T.C.

BAHÇEŞEHİR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLİŞİM HUKUKU ANABİLİM DALI

ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMA VE KİŞİSEL VERİLERİN KORUNMASI

YÜKSEK LİSANS TEZİ

CEREN TUĞÇE SAVAŞCI

TEZ DANIŞMANI

Prof. Dr. Ahmet Naci Ünal

İSTANBUL, 2023

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 : Ceren Tuğçe Savaşcı

İmza :

ÖZET

ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMA VE KİŞİSEL VERİLERİN KORUNMASI

Savaşcı, Ceren Tuğçe

Bilişim Hukuku Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Ahmet Naci ÜNAL

Eylül 2023, 143 sayfa

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ve artan internet kullanımının sonucu olarak dijital teknolojiler, hayatımızın ekonomik, sosyal, kültürel ve siyasi alanlarına erişmiş, bunları değiştirip, adeta yeniden düzenlemiştir. İnsan hayatının çeşitli alanlarında gerçekleşen bu çığır açan nitelikteki gelişmeler sayesinde, bankacılık işlemlerinden, sağlık hizmetlerine, sosyal medya kullanımından, ticaret işlemlerine kadar pek çok süreç, dijital ağlar üzerinden kolaylıkla yapılabilir hale gelmiştir. Özellikle e-ticaret alanında meydana gelen gelişmeler, dijital pazarların dünya ekonomisindeki payını gün geçtikçe artırmaktadır. Ancak ortaya çıkan küresel çaplı dijital pazarlar ve diğer her türlü çevrimiçi işlem, süreçleri kolaylaştırarak, kişilere zaman ve paradan tasarruf etmek gibi yararlar sağlarken, aynı zamanda da veri güvenliği ve mahremiyete ilişkin bir takım tehditleri de beraberinde getirmiştir. Nitekim çok çeşitlenerek yaygınlaşan dijital işlemler sırasında kayıt altına alınan kişisel verilerin miktar ve çeşitliliği ile veri hareketliliğinin artması, bu verilere üçüncü kişiler tarafından erişilerek, verilerin farklı amaçlarla farklı şekillerde işlenebilme kapasitelerini de artırmıştır. Bu durum, ilgili kişilerin, temel hak ve özgürlükler bağlamında korunan kişisel verileri üzerindeki kontrolünü zorlaştırarak, bir takım temel hak ihlallerine ve dolayısıyla da maddi-manevi kayıplara sebep olabilmektedir. Söz konusu olumsuzluklara rağmen, küresel arenada dijital dünyadan, özellikle de ortaya çıkan dijital ekonomiden alınabilecek payın bir kenara bırakılamayacağı da aşikârdır. Zira dijital dünyada var olamayan devlet, kurum ve kuruluşların gelecekte ekonomik varlıklarını parlak bir şekilde devam ettirebilmeleri olası gözükmemektedir. Tüm bunların bilinciyle, kişisel verilerin daha iyi nasıl korunması gerektiği hususu,

2000'li yıllardan itibaren Avrupa Birliği'nin ("Birlik") gündeminden neredeyse hiç düşmemiştir.

Avrupa Birliği, hem Birlik'in manevi köklerinin dayandığı temel hak ve özgürlüklerin gelişen teknolojiler karşısında güncelliğini sağlamak, hem de Avrupa dijital tek pazarının oluşumunu tamamlayarak, her geçen gün gelişerek toplam ticaret içindeki payını artıran dijital ekonomiden hak ettiği payı alıp, küresel rakipleri karşısında rekabet avantajını yitirmemek amacı ile kişisel verilerin korunmasına ilişkin çeşitli yasal düzenlemeler yapmaktadır. 2018 yılında yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü ("GVKT") de bu yolda atılmış önemli bir adımdır.

Dijital çağda kişisel verilerin korunması dünya gündemini uzun süredir meşgul etmiş ve özellikle Avrupa Birliği sınırları dahilinde, bu korumanın uygun, yeterli ve gerekli şekilde sağlanabilmesine yönelik düzenlemeler gerçekleştirilmiştir. Çalışmada öncelikle kişisel veri koruma kapsamı ve Türkiye mevzuatı incelenmiş, sonrasında ise Avrupa Birliği'nce kişisel verilerin korunması alanında özellikle de çevrimiçi davranışsal pazarlama uygulamaları kapsamında yapılmış ve yapılması planlanan düzenlemeler açıklanmıştır. Dijital devrim sonucu ortaya çıkan ve çevrimiçi davranışsal pazarlama uygulamalarının neredeyse her bireye etki ettiği yeni dünya düzeninde, ilgili Avrupa Birliği düzenlemelerinin Türkiye mevzuatı ile karşılaştırılmasının da amaçlandığı bu çalışmada; tespit edilen eksiklikler gösterilmeye çalışılmış ve çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Çevrimiçi, davranışsal pazarlama, kişisel verilerin korunması.

ABSTRACT

ONLINE BEHAVIORAL MARKETING AND PERSONAL DATA PROTECTION

Savaşcı, Ceren Tuğçe

Master's Program in Information Technology Law

Supervisor: Prof. Dr. Ahmet Naci ÜNAL

September 2023, 143 pages

Due to advancements in information and communication technologies coupled with the growing utilization of the internet, digital technologies have permeated, altered, and reshaped the economic, social, cultural, and political facets of society. These transformative changes have facilitated numerous activities—ranging from banking operations to healthcare, and from social media interactions to commercial engagements—through digital networks. Notably, advancements in e-commerce have augmented the significance of digital markets within the global economy. While such expansive digital markets and varied online transactions confer benefits by streamlining operations and yielding economic efficiencies, they concurrently introduce challenges pertaining to data security. The proliferation and diversification of personal data collected during digital transactions and the enhanced mobility of such data have amplified the potential for diverse processing by unauthorized third parties. This not only impedes individuals' control over their personal data, which is safeguarded under fundamental rights and freedoms, but also heightens the risk of infringements leading to tangible and intangible damages. Nonetheless, the global landscape recognizes the indispensable value of the burgeoning digital economy. It is seemingly implausible for states, entities, and organizations to maintain a prosperous economic trajectory without a digital presence. Recognizing these dynamics, the European Union has consistently prioritized the protection of personal data since the early 2000s.

The European Union, both to protect the fundamental rights and freedoms on which the moral roots of the Union are based, within the scope of current and harmonized

laws in the face of developing technologies, as well as to complete the formation of the European digital single market, to get its rightful share from the digital economy, which increases its share in total trade by developing day by day, in order not to lose its competitive advantage against its global competitors, makes various legal regulations regarding the protection of personal data. A notable manifestation of this commitment is the European Union General Data Protection Regulation, which was enacted in 2018.

The protection of personal data in the digital age has been a significant concern on the global agenda for a long time. Particularly within the borders of the European Union, important steps have been taken to ensure appropriate, sufficient, and necessary protection. This analysis initially delves into the domain of personal data protection and the pertinent legislation in Turkey. It then elucidates regulations instituted, and anticipated, by the European Union concerning personal data protection, emphasizing online behavioral marketing practices. Given the pervasive influence of the digital revolution, manifesting predominantly through online behavioral marketing, this study endeavors to juxtapose relevant EU directives with Turkish legal frameworks, spotlighting discerned lacunae and proffering remedial recommendations.

Keywords: Online, behavioral marketing, protection of personal data.

