul'a bilgi verilmesi gerekmektedir. Bununla birlikte, bağlayıcı şirket kurallarının uygulanması açısından geçerli olan yasal düzenlemelerin KVKK olduğu açık şekilde yazılmalı ve Kurul, yetkili makam şeklinde gösterilmelidir. Bağlayıcı şirket kurallarında, üçüncü ülkelerin iç mevzuatından kaynaklanabilecek, idari makamların denetim yetkisine dair bir istisna yer almaktadır. Kurul duyurusunda bahse konu istisna "her halükârda demokratik bir devlet düzenlemesinin gereklerini aşmayacak şekilde" ibaresiyle, belirsiz bir şekilde hüküm altına alınmıştır. Tüm belirsizliklerin giderilmesi ve özellikle etkin bir dış bağlayıcılık açısından mevzuat değişikliği önem arz etmektedir.

Bağlayıcı şirket kurallarına ilişkin şirketlerin irtibatlı oldukları veri koruma kurulları, ilgili ülkenin veri koruma kurulu olmaktadır. Ancak Regülasyon kapsamında (m.70) Avrupa Veri Koruma Kurulu'nun Regülasyon'un düzenli uygulanmasını sağlamak ve Avrupa Komisyonu'na; veri sorumluları, veri işleyenler ve denetim kurumları arasındaki veri aktarımlarına dair bağlayıcı şirket kurallarının şekli ve usullerine dair tavsiyelerde bulunmak gibi denetim görevleri bulunmaktadır. İlgili ülkelerdeki veri koruma kurullarının ülkemizdeki Kurul'un görevini yerine getirdiği söylenebilse de, bu durumda denetim organı olabilecek bir üst kurulun ülkemizde bulunmadığı ifade edilebilir.

Sonuç olarak, bağlayıcı şirket kurallarının taahhüdü veren grup şirketin Türkiye'deki üyesi için birçok yarar sağlayacağı açıktır. Çünkü, bağlayıcı şirket kuralları kapsamındaki taahhütleri verebilen ve bunu uygulayabilen Türkiye'deki üye şirket, Regülasyon'daki veri koruması kurallarına uyum sağlamış olacaktır. Bu durum Türkiye'deki üye şirket için büyük bir ekonomik yarar, ispat kolaylığı ve şeffaflık getirecektir. Ancak şu anki hali ile Regülasyon ve KVKK'nın bu kurallar açısından farklılık gösterdiği noktalarının olması bu uyumun sağlanmasında her zaman bir engel teşkil edecektir. Bağlayıcı şirket kurallarının Kurul duyurusu ile getirilmiş olması

güzel bir gelişme olsa da, kanaatimizce henüz veri koruma yetkilisi, etki analizi gibi mekanizmalar dahi Türk mevzuatı ve uygulamasında yerini bulamamışken bu mekanizmaların içinde yer alması gereken bağlayıcı şirket kurallarının bunlardan önce getirilmiş olması sıralama açısından hatalıdır. Bu kuralların Kanun'da henüz yerini almamış olması da eksikliktir.

Veri Koruma Hukuku açısından uluslarası bir korumayı taahhüt edebilecek nitelikte olan bu kuralların onay sürecinin 1,5 yıla yakın sürebilecek olması bu süre zarfında kişisel veriler aktarılırken özellikle veri sorumlularınca ne yapılacağını ve nasıl davranılacağını düşündürtmektedir. Uzun süren onay süreci nedeniyle şirketler Kurul'dan onay beklerken halihazırda yaptıkları hatalı aktarımlara onay süresince devam edebileceğinden, uygulamada bu bekleme süreci ihlal oluşturabilecek veri aktarımına yol açabilecektir.

Ek olarak, Kurul'un bağlayıcı şirket kuralları yönüyle başvuru sonuçlarını 'gerektiğinde' açıklaması yerine tüm başvuruların neticelerini açıklaması ve bu kurallardaki eksiklikleri kamuoyuyla paylaşması gereklidir.

Türk Hukukunda ancak belirtilen eksikliklerin giderilmesi sayesinde Regülasyon ile sağlanmak istenen uyum tam olarak sağlanabilecek ve bu kurallar etkin bir aktarım yolu şeklinde kullanılabilecektir.