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
AK	: Avrupa Konseyi
ABD	: Amerika Birleşik Devletleri
a.g.k.	: Adı geçen kaynak
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme
AYM	: Anayasa Mahkemesi
bkz.	: Bakınız
BM	: Birleşmiş Milletler
BM Rehber İlkeleri	: Birleşmiş Milletler Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
COPPA	: 16 CFR Part 312 Sayılı Amerika Birleşik Devletleri Çocukların Çevrimiçi Gizliliğini Koruma Federal Yasası
CCPA	: Kaliforniya Tüketici Gizlilik Yasası
ÇDP	: Çevrimiçi Davranışsal Pazarlama
ÇKK	: 5395 sayılı Çocuk Koruma Kanunu
Direktif	: 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
EDPB	: European Data Protection Board (Avrupa Veri Koruma Kurulu)
EGT	: Avrupa Birliği Gizlilik ve Elektronik Haberleşme Tüzüğü
EHK	**:** 5809 Sayılı Elektronik Haberleşme Kanunu
ETK	**:** 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
FTC	:Amerika Federal Ticaret Komisyonu
GVKT veya GDPR	: 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü
İHEB	: Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
KVKK	: 6698 sayılı Kişisel Verilerin Korunması Kanunu
m.	: Madde
MSHS	: Birleşmiş Milletler Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme
OECD	: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TMK	: Türk Medeni Kanunu
t.y.	: tarih yok
vd.	: ve devamı
WP 29	: Madde 29 Veri Koruma Çalışma Grubu
108 +	: Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşmeyi Değiştiren 223 sayılı Protokol

108 sayılı Sözleşme : Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

GİRİŞ

İçinde bulunduğumuz bilişim çağında, teknolojiden ve teknoloji ürünü araçlardan uzak bir yaşam sürdürebilmek neredeyse imkânsız bir hal almıştır. Her geçen gün, büyük bir hızla değişip gelişen teknoloji, pek çok araç ile insan hayatına müdahil olmaktadır. Bunların başında akıllı telefonlar ve bilgisayarlar gelse de; tabletler, akıllı saat ve bileklikler, akıllı ev cihazları da teknoloji ile insan hayatına dâhil olan diğer araçlar arasında yer almaktadır. We Are Social[1]'in sunmuş olduğu verilere göre; 2023 yılı itibarıyla, 8.01 milyarlık Dünya nüfusunun 5.44 milyarı (%68) akıllı telefon, 5.16 milyarı (%64.4) internet kullanmakta, 4.76 milyarı (%59.4) aktif sosyal medya kullanıcısı olarak dijital dünyaya dâhil olmakta ve dünya çapında ortalama olarak her bir internet kullanıcısı, günlük 7 saate yakın süre internette zaman geçirmektedir. İnternet bir mecra olarak, bireylere; eğitimden alışverişe, iletişimden yatırıma pek çok konuda imkân ve alan sağlamakta, bu alanda gerçekleşen hizmetlerden yararlanmak üzere çoğunlukla kişisel veriler kullanıma sunulmaktadır. Yalnızca internet ortamında değil, internet ortamı dışında gerçekleşen faaliyetlerde de kişisel veriler işlenmekte, kimi zaman işlenen kişisel veriler başka veri sorumlularına aktarılmakta ve kişisel veri işleme, süreklilik arz eden bir faaliyet olarak insan hayatının ayrılmaz bir parçası haline gelmektedir. Bundan ötürüdür ki; gerek çevrimiçi gerekse yüz yüze ortamlarda kişisel verilerin korunması; günümüz çağında bir gereklilik, hatta bir zorunluluk haline gelmiştir.

İç hukukumuzda kişisel verilerin korunmasına hizmet eden farklı düzenlemeler bulunsa da, bu amaca hasredilmiş genel nitelikte bir düzenlemenin yürürlüğe girişi için 2016 yılını beklemek gerekmiştir. İlk olarak 2010 yılında Anayasa'nın "özel hayatın gizliliği" bahsini düzenleyen 20. maddesinde yapılan değişiklik ile kişisel verilerin korunması anayasal bir statüye kavuşturulmuş, akabinde yalnızca kişisel verilerin korunmasını konu edinen, kişisel veri işleme faaliyetlerine uygulanmak üzere hazırlanan ve 07.04.2016 tarihli ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK" veya "Kanun") ile kişisel verilerin işlenmesinde esas alınacak temel çerçeve çizilmiştir.

[1] We Are Social, Digital 2023 Global Overview Report (January 2023), https://www.slideshare.net/DataReportal/digital-2023-global-overview-report-summary-version-january-2023-v02

Kişisel verilerin hangi durumlarda işlenebileceğini beşinci ve altıncı maddelerinde düzenleme altına alan iş bu Kanun; bireyin, kendi verilerinin geleceğini tayin edebilmesi anlamında, kişisel veriler ve özel nitelikli kişisel veriler bakımından "ilgili kişinin açık rızasını", kişisel veri işleme faaliyetini hukuka uygun kılan haller arasında düzenlemiştir. Benzer şekilde, kişisel verilerin yurt içinde ve yurt dışında aktarımına da imkan sağlayan "açık rıza"; Kanun ve ikincil mevzuat kapsamında verilmiş bir açık rıza olması şartı ile, kişisel verilerin işlenmesinde, faaliyetin yasal zemine oturtulmasına hizmet eden ana araçlardan biri olarak öngörülmüştür.

Kişisel verilerin korunması hukuku bakımından bu denli önem arz eden kavramın, detaylı şekilde incelenmesi ve çevrimiçi ortamlarda işlenen kişisel veriler açısından getirilmiş hukuki düzenlemelerle olan ilişkisi bu çalışmanın başlangıç noktasını teşkil etmektedir.

BİRİNCİ BÖLÜM

KİŞİSEL VERİ KAVRAMININ GELİŞİMİ VE KONUYA İLİŞKİN TEMEL DÜZENLEMELER

Kişisel verilerin korunması, ilişkili düzenlemeler ve çevrimiçi davranışsal pazarlama süreçlerini doğru değerlendirebilmek adına bu bölümde öncelikli olarak kişisel verilerin korunması kavramının gelişimi ve bu çerçevede ortaya çıkan ulusal ve dahi uluslararası düzenlemeler incelenmiştir. Çevrimiçi davranışsal pazarlama uygulamalarının vazgeçilmez parçası olan kişisel veri kavramının günümüzdeki anlamına nasıl ulaştığı ve mevcut koruma hükümlerinin hangi aşamalardan geçerek şekillendiği, çalışmanın son bölümünde yapılan değerlendirmelerin doğru anlaşılabilmesi için önem arz etmektedir.

1.1.Kişisel Verilerin Korunması Kavramının Ortaya Çıkışı ve Gelişimi

Kişisel veri, en genel tabiriyle, "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi"yi ifade etmektedir[2]. Kişisel verilerin korunması ise söz konusu bilgilerin gizli tutulması ve/veya uygun kurallar çerçevesinde kullanılmasına ilişkin faaliyet ve çabaların bütünüyle ilgili bir kavramdır. "Kişisel verilerin korunması" kavramının günümüz anlamıyla ortaya çıkışı, yakın geçmişte gerçekleşmiş olsa da, kişinin kendisine ait birtakım bilgileri gizli tutmak istemesi, insanlık tarihi boyunca varlığını göstermiş bir içgüdüdür. İnsanın sıradan bir canlı değil; toplumsal hayata yön veren bir "kişi" olduğunun farkına varılması ile birlikte, insana ait bilginin ifşa edilmemesi ve gizli tutulması gerekliliği kolaylıkla kabul görmüştür. Kişinin kendi özel hayatına dâhil bilgilerin başkalarına açıklanması ise, özellikle güven ilişkisi çerçevesinde mesleki bir yükümlülüğün ifası kapsamında somutlaşmış; bu durum, ilgili meslek mensuplarına, mesleki ilişkisi çerçevesinde birtakım bilgilerine vakıf olduğu kişilere ilişkin olarak susma yükümlülüğü yüklemiştir[3]. Milattan önce 5. yüzyıldan bu yana geçerliliğini koruyan "hekimin sır saklama yükümlülüğü" ve bu kapsamda icra edilen Hipokrat yemini bunun en bilinen örneklerinden biridir. Hekimin

[2] 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 3/1-d "Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"
[3] Şimşek, Oğuz. 2008, Anayasa Hukukunda Kişisel Verilerin Korunması, s. 5-7.

sır saklama yükümlülüğü kapsamında hekime, hasta-hekim ilişkisi çerçevesinde edinmiş olduğu bilgileri saklama ve başkalarına açıklamama yükümlülüğü getirilmiş ve bu yükümlülük ile bireyin hastalığının toplum tarafından bilinmesi sebebiyle, bireyin sosyal açıdan zarar görmesinin engellenmesi ve hekimlik mesleğine güvenilmesi amaçlanmıştır[4]. Bu uygulamayı ise hekim-hasta ilişkisine benzer şekilde, din adamlarının sır saklama yükümlülükleri, memurun görev sırrı, banka sırrı, avukatın sır saklama yükümlülüğü gibi başka mesleki yükümlülükler kapsamında gizliliğin korunması uygulamaları izlemiş ve mesleği sebebiyle kendisine güvenilerek bilgi verilen kişilerin, güven ilkesi çerçevesinde sahip oldukları bilgileri hukuka aykırı ve yetkisiz şekilde üçüncü kişilere aktarmamaları amaçlanmıştır[5].

Günümüz anlamıyla "kişisel verilerin korunması" kavramının gelişiminde ise, başta bilişim teknolojileri sektörü olmak üzere pek çok kurum ve kuruluşun, hizmetlerini sunarken kişisel verilere duydukları ihtiyacın artması rol oynamıştır[6]. Bu dönemde kamu organları, düzenin sağlanması ve kamu hizmetlerinin sunulması gibi nedenlerle; özel teşebbüsler ise verimliliğin ve kârlılığın geliştirilmesi amacıyla bilgiye gereksinim duymakta, bu kapsamda da bilginin eskiye nazaran daha az maliyetle, daha kolay ve hızlı şekilde depolanabilmesi ve internetin kullanımının yaygınlaşması ise bilgiye erişimi daha kolay bir hale getirmektedir[7].

Gelişen teknoloji sayesinde verimlilik ve üretkenliğin hızla artmasıyla bilgiye erişimin kolaylaşması, birçok açıdan önemli avantajlar sağlasa da bazı dezavantajları beraberinde getirmektedir. Özellikle yakın geçmişte teknolojinin kat ettiği mesafe; izleme ve profil oluşturma tekniklerini daha kolay, daha ucuz ve daha doğru tahminlenebilir hale getirmiş, bu durum gerek kamu sektöründe gerek özel sektörde gözetimin artırılması ihtiyacını doğurmuştur. Bu kapsamda, kişinin ilgi alanları, siyasi görüşü ya da felsefi inancı, beğenileri, kişisel ilişkileri başta olmak üzere bireyin kişiliğine ve özel yaşamına ait pek çok bilginin elde edilmesi ve bu bilgilerin işlenmesi ile birçok başka veriye de ulaşılabilmesi tek tıkla mümkün hale gelmiştir. Teknolojinin çoğu kişi tarafından anlaşılamayan yüzü sebebiyle bireylerin, mahremiyet duygusunun ihlal edildiğine ilişkin endişeleri artmış; ve buna ek olarak insanlık, bireyin düşünme

[4] Şimşek, 2008:5-6.
[5] Şimşek, 2008: 6.
[6] Korkmaz, İbrahim. 2017, Kişisel verilerin ceza hukuku kapsamında korunması, s.71.
[7] Mendos Kuşkonmaz, Elif. 2013, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması Yüksek Lisans Tezi, s.13.

ve hareket etme şekline ya da ifade ve örgütlenme özgürlüğü gibi diğer haklarına etki edebilmesini mümkün kılacak potansiyel bir tehdit ile karşı karşıya olduğunun farkına varmıştır. İleride gerçekleşmesi beklenen amaçları yerine getirmek üzere veri depolanması yoluna gidilmesi ile kişinin kendi verileri üzerindeki denetim hakkının neredeyse kaldırılması; bu yolla bireyin temel hak ve özgürlüklerinin zayıflatılması ve bireyin güçsüzleştirilmesi de diğer bir risk alanı olarak ortaya çıkmıştır[8].

Anılan risklerin bertaraf edilmesi ve her geçen gün gelişen teknoloji sayesinde bireylere gerçek bir korumanın sağlanması, ancak kişisel verilerin kişilik alanına dâhil birer değer olduğunun kabulü ile mümkündür. Bu bakımdan, aşağıda detaylarıyla ele alınacak olan kişisel verilerin korunması hakkı; temel itibarıyla kişinin, kendine ait veriler üzerinde söz sahibi olabilmesi ve kendi verilerinin geleceğini tayin etmesi amacına hizmet etmektedir.

Bilişim teknolojilerindeki gelişmelerin, kişisel verilere erişimin kolaylaşmasına imkân sağladığının fark edilmesi, kişisel verilerin korunması alanındaki ilk tartışmalara zemin hazırlamıştır. 1960'lı yıllarda kişilerin kredi verilebilirliğine büyük önem atfeden Amerika Birleşik Devletleri'nde ("ABD"), bir hesaplama aracı olarak kullanılan bilgisayarların hata yaptığı algısının yaratılması, o dönem büyük bir sosyal değer olarak görülen kredi verilebilirlik hususunda birtakım endişeleri de beraberinde getirmiştir. Anılan tartışmaları, vatandaşların verilerinin bir merkezde toplandığı ve devletin kişilere ait çok sayıda veriyi sakladığı yönündeki haberler takip etmiş; bu gelişmeler neticesinde toplumda, kamusal makamlar tarafından özel yaşam alanlarına müdahale edilebileceği yönünde bir çekince oluşmuştur. ABD'deki gelişmeleri müteakip, İsveç'te de nüfus ve vergi sicillerinin birleştirilmesi ve bireylere ait tüm verilerin burada toplanması yönünde çalışmalar başlatılmıştır. Devletin, ilerleyen teknoloji sayesinde bireylerin verilerine kontrolsüz şekilde erişebilmesi ve elde edilen verilerin merkezileştirilmesine ilişkin uygulamaları; bireyler nezdinde verilerin kötüye kullanılabileceği ve gizliliklerinin ihlal edilebileceği noktasındaki kaygıları had safhaya ulaştırmıştır[9].

Bilgisayarların ortaya çıktığı ve ilk modellerinin yaygınlaştığı yıllarda, kişisel verilerin kaydı konusundaki yeni gelişmelere şüphe ile yaklaşılması, özel hayatın gizliliği

[8] Mendos Kuşkonmaz, 2013:16.
[9] Yüzbaşı Topaz, Firdevs. 2021, Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması, s.118-119.

noktasında yaşanan endişeler ve kişisel verilerin kötüye kullanılmasına ilişkin olumsuz tecrübeler, kişisel verilerin korunması olgusunun ortaya çıkmasına ve böylece ilk yasal düzenlemelerin oluşturulmasına zemin hazırlamıştır[10]. Öte yandan kişisel veri koruma hukukuna ilişkin olarak çıkarılan ilk ulusal düzenleme, Almanya'da yayımlanmış 1970 tarihli Hessen Eyalet Veri Koruma Kanunu olmuştur[11]. Gerek bu kanunun kabulünde gerek kişisel verilerin korunmasına ilişkin olarak Almanya'da federal bir düzenlemenin yapılmasında "Hessen Planı" olarak adlandırılan bir program içerisinde merkezi bir veri bankasının kurulması ve bu durumun özel hayatın gizliliği hakkı üzerindeki olası sonuçları etkili olmuştur. Verilerin korunması görevini aynı zamanda milli istihbarat ve polis teşkilatından da sorumlu İçişleri Bakanlığına veren 1977 tarihli Federal Almanya Veri Koruma Yasası oldukça eleştirilse de söz konusu gelişmeler hızla devam etmiş; Federal Yasa öncesinde çıkarılan 1973 tarihli İsveç[12] ve 1974 tarihli ABD[13] yasalarını, 1978 tarihli Fransa[14] ve diğer Avrupa ülkeleri de takip etmiştir[15].

1970'lerde başlayan ulusal regülasyonları, 1980'li yıllarda uluslararası düzeyde yapılan gelişmeler izlemiştir. Bu kapsamda Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi ("IHEB"), Birleşmiş Milletler Medeni ve Siyasi Haklara ilişkin Uluslararası Sözleşme ("MSHS"), İnsan Hakları ve Temel Özgürlüklerin Korunmasına ilişkin Sözleşme ("AİHS") gibi birçok kaynakta, kişisel verilerin korunması ile özel yaşamın gizliliği hakkının ilişkilendirildiği görülmektedir. Ancak uluslararası alanda doğrudan kişisel verilerin korunmasını hedef alan esas düzenleme, 23 Eylül 1980 tarihinde Ekonomik işbirliği ve Kalkınma Örgütü ("OECD") bünyesinde yapılan "Özel Hayatın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler" olmuştur[16]. Ancak söz konusu ilkelerin bağlayıcı olmayışı, uluslararası sahada bağlayıcılığı bulunan, katılımcı nitelikteki bir metne olan ihtiyacı da gözler önüne sermiş; bu doğrultuda Avrupa Konseyi'nce ("AK") "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması

[10] Küzeci, Elif. 2020, Kişisel Verilerin Korunması, s.117
[11] Dal, Ufuk. 2019, Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti. Kişisel Verileri Koruma Dergisi, 1 (1), s.23.
[12] İsveç Veri Kanunu (Swedish Data Act (SFS 1973:289)).
[13] ABD Gizlilik Kanunu 1974 (The Privacy Act of 1974, as amended, 5 U.S.C. § 552a).
[14] Bilişim ve Özgürlük' Kanunu 1978 (Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties)
[15] Taştan, Furkan Güven. 2017, Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, s.11.
[16] Arslan Öncü, Gülay. 2019. Özel Yaşama ve Aile Yaşamına Saygı Hakkı, s.78-79.