KAYNAKÇA

Akdağ, Hale, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, Adalet Yayınevi, 1. Baskı, 2013.

Akgül, Aydın, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*, İstanbul, Legal, 2014. (Akgül Kararlar şeklinde anılmıştır)

Akgül, Aydın, *Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi*, Kocaeli Üniversitesi Doktora Tezi, Kocaeli, 2013. (Akgül Tez şeklinde anılmıştır)

Akgül, Aydın, *Danıştay Kararları Işığında Kişisel Sağlık Verilerin Korunması*, Danıştay Dergisi, (133), s:21-45, 2013.

Akipek, Jale G., Akıntürk, Turgut, Ateş Karaman, Derya, *Türk Medeni Hukuku, Başlangıç Hükümleri, Kişiler Hukuku*, 11. Bası, C.I, Beta Yayınevi, İstanbul, 2014.

Akkurt, Sinan Sami, *Sosyal Medyada Gerçekleşen İhlâller Karşısında Kişilik Hakkının Korunması*, Ankara, Seçkin, 2019.

Akman, Sermet, Burcuoğlu, Haluk, Altop, Atilla, *Tekinay Borçlar Hukuku Genel Hükümler*, İstanbul, 1993.

Aksoy, Hüseyin Can, *The Right to Personality and It's Different Manifestations as the Core of Personal Data*, Ankara Law Review, 5 (2), s.215 vd., 2008.

Aksoy, Hüseyin Can, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, 1. Baskı, Ankara, Çakmak Yayınevi, 2010.

Akyol, Şener, *Dürüstlük Kuralı ve Hakkın Kötüye Kullanılması Yasağı*, Filiz Kitapevi, İstanbul, 1995.

Antalya, Osman Gökhan ve Topuz, Murat, *Eşya Hukuku Marmara Hukuk Yorumu*, 4(1), Ankara, Seçkin, 2019.

Antalya, Osman Gökhan/ Topuz, Murat, *Medeni Hukuk C. I*, Genişletilmiş 3. Baskı, Ankara 2019.

Arkan, Sabih, Ticari İşletme Hukuku, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayını, Ankara, Türkiye 2014.

Aşıkoğlu, Şehriban İpek, *Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri*, İstanbul, On İki Levha Yayınları, 1. Baskı, 2018.

Avcı Braun, Cihan, Kişisel Verilerin İşlenmesinde Rıza, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Cilt:15, Sayı:1, s.13-34, Haziran 2018.

Ayan, Mehmet ve Ayan, Nurşen, *Kişiler Hukuku*, Ankara, Seçkin, 2016.

Aydın, Muhammet, Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu ve Yargısal Denetimi, Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü, *Yüksek Lisans Tezi*, Ankara, 2020.

Aydın, Sedat Erdem, *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu*, On İki Levha Yayıncılık, İstanbul, 1. Baskı, 2015.

Ayözger Öngün, Çiğdem, *Kişisel Verilerin Korunması Hukuku Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil*, İstanbul, Beta Yayınları, Genişletilmiş 2. Baskı, İstanbul, 2019.

Başalp, Nilgün, *Kişisel Verilerin Korunması ve Saklanması*, Yetkin Yayınları, Ankara, 2004.

Başalp, Nilgün, Sırabaşı, Volkan, İlbaş, Çığır, Hanesson, Einar, *Kişisel Verilerin Korunması, Ankara Barosu Uluslararası Hukuk Kurultayı 2008 Bilişim ve Hukuk*, II, 291-323, 2008.

Bartow, Ann, *Our Date, Ourselves: Privacy, Propertization and Gender. USFL. Review*, 1999.

Belge, Ayşe Merve, *Özellikle Kişisel Verilerin Korunması Kanunu Çerçevesinde İşçilerin Kişisel Verilerinin İhlâli ve Korunması Yolları*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 19, (Şeref Ertaş Armağanı Özel Sayısı), 2017.

Beyleveld Deryck, Towned, David, Segolene Rouille- Mirza and Jessica Wright, *The Data Protection Directive and Medical Research Across Europe*, Burlington:Ashgate Publishing Limited, 2004.