Sözleşmesi" ("108 sayılı Sözleşme") 28 Ocak 1981 tarihinde kabul edilerek imzaya açılmıştır. Böylece ilk defa uluslararası alanda bağlayıcı bir düzenleme ile kişisel verilerin korunması güvence altına alınmıştır[17].

Avrupa'da 1970'li yıllar itibariyle kişisel verilerin korunması adına yapılan çalışmaların ulusal düzeyde kalması ve genel bağlayıcı bir metnin oluşturulmasına duyulan ihtiyaç neticesinde ortaya konulan diğer bir belge de "95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" ("Direktif") dir. 24 Ekim 1995 tarihli Direktif, ortaya konulan ilkeler ve ulaşılması gereken hedefler açısından öncü niteliğe sahip olmuş, ülkemiz başta olmak üzere kişisel verilerin korunması adına yapılan yeni düzenlemeler açısından da önemli bir kaynak oluşturmuştur[18]. Direktifin yürürlüğe girmesinden itibaren geçen zaman zarfında internetin günlük yaşamın bir parçası haline gelmesi, kişisel veri işleme süreçlerinin gelişmesi ve yeni teknolojilerin ortaya çıkardığı sorunlara karşı bireylerin farkındalığının artması gibi gelişmeler sonucunda Direktif de yetersiz hale gelmiş ve yerine, ihtiyaçlara cevap veren yeni bir düzenlemenin yapılması ihtiyacı hasıl olmuştur. Bu ihtiyaç doğrultusunda, 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ("GVKT"); 2016 yılında kabul edilmiş ve 25 Mayıs 2018 tarihinde yürürlüğe girmiştir[19]. Tüm üye devletler bakımından bağlayıcı olan GVKT ile, Direktif düzenlemeleri revize edilmiş, Direktif'teki düzenlemelere ek olarak birçok yeni hak ve yükümlülük belirlenmiş, bu yönüyle GVKT getirdiği yeniliklerle bağlayıcılığı bulunan Avrupa Birliği ("AB") sınırlarını da aşmıştır.

1.2.Kişisel Verilerin Korunması Hukukuna İlişkin Düzenlemeler

1.2.1.Genel olarak

Yukarıda tarihsel gelişimine yer verilen "kişisel verilerin korunması" kavramı, zaman içerisinde büyük gelişme göstermiş, alana ilişkin olarak ortaya konulan kazanımlar kimi zaman bağlayıcı kimi zaman ise tavsiye niteliği bulunan belgelerle koruma altına alınmak istenmiştir. Bu kapsamda, kişisel verilerin korunmasına ilişkin olarak farklı uluslararası kuruluşlar tarafından birçok uluslararası belge düzenlenmiş; bunların bir

[17] Duman, Berat. 2020, Anayasa Hukukunda Kişisel Verilerin Korunması, s.24
[18] Uygun, Murat. 2020, Avrupa Birliğinin 95/46 sayılı veri koruma yönergesi ışığında kişisel verilerin korunması.
[19] Küzeci, 2020: 221-222

kısmı değişen ihtiyaçlara cevap veremediği için yürürlükten kaldırılmış, bazılarının ise revize edilerek uygulanmasına devam edilmiştir[20].

Kişisel verilerin korunması hukuku kaynakları incelendiğinde, kavramın, farklı pek çok disiplin ile yakın ilişki içerisinde olması sebebiyle, konuya ilişkin genel düzenlemelerin yanı sıra farklı alanlarda kişisel verilerin korunmasına ilişkin özel niteliği bulunan birçok düzenlemenin de bulunduğu görülmektedir. Çalışmanın kapsamını aşmamak adına bu başlıkta, kişisel verilerin korunması hukuku bakımından genel niteliği olan temel düzenlemelere yer verilecek olup; belirli bir konuya ilişkin olarak kişisel verilerin işlenmesini konu edinen özel nitelikli belgelere yeri geldikçe değinilecektir.

1.2.2.Uluslararası düzenlemeler

1.2.2.1.İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme

4 Kasım 1950 tarihinde AK tarafından kabul edilen ve Roma'da imzalanan, Avrupa İnsan Hakları Sözleşmesi olarak da bilinen "İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme", insan haklarının korunması bağlamında yapılan temel düzenlemelerden biridir. Türkiye'de 18 Mayıs 1954 tarihinde onaylanarak yürürlüğe giren bu Sözleşme, henüz kişisel veri kavramının tam anlamıyla tanınmadığı bir dönemde imzaya açılması sebebiyle kişisel verilerin korunması hakkını, ayrı bir insan hakkı olarak düzenlememiştir. Bununla birlikte kişisel verilerin korunması kavramının ortaya çıkışı ile birlikte, özel hayatın ve aile hayatının korunması hakkını düzenleyen 8. madde kapsamında değerlendirilerek ele alınmıştır[21].

İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin "özel hayata ve aile hayatına saygı hakkı" başlıklı 8. maddesi incelendiğinde, düzenlemenin özel yaşam, aile yaşamı, ev ve haberleşmeler olmak üzere dört alana ilişkin koruma getirdiği anlaşılmaktadır. Buna karşın AİHS anlamında, kişisel verilerin korunmasının; özel alana riayet hakkının, şekillendirilmiş kısmi bir alanını

[20] Özel, Kadir Can. 2020, Ana Hatlarıyla Kişisel Verilerin Korunmasının Tarihsel Süreci ile Amacı ve Kişisel Verilerin Korunması Hakkı.

[21] İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme'nin 8. Maddesi:
Özel hayata ve aile hayatına saygı hakkı
1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin hukuka uygun ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

oluşturduğu ifade edilmekte ve bu nedenle AİHS m. 8 düzenlemesinin, kişisel verilerin işlenmesi konusundaki bireyin kapsamı belirleme hakkını da içerdiği kabul edilmektedir. AİHS'in yorumlanması ve uygulanması ile ilgili konularda yargılama yetkisine sahip olan Avrupa İnsan Hakları Mahkemesi ("AİHM"), söz konusu kavramların ne olduğu noktasında başvurulacak ana kaynak niteliğini taşımaktadır[22]. Bu sebeple kişisel verilerin korunması hakkının, bünyesinde yer aldığı değerlendirilen "özel hayat"tan ne anlaşılması gerektiği hususunda AİHM kararlarına da başvurmak gerekmektedir.

Özel hayat kavramı hakkında AİHM; kavramın genişliği sebebiyle kapsamlı bir tanıma elverişli olmadığı kanaatinde olup; özel hayatın, kişinin adı, fotoğrafı, fiziksel ve ahlaki bütünlüğü gibi kişisel kimliğine ilişkin yönlerini kapsadığı, bunun haricinde, kişinin hayatını özel bir şekilde yaşama hakkını içerdiğini kabul etmektedir. Bu anlamda özel hayat kavramının, AİHS m. 8 bağlamında açıkça düzenlenmeyen hakları da kapsayacak şekilde geniş yorumlandığı anlaşılmaktadır.

AİHM, konunun genişliğini ve özel hayat kapsamında yer aldığı değerlendirilen konuların çokluğunu göz önünde bulundurarak özel hayata ilişkin davaları, üç ana başlık altında ele almaktadır. Bu başlıklar; kişinin, fiziksel, psikolojik ve ahlaki bütünlüğü; özel hayatı; kimliği ve özerkliği başlıkları olarak karşımıza çıkmaktadır. Bu bağlamda AİHM; kişinin ismi, fotoğrafı, ev adresi, aile bağları, sağlığı, DNA profili gibi kişisel verilerinin işlenmesinin yanı sıra kişisel verilerin resmi makamlarca toplanarak arşivlenmesi, toplanan verilerin elde edilme amacı dışında kullanılması, çalışanların bilgisayar kullanımının izlenmesi, verinin gerekenden uzun süre saklanması gibi hususları da özel hayat kapsamında değerlendirmektedir. Diğer taraftan AİHM, söz konusu kavramları mutlak surette özel hayat kapsamında değerlendirmemekte, 8. maddenin ikinci fıkrasında yer verilen haller bakımından müdahale edilebilirliği de inceleme konusu etmektedir. Bununla birlikte mezkûr düzenleme, müdahalenin ancak "kanun ile" öngörülmüş olması halinde gerçekleşebileceğine cevaz vermektedir.