Beytar, Erbil, *İşçinin Kişiliğinin ve Kişisel Verilerinin Korunması*, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2018.

Bainbridge, David, *Data Protection, Welwyn Garden City: CLT Professional Publishing*, 2000.

Bilge, Necip, *Hukuk Başlangıcı*, Ankara, Turhan Kitabevi, 2007.

Bowman, John, Gufflet, Myriam, *'Meeting the Challenge of a Global GDPR and BCR Programme', European Data Protection Law Review*, C. 3, S. 2, s.257-261, 2017.

Bygrave, Lee Andrew, *Data Protection Law*, Oxford University Press, 2014.

Carter, Edward L., "*The Right To Be Forgotten*" (Oxford Research Encyclopedia of Communication, Kasım, 2016.

Cunningham, McKay, *Complying with International Data Protection Law, University of Cincinnati Law Review*, S.84 (2), 2018.

Çabuk, Ezgi, *Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*, Bahçeşehir Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2020.

Çekin, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 3.Baskı, Oniki Levha Yayınları, İstanbul 2020.

Çekin, Mesut Serdar, '*6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanununun Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi'*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 74, S.2, s. 629-644, 2016,

Çekin, Mesut Serdar, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, 1.Bası, İstanbul, Onikilevha Yayınevi, 2018.

Çelik, Yeşim, *Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı*, Türkiye Adalet Akademisi Dergisi, 8 (32), s.391 vd., 2017.

Dağ, Güray, *Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması*, Marmara Üniversitesi, Yayımlanmamış Doktora Tezi, İstanbul, 2011.

Determann, Lothar; *Kişisel Verilerin Korunması Uygulama Kılavuzu – Şirketlerin Uluslararası Mevzuata Uyumu*, Çeviri: Av. Hilal Temel, On İki Levha Yayınları, İstanbul, Ocak 2020.

Develioğlu, Hüseyin Murat, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*, 1. Baskı, On İki Levha Yayıncılık, İstanbul, 2017.

Dove, Edward, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, *The Journal of Law, Medicine & Ethics*, 46, s.1013-1030, 2018.

Döner, Ayhan, *Şeffaf Devlette Bilgi Edinme Hakkı ve Sınırları*, İstanbul, Oniki Levha Yayınları, 2010.

Dural, Mustafa, Öğüz Tufan, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 16. Baskı, Filiz Kitabevi, İstanbul, 2015.

Dural, Mustafa, Öğüz Tufan, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 12 Basıdan 13. Tıpkı Basım, Filiz Kitabevi, İstanbul, 2013.

Dülger, Murat Volkan, *Kişisel Verilerin Korunması Hukuku,* İstanbul, Hukuk Akademisi Yayınları, 1.Baskı, 2019.

Dülger, Murat Volkan, *KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları*, Bkz: https://www.hukukihaber.net/kvkkdan-kisisel-verilerin-yurt-disina-aktariminda-onemli-bir-adim-baglayici-sirket-kurallari-makale,7685.html.

Eraslan Türkmen, Sevgi, *Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller*,1. Baskı, On İki Levha Yayıncılık, İstanbul, 2019.

Eren, Fikret, *Borçlar Hukuku Genel Hükümler*, Yetkin Yayınları, 21. Bası, Ankara 2017.

European Union Agency For Fundamental Rights, *Handbook on European Data Protection Law*, Luxembourg, 2018.

Göçmen Uyarer, Sinem, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması,* 1. Baskı, Seçkin Yayıncılık, Ankara, 2019.

Gürpınar, Damla, *Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*, D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Şeref ERTAŞ'a Armağan, C. 19, Özel Sayı-, s.679-694, 2017.

Gürkan, Ülker, *Kişilik Kavramının Evrimi. Prof. Dr. Hamide Topçuoğlu'na Armağan*, Ankara, 1995.

Han, Işık Aslı, *Kişisel Verilerin İşlenmesi Bağlamında Hukuka Uygunluk Sebebi Olarak Veri Sahibinin Rızası*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, Cilt:18, Sayı:1, Ocak 2019.

Hatemi, Hüseyin, *Kişiler Hukuku*, İstanbul, On İki Levha, 2018.