AİHM; hakka müdahale edilmesinin sınırlarını çizen "kanunla öngörülme" koşulunu, düzenlemenin belirli olmasının yanı sıra bu hukuksal temelin ulaşılabilir ve öngörülebilir olması, aynı zamanda iç hukukta dava yollarının bulunması ve gerekli

[22] Aksar, Yusuf. 2013, Teoride ve uygulamada uluslararası hukuk- II, s.331.

güvencelerin sağlanması gerektiği şeklinde yorumlamaktadır. Bu kapsamda olası suistimallere karşı müdahalenin usulü ve koşullarının saptanması, kişisel verilere erişim şekline ve amacına ilişkin ayrıntılı kuralların ve asgari güvencelerin belirlenmiş olması; verilerin saklanması, kullanılması, aktarımı ve imhası gibi işlemlere ilişkin olarak düzenlenmiş kuralların bulunması beklenmektedir[23].

Avrupa İnsan Hakları Mahkemesi'nin yerleşik içtihatları uyarınca, "demokratik bir toplumda gereklilik testi"; ilgili müdahalenin acil sosyal ihtiyaca karşılık gelip gelmediği, izlenilen meşru amaçla orantılı olup olmadığı ve ulusal makamlar tarafından bunu haklı kılmak için verilen gerekçelerin ilgili ve yeterli olup olmadığı hususlarının değerlendirilmesine ilişkindir.

Avrupa İnsan Hakları Mahkemesi bakımından "gereklilik" unsuru ise; zorlayıcı toplumsal gereksinim ve müdahalenin yöneldiği amaç ile orantılılık olarak yorumlanmakta, üye devletlerin bu noktada sınırsız olmayan bir takdir yetkisi bulunduğu kabul edilmektedir. Bu durumda ise müdahalenin ciddiliği, müdahaleye sebep olan meşru amacın önemi, ilgili hak ve özgürlüğün niteliği gibi unsurlar dikkate alınmaktadır[24].

Kanaatimizce AİHS'in kişisel verilerin korunması hakkını ayrıca düzenlememesine karşın, özel hayat kapsamında ele alması önemli bir yaklaşımdır. Bununla birlikte AİHM'in yargı yetkisinin ancak devletler nezdinde gerçekleşen ihlalleri konu alması sebebiyle ilgili kişiler bakımından gerçekleştirilecek tüm ihlaller doğrudan AİHS kapsamında değerlendirme konusu edilememektedir. Bununla birlikte AİHS hükümleri; taraf devletlere hakka dokunmama yükümlülüğü getirmenin yanı sıra, m. 8'in uygulama alanına ilişkin olarak harekete geçme ve gerekli tedbirleri alma yükümlülüğü de yüklediğinden, söz konusu tedbirlerin alınmaması halinde AİHM, ilgili devleti sorumlu tutacak; bu vesile ile belli ölçüde özel kişilere karşı gerçekleştirilmesi muhtemel ihlallere karşı da koruma sağlanacaktır.

1.2.2.2. Özel Hayatın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler

OECD, İkinci Dünya Savaşı sonrasında Batı Avrupa ekonomilerinin desteklenmesi ve onarımı amacıyla, Marshall Planı çerçevesinde yapılan yardımların dağıtımına

[23] Küzeci, 2020: 162.
[24] Küzeci, 2020: 163-164.

yardımcı olma ve Avrupa ülkeleri arasındaki ticari ödemeleri serbestleştirerek geliştirme amaçlarıyla, 1947-1960 yılları arasında faaliyette bulunan Avrupa Ekonomi İşbirliği Örgütü'nün işlevini tamamlaması üzerine, onun yerine ve daha geniş bir görev tanımı çerçevesinde 1961 yılında kurulmuştur. Ekonomik büyüme, mali istikrar, ticaret ve yatırım, teknoloji ve kalkınma gibi alanlarda işbirliği yoluyla refahın sağlanması, yoksullukla mücadelede hükümetlere yardımcı olma, iş imkânı yaratma, yeni gelişme ve sorunları anlayarak bunlara çözüm üretme konularında hükümetlere tavsiyelerde bulunma gibi temel hedefleri bulunan Örgüt, kişisel verilerin korunması alanında öncü bir yaklaşım sergileyerek uluslararası alanda kişisel verilerin korunması hususuna doğrudan doğruya yer verilen ilk düzenlemeyi ortaya koymuştur.

Bu anlamda 23 Eylül 1980 tarihli "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler", kişisel verilerin korunmasını hedef alan ilk düzenleme olarak karşımıza çıkmaktadır. OECD bünyesinde kabul edilen bu sekiz ilke ile kişisel verilerin korunması noktasında asgari standartlar tespit edilmiştir. Bu ilkeler; "veri toplamanın sınırlı olması ilkesi", "verilerin belirli bir niteliği karşılaması (veri kalitesi) ilkesi", "amacın belirliliği ilkesi", "kullanımın sınırlı olması ilkesi", "veri güvenliği ilkesi", "açıklık ilkesi", "bireyin katılımı ilkesi" ve "hesap verilebilirlik ilkesi" olarak öngörülmüştür. Söz konusu ilkeler, tavsiye niteliğinde olup, bağlayıcı nitelik göstermemekle birlikte, üye ülkeler açısından gerekli politikaların belirlenmesi ve düzenlemelerin yapılması adına yol gösterici bir gelişme olarak kritik bir öneme sahip olmuştur. Düzenlemenin bir diğer önemi ise ilkelerin belirlenmesinde çeşitli kıtalardan temsilcilerin katkısının bulunması ve bu anlamda kişisel verilerin, ilgili kişi tarafından denetiminin nasıl yapılacağı, kullanım şekillerinin nasıl saptanacağı gibi konularda geniş kapsamlı bir uzlaşıyı yansıtması olarak görülmektedir[25].

1.2.2.3. Birleşmiş Milletler Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler

Birleşmiş Milletler ("BM"), İkinci Dünya Savaşı'nın insanlığa yaşattığı acı tecrübelerin ardından, yaşanan savaşların ve barışa yönelik tehditlerin tekrarını önlemek ve uluslararası barış ve güvenliğin korunması amaçlarıyla kurulmuş bir uluslararası örgüttür. BM'nin temel amaçlarının da yer aldığı, örgütün kurucu metni

[25] Küzeci, 2020: 131.

olan BM Şartı, 26 Haziran 1945 tarihinde imzalanmış ve 24 Ekim 1945'te yürürlüğe girmiştir.

Birleşmiş Milletler Şartı'nın birinci maddesinde "ekonomik, sosyal, kültürel veya insani nitelikteki uluslararası sorunların çözümünde; ırk, cinsiyet, dil veya din ayrımı yapılmaksızın herkes için insan haklarına ve temel özgürlüklere saygının teşvik edilmesinde uluslararası işbirliği sağlamak", açıkça Şart'ın amaç ve ilkeleri arasında düzenlenmiştir. Bu amaca uygun olarak BM; insan haklarının korunmasına ilişkin olarak İHEB ve MSHS'yi kabul etmiştir. Gerek İHEB gerek MSHS; kişisel verilerin işlenmesine ilişkin olarak doğrudan özel bir düzenlemeye yer vermemekle birlikte düzenlemeler, "hiç kimsenin özel yaşamına, ailesine, evine ya da iletişimine keyfi olarak karışılamayacağı" ve bu gibi durumlarda "herkesin müdahale ya da saldırılara karşı yasa tarafından korunma hakkı" olduğunun belirtilmesi açısından önem taşımaktadır. Diğer taraftan, kişisel verilerin korunması hakkının, MSHS'de yer alan özel hayatın gizliliği kapsamında görüldüğünün BM İnsan Hakları Komitesi tarafından kabul edilmiş olması, kişisel verilerin korunmasına ilişkin olarak düzenlemenin ayrı bir öneme sahip olduğunu vurgulamaktadır[26].

Bununla birlikte BM nezdinde kişisel verilerin doğrudan ele alındığı ilk düzenleme, "Birleşmiş Milletler Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeler" ("BM Rehber İlkeleri") olmuştur. Kişisel verilerin korunmasına ilişkin standartları belirlemeyi amaçlayan ve 14 Aralık 1990 tarihinde kabul edilen düzenleme, üye ülkeler açısından bağlayıcı nitelikte olmayıp, yalnızca bilgisayarla işlenen kişisel veri dosyalarına yönelik olarak kabul edilmiştir. Söz konusu ilkeler; işleme faaliyetleri bakımından hukuka uygunluk ve adillik, doğruluk, işleme amacının meşru olması ve sınırlılığı, ilgili kişinin verilerine erişimi, özel niteliği bulunan veriler bakımından ayrımcılık yapmama, olası tehditlere karşı uygun önlemleri alma, karşılıklı ve uygun güvencelerin sağlanması halinde verilerin sınır ötesi akışı ilkeleri olarak belirtilmiştir. BM Rehber İlkelerini, kişisel verilerin korunmasına ilişkin birçok uluslararası düzenlemeden ayıran, söz konusu ilkelerin uygulanmasına ilişkin olarak bir denetim mekanizması öngörülmesinden ileri gelmekte olup; "denetim ve yaptırımlar" başlıklı 8. maddede, ilkelere uyulmasının denetlenmesini teminen her ülkenin kendi yasalarına uygun şekilde bir bağımsız ve tarafsız bir organ kuracağı belirtilmiştir. Bu yönüyle bir ilk olma özelliği taşıyan BM Rehber İlkeleri; uygulama

[26] Küzeci, 2020: 135.

alanı bakımından kural olarak kamu sektöründe ve özel sektörde gerçekleşen kişisel veri işleme faaliyetlerini esas almıştır[27].

1.2.2.4. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Kişisel verilerin korunması hakkının ortaya çıkması ve gelişmesinde etkin rol oynayan elektronik ortamlarda veri işleme alanındaki hızlı ilerleme neticesinde ve kişisel verilerin elektronik ortamlarda depolanması yönünde ortaya çıkan eğilimin de etkisi ile AK, kişisel verilerin adil olmayan bir şekilde toplanması ve işlenmesini önlemek amacıyla belirli ilkeler ve normların öngörülmesi ile bir çerçeve oluşturulması gerektiğine kanaat getirmiştir. Bu kapsamda Bakanlar Komitesi, özel sektör ve kamu sektörlerindeki otomatik veri bankalarında kişisel verilerin korunmasına yönelik olarak belirlenen ilkeleri içeren "Özel Sektörde Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına ilişkin Karar" ile "Kamu Sektöründe Elektronik Veri Bankaları Karşısında Bireylerin Özel Yaşamlarının Korunmasına ilişkin Karar"ı kabul etmiştir[28]. Bu düzenlemeler ile ulusal mevzuatın geliştirilmesinin harekete geçirilmesi amaçlanmakla birlikte, ilgili süreçte kişisel verilerin kapsamlı bir şekilde korunabilmesi için uluslararası ve bağlayıcı metinlerin daha etkili olacağı fark edilmiştir. Gerçekleştirilen müzakere süreçlerini takiben 108 sayılı Sözleşme 28 Ocak 1981 tarihinde imzaya açılmış, aynı tarihte Sözleşme'yi imzalayan Türkiye, ilk imzacı devletler arasında yerini almıştır. Bununla birlikte 108 sayılı Sözleşme'nin yürürlüğe girişi hemen mümkün olmamış, Sözleşme'nin 22. maddesinde yer alan düzenleme uyarınca Sözleşme 1 Ekim 1985 tarihinde yürürlüğe girmiştir[29].

Sözleşme, kişisel verilerin korunması alanında uluslararası düzeyde bağlayıcılığı bulunan ilk düzenleme olması bakımından büyük öneme sahiptir. Sözleşme'nin diğer bir önemi ise hem kamu sektörünün hem özel sektörün hedeflenmesi ile Konsey üye ülkeleri dışında Sözleşme'ye taraf olmak isteyen devletlere de taraf olabilme imkanının sağlanması sayesinde geniş bir uygulama alanı oluşturulmasıdır. Bunun yanı sıra, kişisel verilerin korunmasına ilişkin olarak da uygulanan AİHS m. 8 düzenlemesinin yeterli güvence sağlayıp sağlayamayacağı hususunun, 108 sayılı Sözleşme'nin yürürlüğe girdiği dönemde henüz netleştirilmemiş olması sebebiyle, 108

[27] Yüzbaşı Topaz, 2021: 141.
[28] Atak Songül. 2010, Avrupa Konseyi'nin kişisel veriler açısından sağladığı temel güvenceler, s.91-92.
[29] Göçmen Uyarer, Sinem. 2020, Kişisel Verilerin Korunması, s.97.

sayılı Sözleşme ile AİHS'in uygulanmasında oluşan boşlukların doldurulabilmesi hedeflendiğinden AİHS ve 108 sayılı Sözleşme arasında tamamlayıcı bir ilişki olduğunu söylemek de mümkün olacaktır[30].

Sözleşmenin temel amacı; Sözleşme'ye taraf her ülkede, uyruğu ne olursa olsun her bir gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır[31]. Bu düzenlemeden, sağlanan güvencenin yalnızca otomatik yollarla işlenen kişisel verileri kapsadığı anlaşılmaktadır. Bununla birlikte Sözleşme'nin 2. maddesinin (c) bendinde[32], kısmen otomatik yollarla işlenen kişisel verilerin de Sözleşme kapsamına dâhil olduğu açıkça belirtilmiştir.

Sözleşme'nin koruma sahası, kural olarak gerçek kişilere ilişkindir. Bununla birlikte Sözleşme'nin 3. maddesinin ikinci fıkrasının (b) bendinde, taraf devletlere bir yetki tanınarak, Sözleşme hükümlerinin; topluluklar, dernekler, vakıflar, şirketler, kurumlar ve tüzel kişiliğe sahip olup olmadığına bakılmaksızın gerçek kişilerin bir araya gelmesi ile oluşmuş her türlü kuruluş hakkında uygulanabileceği hüküm altına alınmıştır.

Sözleşme kapsamında, gerçek kişilerin ya da taraf devletin yetkisi dâhilinde belirtilen kuruluşların korunmasına ilişkin olarak; Sözleşme'nin 6. maddesinde özel veri kategorileri bakımından kişisel verilerin korunması[33], 7. maddesinde veri güvenliği[34] ve 8. maddesinde[35] ilgili kişiler hakkında ek güvencelere yer verilmiştir.

Diğer taraftan AK Danışma Komitesi, 108 sayılı Sözleşme'ye yapmış olduğu ek bir Protokol olan 181 sayılı "Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol" ile yukarıda açıklanan ilke ve esasların uygulanmasına ilişkin olarak taraf

---

[30] Küzeci, 2020: 145.

[31] Kişisel Verileri Koruma Kurumu. 2019, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s.17.

[32] 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi tutulması Karşısında Bireylerin Korunması Sözleşmesi, Madde 2/c: *"Otomatik işlem"den tamamen veya kısmen otomatik yöntemlerle gerçekleştirilen; verilerin kaydı, bu verilere mantıksal ve/veya aritmetik işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya dağıtılması anlaşılır."*.

[33] 6. maddede; ırk, siyasi düşünce, din veya diğer inançları ortaya koyan kişisel veriler ile sağlık, cinsel hayat veya ceza mahkûmiyetiyle ilgili kişisel verilerin, iç hukukta uygun güvenceler sağlanmadıkça otomatik işleme tabi tutulmayacağı düzenleme altına alınmıştır.

[34] 7. maddede ise otomatik veri dosyalarında depolanan kişisel verilerin korunabilmesi için verilerin kazaen ya da izinsiz olarak imha edilmesi ya da kazaen kaybolmasına yahut izinsiz elde edilmesi, değiştirilmesi ya da aktarılmasına karşı uygun güvenlik önlemlerinin alınacağı hükme bağlanmıştır.

[35] 8. maddede ise herkesin; verilerine ilişkin hususlarda bilgi edinme, gerekli olan durumlarda kişisel verilerinin düzeltilmesini veya koşulları varsa silinmesini talep etme hakkı olduğu ve bu haklara ilişkin olarak gerçekleşen taleplerin yerine getirilmemesi halinde bir başvuru yolundan yararlanma hakkına sahip olacağı hüküm altına alınmıştır.

devletlere bağımsız bir denetleyici makam oluşturma yükümlülüğü yüklemiş, ayrıca Protokol ile kişisel verilerin yeterli düzeyde koruma sağlamayan ülkelere ve uluslararası örgütlere transfer edilmesi yasaklanmıştır.