Helvacı, Serap, *Gerçek Kişiler*, İstanbul, Legal Yayıncılık, 4. Bası, 2012.

Henkoğlu, Türkay, *Bilgi Güvenliği ve Kişisel Verilerin Korunması,* Yetkin Yayınları, Ankara, 2015.

Houser, Kimberly, Voss, Gregory, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?, *Richmond Journal of Law & Technology,* 2018.

İmre, Zahit, *Kişilik Hakkının Korunmasına İlişkin Genel Esaslar, Özellikle İsim Hakkı ve İsim Hakkının Korunması*, Seçkin Armağanı, Ankara, 1974.

İşgüzar, Hasan, "*3444 Sayılı Kanunla Değiştirilen Borçlar Kanununun 49. Maddesine Göre Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları*", Ankara Barosu Dergisi, 1990/6.

Kağıtçıoğlu, Mutlu, *Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bakış*, İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi, 1(2), s.72-99, 2016.

Kahraman, Zafer, *Medeni Hukuk Bakımından Tıbbi Müdahaleye Hastanın Rızası*, İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt 7, Sayı 1, s:479 – 510, 2016.

Kang, Jerry, *Information Privacy in Cyberspace Transactions. Stanford Law Review*, 1998.

Kama Işık, Sezen, *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış: 2016/679 Sayılı GVKT ile 6698 Sayılı KVKK'nın Detaylı Analiz ve Karşılaştırması*, 1. Basım, On İki Levha Yayıncılık, İstanbul, 2020.

Kara, Hacı, '*Türk Hukukunda İrtibat Bürosu ve Özellikleri'*, İzmir Barosu Dergisi, C. 83, S. 3, s.167-198, 2019.

Kaya, Afra Ece, *Kişilik Hakkı Olarak Kişisel Veriler ve Yeni Kişisel Verilerin Korunması Kanunu*, Terazi Hukuk Dergisi, Cilt:12, Sayı:125, s.67-80, Ocak 2017.

Kaya, Bedii, *Kişisel Verileri Koruma Hukuku– Mevzuat ve İçtihat*, 1. Basım, On İki Levha Yayıncılık, İstanbul, 2018.

Kaya, Cemil, *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi*, *İÜHFM*, C. 69, S. 1-2, s.317-334, 2011.

Kılıçoğlu, Ahmet, *Şeref Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk*, 4. Bası, Turhan Kitapevi, Ankara, 2013.

Kılınç, Doğan, Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, *AÜHFD*, C.61, S.3, s.1089-1169, 2012.

Kişisel Verileri Koruma Kurumu, *6698 sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar*, Yayın No: 31, Ankara, 2020. Bkz: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/28d8adba-2b41-41b2- bf36-d0ff0d845666.pdf, (Doğru Bilinen Yanlışlar).

Kişisel Verileri Koruma Kurumu, *100 Soruda Kişisel Verilerin Korunması Kanunu*, KVKK Yayınları, Ankara, 1. Baskı, 2018.

Kişisel Verileri Koruma Kurumu, '*Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesine İlişkin Rehberi'*, Sage Matbaacılık, Ankara, 2017, Bkz: https://www.kvkk.gov.tr/yayinlar/kişisel%20verilerin%20silinmesi, %20yok%20edilmesi%20veya%20anonim%20hale%20getirilmesi%20rehberi.pdf.

Kişisel Verileri Koruma Kurumu, '*Veri Güvenliği Rehberi'*, ISBN : 978-975-19-6834-O, KVKK Yayınları, Ankara, 2018, Bkz: https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf.

KOCABAŞ, Gediz, "*KVKK'da Yer Alan Kurum ve Kavramların TMK ve Kıta Avrupası Hukuk Sistemi Kapsamında Değerlendirilmesi*", Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku, Editörler: Leyla Keser Berber, Ali Cem Bilgili, Marmara Hukuk Bilimsel Toplantılar Serisi-I, 17 Nisan 2019, On İki Levha Yayınları, İstanbul, Ocak 2020.

Korkmaz, İbrahim, *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*, Seçkin Yayıncılık, Ankara, 1. Baskı, 2017.

Korkmaz, İbrahim, *Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme*, TBB Dergisi, s.81-152, 2016.

Kulezsa, Joanna, Transboundary Data Protection And İnternational Business Compliance, *International Data Privacy Law*, C.4, S.4, s.298 – 306, 2014.

Kuner, Christopher, *European Data Protection Law (Corporate Compliance and Regulation),* Second Edition, Oxford University Press, 2007.

Küzeci, Elif, *Kişisel Verilerin Korunması*, Turhan, Ankara, 2010.

Küzeci, Elif, *Kişisel Verilerin Korunması*, Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara, 2019.

Lachaud, Eric, Why the Certification Process Defined in the GDPR Cannot Be Successful, *Computer Law & Security Review*, C. 32, s.814–826, 2016.

Lambert, Paul, *Understanding the New European Data Protection Rules*, Taylor & Francis, 2017.

Lieshout, Marc, The Value of Personal Data, *IFIP Advances in Information and Communication Technology*, C.457, S.5, s.26-38, 2015.

Litman, Jessica, *Information Privacy / Information Property, Stanford Law Review*, 2000.

Marques, João, *And they built a crooked harbour – the Schrems ruling and what it means for the future of data transfers between the EU and US, UNIO - EU Law Journal*, C.2, S.2, s.54-70, June 2016.

Masoch, Daniela Fábián "*Why Should Companies Invest in Binding Corporate Rules?*", The International Comparative Legal Guide to: Data Protection, 2019.

Memiş, Tekin, '*Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni'*, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt:3, Sayı:6, Aralık 2017.

Mendos Kuşkonmaz, Elif, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, İstanbul Üniversitesi, *Yayımlanmamış Yüksek Lisans Tezi*, İstanbul, 2013.

Moerel, Lokke, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, Oxford University Press, 2012.

Nomer, Haluk N., *Borçlar Hukuku Genel Hükümler*, 15.Bası, Beta Yayınevi, İstanbul 2017.

Oktay Özdemir, Saibe, *Tıbbi Müdahaleye ve Tıbbi Müdahalenin Durdurulmasına Rızanın Kimler Tarafından Verileceği*, Prof. Dr. Rona Serozan'a Armağan, C.II, On İki Levha Yayıncılık, İstanbul 2010.

Oğuzman, M. Kemal, Seliçi, Özer, Oktay Özdemir, Saibe, *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, 14. B, İstanbul, Filiz Kitapevi, 2014.

Oğuzman, Mustafa Kemal, Seliçi, Özer, ve Oktay Özdemir, Saibe, *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, 17.B, İstanbul, Filiz Kitapevi, 2018.

Oğuzman, M.Kemal, Öz, Turgut, *Borçlar Hukuku Genel Hükümler* Cilt – II, 14. Bası, Vedat Kitapçılık, İstanbul, 2018.

Özdemir, Hayrunnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,* Seçkin, Ankara, 2009.

Özkan, Oğulcan, *Kişisel Verilerin Korunması,* Ankara Üniversitesi Sosyal Bilimler Enstitüsü, *Yüksek Lisans Tezi*, Ankara, 2020.

Öztürk, Bahri, Altınok Çalışkan, Elif, *"Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu",* Fasikül Hukuk Dergisi, Cilt: 10, Sayı:100, Mart 2018.

Parlak Börü, Şafak, "*Esra Kararı Işığında Bir Hassas Denge Değerlendirmesi: Kişilik Haklarının Korunması vs. Sanat Özgürlüğü",* İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 8, Sayı: 2, 2017.

Polat, Alperen, *Sorumluluk Hukukunda Rıza*, On İki Levha Yayıncılık, İstanbul, 2019.

Purtova, Nadezhda, *Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights, Netherlands Quarterly of Human Rights Journal*, 2010.

Prins, Corien, *When Personal Data, Behavior and Virtual Identities Become a Commodity: Would a Property Rights Approach Matter? Script – ed.*, 2006.

Reisoğlu, Safa, *Türk Borçlar Hukuku Genel Hükümler*, 23. Bası, Beta, İstanbul, 2012.

Samuelson, Pamela, *Privacy as Intellectual Property?* Stanford Law Review, Vol. 52, No. 5, May, 2000 Symposium: *Cyberspace and Privacy: A New Legal Paradigm?*, 2000.