108 Sayılı Sözleşme'nin, ilkesel hareket ederek olabildiğince uzun süre uygulanması mümkün olsa da, teknolojideki hızlı ilerleme ve bu durumun insan hayatı üzerindeki etkileri ileri vadede öngörülemediğinden yenilenmesine ihtiyaç duyulmuştur[36]. Bu yenilenme süreci, 18 Mayıs 2018 tarihinde "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşmeyi Değiştiren 223 sayılı Protokol'ün ("108+") AK Bakanlar Komitesi tarafından kabul edilmesi ile sonuçlanmıştır. 108+ genel olarak incelendiğinde, 108 sayılı Sözleşme'nin temel prensiplere odaklı ve genel karakterinin korunduğu; 108 sayılı Sözleşme'den farklı olarak, mevcut koruma standartlarının yükseltildiği ve Sözleşme'nin kapsamının genişletildiği, bu sayede AB mevzuatı ile paralelliğin sağlandığı göze çarpmaktadır[37]. Bu kapsamda 108 sayılı Sözleşme'de yer verilmeyen "veri işleyen" ve "alıcı" kavramları tanımlanmış, ilgili kişilerin haklarına ilişkin özel nitelikli veri kategorileri arasına etnik köken, sendika üyeliği, biyometrik ve genetik veriler eklenmiş, uluslararası kuruluşların taraf olmasına imkân sağlanmış, ilkeler arasında şeffaflığa açıkça yer verilmiş ve 8. maddede şeffaflığa ilişkin olarak özel bir düzenleme getirilmiş, ilgili kişilerin sahip olduğu haklar genişletilerek, veri ihlali halinde ihlalin, gecikmeksizin denetim makamına bildirilmesi gerekliliği öngörülmüştür.

1.2.2.5. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

Kişisel verilerin korunmasına ilişkin olarak AB nezdinde kabul edilen önemli bir düzenleme de 95/46 sayılı Direktif olarak karşımıza çıkmaktadır. Temelde kişisel verilerin korunması kavramının gelişim sürecinde farklı uluslararası kuruluşlar nezdinde kabul edilen metinlerin uyumlaştırılması ihtiyacı sonucu ortaya çıkan metin; diğer uluslararası düzenlemelere taraf olan devletlerin, iç hukuklarını sözleşme hükümleri ile uyumlu hale getirme yükümlülüğüne istinaden yapmış oldukları ulusal düzenlemelerinin farklılık arz etmesi neticesinde oluşan sorunların çözümüne ilişkin çabaların bir ürünüdür. Her üye ülkede yeknesak şekilde kişisel verilerin korunmasının

[36] Küzeci, 2020: 151.
[37] Akçalı Gür, Berna. 2019, Uluslararası hukuk ve AB hukuku boyutuyla kişisel verilerin yurt dışına aktarılması, s.856.

garanti altına alınmasını hedefleyen Direktif, 24 Ekim 1995'te kabul edilerek 13 Aralık 1995'te yürürlüğe girmiş; yürürlükte bulunduğu süre zarfında AB üye devletleri bakımından kişisel verilerin korunmasına ilişkin uygulanacak temel düzenleme olma özelliği göstermiştir.

Düzenlemenin amacı, Direktif'in 1. maddesinin ilk fıkrasında ifade edilmiştir[38]. İkinci fıkrada ise ilk fıkrada sağlanan koruma ile bağlantılı sebepler için üye devletlerin, üye ülkeler arasında kişisel verilerin serbest akışını sınırlayamayacağı ve yasaklayamayacağı belirtilmiştir. Bu bakımdan Direktif'te hem kişisel verilerin serbest akışının sağlanması hem de bireylerin temel haklarının korunması anlamında bir denge kurulması amaçlanmıştır[39].

Direktif, kural olarak tamamen ya da kısmen otomatik yollarla işlenen kişisel veriler ile otomatik yollarla işlenmemesine karşın bir dosyalama sisteminin parçası olarak ya da dosyalama sisteminin parçası olma amacı ile işlenen kişisel verileri kapsamına almıştır. Bununla veri işlemenin kamu güvenliği, savunma, devlet güvenliği hususlarına ilişkin olduğu durumlarda, devletin ceza hukukunu ilgilendiren faaliyetleri ile gerçek kişilerce tamamen kişisel olarak yürütülen işlemeler Direktif'ten istisna tutulmuştur. Direktifin uygulanmasında gerçek kişiler koruma altına alınmış olmakla birlikte, üye devletlerin tüzel kişileri de koruma sahası içine alabilmesi mümkün kılınmıştır. Buna karşın tüzel kişilere ilişkin verileri; piyasa düzenlemeleri, istatistik, telekomünikasyon gibi verilerin korumasına ilişkin düzenlemeler içerisine almak Birlik'in takdirine bırakılmıştır. Direktif bakımından gerçek kişiye ait bilginin, belirli ya da belirlenebilir olması ön koşul olarak gösterildiğinden anonim veriler de kapsam dışında tutulmuş; Direktifin 26 numaralı gerekçesinde de bu durum açıkça belirtilmiştir.

108 sayılı Sözleşme gibi hem özel sektör hem kamu sektörü bakımından uygulama alanı bulan Direktif, kişisel veri işleme faaliyetlerine ilişkin olarak genel ilkeler öngörmüştür. Bu ilkeler, verilerin adil ve hukuka uygun olarak, belirli, açık ve meşru amaçlar için işlenmesi ve veri toplamanın amacı ile ilgili ve bu amacı aşmayacak

[38] Direktif'in amacı birinci maddesinde kişisel verilerin işlenmesine ilişkin olarak kişisel mahremiyet hakkı başta olmak üzere gerçek kişilerin temel hak ve özgürlüklerinin korunması olarak değerlendirilmiştir. (*Object of the Directive / 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046).

[39] Anı, Nevzat Ali. 2018, Kişisel Verilerin İşlenmesi ve Açık Rıza, s.31

şekilde işlenmesi, doğru ve gerektiğinde güncel olma ile verinin toplanma amacı ya da daha sonrası için öngörülen işlenme amaçları bakımından gerekli olan süreden daha fazla saklanmaması olarak ifade edilmiştir. Diğer taraftan kişisel verilerin hangi şartlar dâhilinde işlenebileceği Direktifin 7 ve 8. maddelerinde ele alınmış; veri sorumluları bakımından ilgili kişilere bilgi verme yükümlülüğü öngörülmüş; ayrıca Direktif kapsamında ilgili kişilerin hangi haklara sahip olduğu da düzenlenmiştir. Bu kapsamda kişilere; verilerine erişebilme hakkı tanınmış ve erişim hakkı bağlamında işleme süreçlerine ilişkin bilgi alabilme, verinin eksik ya da yanlış olması halinde bunları düzeltilmesini talep edebilme veya bunun imkânsız olması ya da orantısız bir çabayı gerektirmesi halleri dışında kişisel veri üzerinde yapılan işlemler hakkında verilerin aktarıldığı üçüncü kişilere bilgilendirmede bulunma hakları sağlanmıştır. Yine kişisel verilerin işlenmesi faaliyetlerine ilişkin olarak (ulusal mevzuatın, aksine bir düzenleme öngördüğü haller dışında) kişinin özel durumuna ilişkin zorlayıcı yasal gerekçelere ve doğrudan pazarlama amaçları kapsamında verinin işlenmesine itiraz etme, kendisine ilişkin bazı kişisel yönleri değerlendirmek amacıyla yalnızca verilerin otomatik işlenmesine dayanan ve kişiyi önemli derecede etkileyen/veya ona ilişkin yasal etkilere sebep olan bir karara tabi olmama hakkı bulunduğu da hükme bağlanmıştır.

Direktife konu edilen bir diğer konu da Birlik içerisinde ya da Birlik dışındaki ülkelere veri aktarımlarıdır. Direktifin 25. maddesinde, Birlik içerisinde ulusal düzenlemelere halel getirilmeksizin veri aktarımının serbest olduğu, Birlik dışında kalan üçüncü ülkelere ise yeterli korumanın sağlanması halinde veri aktarımının gerçekleştirilebileceği hüküm altına alınmış; 26. maddede ise bu kuralın, hangi hallerde uygulanmayacağına ilişkin düzenlemelere yer verilmiştir.