Serdar, İlknur, *Radyo ve Televizyon Yoluyla Kişilik Hakkının İhlali ve Kişiliğin Korunması*, Ankara, Seçkin Yayınevi, 1999.

Serozan, Rona, *Medeni Hukuk Genel Bölüm – Kişiler Hukuku*, Yayın No:253, Vedat Kitapçılık, İstanbul, 2011.

SEROZAN, Rona, *İfa, İfa Engelleri, Haksız Zenginleşme, Borçlar Hukuku Genel Bölüm,* Cilt 3, Filiz, İstanbul, 2009.

Sullivan, Claire, EU GDPR Or APEC CBPR? A Comparative Analysis of The Approach of The EU And APEC To Cross Border Data Transfers And Protection of Personal Data İn The Iot Era, *Computer Law and Security Review*, C. 35, s.380-397, 2019.

Şen, Ersan, *Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi*, İBD, 83(3), 2009.

Şener, Gülnihal Emine, *Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, Adalet Dergisi*, s.72-86, 2011.

Şimşek, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Yayınları, İstanbul, 2008.

Taştan, Furkan Güven, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, İstanbul, On İki Levha Yayınları, 2. Baskı, 2017.

Toparlak, Rüya Tuna, *Genel Veri Koruma Tüzüğünde Bağlayıcı Şirket Kuralları: Avrupa Birliği Hukukunda Uygulama*, Türk-Alma Üniversitesi Sosyal Bilimler Enstitüsü, *Yüksek Lisans Tezi*, İstanbul, 2021.

Turan, Metin, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması,* Seçkin Yayınları, Güncellenmiş 2. Baskı, Ankara, 2019.

Uncular, Selen, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması*, Seçkin Yayıncılık, Ankara, Güncellenmiş ve Genişletilmiş 2. Baskı, 2018.

Uygur, Turgut, *6098 Sayılı Türk Borçlar Kanunu Şerhi*, 1. Baskı, Seçkin Yayıncılık, İstanbul, 2012.

Üçüncü, Sümeyye Hilal, *Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması*, On İki Levha Yayınları, 1. Baskı, İstanbul, 2019.

Ünal, Mehmet ve Başpınar, Veysel, *Şeklî Eşya Hukuku*, Savaş Yayınevi, Ankara, 2017.

Ünsal, Çağrı Zeybek ., "*Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri ile Uyumluluğu ve Avrupa Birliği'nin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi",* Hacettepe Hukuk Fakültesi Dergisi, 3/1, s.99-124, 2013.

Yeditepe Üniversitesi, Avrupa Ve Türk Hukukunda Kişisel Verilerin Korunmasına İlişkin Güncel Sorunlar Uluslararası Sempozyumu Bildiri Özeti, Bkz: https://law.yeditepe.edu.tr/sites/default/files/kvkk_-_kitapcik-v3.pdf.

Yılmaz, Ejder, *Hukuk Sözlüğü*, Ankara, 2004.

Yılmaz, Sabire Sanem, *Kişisel Verilerin Korunması Regülasyonu ve Unutulma Hakkı*, Terazi Hukuk Dergisi, C:13, S.142, s.116-121, Haziran, 2018.

Yörük, Onur Doğan, *(AB) 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Kişisel Verilerin Korunması,* İzmir Ekonomi Üniversitesi Lisansüstü Eğitim Enstitüsü, Yüksek Lisans Tezi, İzmir, 2019.

Yücedağ, Nafiye, *Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri*, İÜHFM, C. 75, S. 2, s.765-790, 2017.

Várkonyi, Gizem, Gültekin, *Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Gerçek Kişilerin Kişisel Sosyal Robot Kullanımından Doğabilecek Sorumlulukları*, Kişisel Verileri Koruma Dergisi, Cilt:2, Sayı:2, 2020.

Velidedeoğlu, Hıfzı Veldet, *Türk Medeni Hukuku, Umumi Esaslar*, İstanbul Üniversitesi Yayınları, İstanbul, C.1, 5. Bası, 1956.

WP Article 29 Data Protection "*Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*'' Bkz: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/binding_corporate_rules_for_controllers.pdf.