Avrupa Birliği direktiflerinin, AB üyesi ülkelere doğrudan uygulanabilir niteliğinin bulunmaması sebebiyle, Direktifin öngörmüş olduğu düzenlemelerin üye devletlerin iç hukuklarına aktarılması gerekmiş ve bu durum, Direktifin amaçları arasında da gösterilen yeknesaklığın sağlanmasını zorlaştırmıştır[40]. Ülkemizin de aralarında bulunduğu pek çok ülkenin veri koruma yasasına kaynak teşkil eden Direktif, çağın gereksinimlerini istenen seviyede karşılayamaması sonucu GVKT'nin yürürlüğe girdiği tarih olan 25 Mayıs 2018 tarihinde yürürlükten kalkmıştır.

[40] Dülger, Murat Volkan. 2020, Kişisel verilerin korunması hukuku, s.96

1.2.2.6. Avrupa Parlamentosu ve Konseyi'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü

Yukarıda, Direktif'in üye devletler arasında yeknesak bir hukuki temel oluşturamaması ve çağın gereklerini karşılamadaki eksikliklerinin, bu aksaklıkların bertaraf edildiği yeni bir düzenlemenin ortaya çıkarılması düşüncesini ortaya çıkardığından söz edilmişti. Direktifin hayata geçirildiği 1995 yılından itibaren teknolojik gelişmelerin insan hayatında giderek artan rolü, getirdiği kolaylıkların yanı sıra kişisel veri işleme faaliyetleri ile insan hayatına daha fazla müdahale edilmesi bakımından mahremiyetin ihlaline ilişkin riskleri de artırmıştır. Direktifin kolaylaştırmış olduğu sınır ötesi veri aktarımlarının, yabancı ülke mahremiyet kurallarının uygulanması zorunluluğunu beraberinde getirmesi; AB vatandaşlarının mahremiyet haklarının olumsuz etkilenmesine ilişkin kaygılarını giderek yükseltmiştir[41].

Bu düşünceler doğrultusunda Direktifin yenilenmesine ilişkin ilk çalışmalar 2009 yılına kadar uzanmakta ise de, süreç, AK'nin GVKT kapsamında şekillenen bir reform paketini gündeme getirmesi ile hızlanmıştır. 2012 yılında hazırlanan GVKT, dört yıllık süre zarfında geçirdiği değişiklikler sonunda nihayetinde Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde kabul edilmiş ve 24 Mayıs 2016'da yürürlüğe girmiştir[42]. Düzenlemenin 99. maddesinde 25 Mayıs 2018 tarihi itibarıyla uygulanacağı hüküm altına alınan GVKT, hâlihazırda yürürlükte olup; AB üye ülkeleri bakımından bağlayıcı niteliğe sahiptir.

GVKT, gerçek kişilerin kişisel verilerinin işlenmesine ilişkin kurallar getirerek aynı zamanda verinin serbest dolaşımına ilişkin esasları da düzenlemektedir. Bu hususlara ek olarak gerçek kişilerin temel hak ve özgürlükleri -bu bağlamda kişisel verilerin korunması hakkı- koruma altına alınmaktadır. Diğer taraftan GVKT'nin 5. maddesinde, kişisel veri işleme faaliyetlerinde uyulması gereken ilkelere yer verilmiş olup, bu ilkeler temel olarak Direktif ile uyumlu şekilde ele alınmıştır. Bu kapsamda işleme faaliyetlerinde; hukuka uygunluk, adillik, şeffaflık, amaçla sınırlı olma, veri

[41] Akıncı, Ayşe Nur. 2019, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, s.74.
[42] Ayözger Öngün, Çiğdem. 2019, Kişisel Verilerin Korunması Hukuku- Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil, s.87.

minimizasyonu, doğruluk, saklama sürelerinin sınırlı olması, bütünlük ve gizlilik ile hesap verilebilirlik gibi ilkelere uyulması gerektiği hüküm altına alınmıştır[43].

Kişisel veri işleme faaliyetleri çerçevesinde detaylı düzenlemelerin yer aldığı GVKT, getirmiş olduğu birçok yenilik ile Direktif'ten ayrılmaktadır. Bu yeniliklerin başında, GVKT'nin, yer bakımından uygulama alanına ilişkin olarak açık bir düzenlemeye yer vermesi gelmektedir. GVKT'nin 3. maddesine göre bu Tüzük, üç durumda uygulama alanı bulmaktadır. Bunlardan ilki, işleme faaliyetinin AB sınırları içinde gerçekleşip gerçekleşmediğinden bağımsız olarak AB sınırları içerisindeki bir veri sorumlusu ya da veri işleyenin işletmesi faaliyetleri kapsamında bağlamında gerçekleştirilmesidir. İkincisi, ilgili kişilere mal ya da hizmet sunulması ya da AB sınırları içerisinde gerçekleştiği ölçüde davranışların izlenmesi durumunda AB içerisinde yer alan ilgili kişilerin kişisel verilerinin AB dışında kurulu olmayan bir veri sorumlusu ya da veri işleyen tarafından işlenmesidir. Üçüncüsü ise üye devlet hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde kurulmuş veri sorumlusu tarafından işleme faaliyeti gerçekleştirilmesidir. Anılan hallerde, düzenlemenin 2. maddesinde belirtilen durumların da gerçekleşmesi şartıyla GVKT hükümleri uygulama alanı bulmaktadır. Bunun haricinde veri işleyenlerin hukuka aykırı işlemeden ve veri ihlallerinden sorumlu tutulabilmesi, veri sorumlularına ispat vasıtalarını sunabilme imkânı tanınması, kişisel veri işleme faaliyetleri sırasında veri ihlali gerçekleşmesi halinde bildirim yükümlülüğü getirilmesi, kişisel verilerin işlenmesine ilişkin olarak veri koruma görevlilerinin atanması, zorunlu veri koruma etki değerlendirmesi uygulamalarının yanı sıra ilgili kişiler lehine unutulma hakkı, veri taşınabilirliği, tasarımda gizlilik ve varsayılan gizlilik uygulamaları gibi hakların tanınması, GVKT ile getirilen önemli yenilikler arasında yer almaktadır. Getirdiği yenilikler kadar uygulanacağı alanın genişliği de dikkate alındığında GVKT'nin AB sınırları dışında da büyük etki yarattığını söylemek uygun olacaktır.

1.2.3.Ulusal düzenlemeler

1.2.3.1.Genel olarak

Avrupa'da kişisel verilerin korunması alanında atılan adımlar, ülkemize oldukça geç yansımış ve kişisel verilerin korunmasına ilişkin düzenlemeler, uzun bir süre gerçek

[43] Develioğlu, Hüseyin Murat. 2017, Avrupa Birliği Genel Veri Koruma Tüzüğü.

anlamıyla mevzuatımıza dâhil edilememiştir. Her ne kadar kişisel verilerin korunması, ülkemizde köklü bir geçmişe sahip bulunmasa da; doğrudan kişisel verilerin korunmasını hedef almamakla birlikte yürürlükte bulunan bazı düzenlemeler, kişisel verilerin korunması amacına hizmet etmiş ve oluşan bu boşluk telafi edilmeye çalışılmıştır. Yine henüz kişisel verilerin korunmasına ilişkin ayrı bir düzenleme öngörülmeden evvel, aşağıda yer verilecek olan kimi düzenlemelerde, "kişisel veriler"den de açıkça söz edildiği görülmektedir.

Ülkemizde kişisel verilerin korunmasına yönelik olarak yapılan düzenlemelerden ilki, 2004 yılında çıkarılan "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" olup; mezkûr Yönetmelik, belirli bir alana özgülenmiş olmasına karşın ülkemizde kişisel verilerin korunmasının da bir hak alanı olarak görülmesine yönelik ilk adımı ifade etmesi anlamında önemlidir. Bu düzenlemeyi, kişisel verilere yönelmiş bazı eylemlerin suç olarak düzenlendiği Türk Ceza Kanunu ("TCK") takip etmiştir. 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı TCK; 135, 136 ve 139[44]. maddelerinde açıkça "kişisel veri" ifadesini kullanmış ve bu veriler üzerinde gerçekleştirilen bazı faaliyetler belli şartlar dâhilinde suç kabul edilerek yaptırıma bağlamıştır.

Türk Ceza Kanunu'nda yapılan düzenlemeden beş yıl sonra, 2010 yılında yapılan Anayasa değişikliği, kişisel verilerin korunmasında bir dönüm noktası olmuş; "özel hayatın gizliliği" başlıklı 20. maddeye getirilen ek fıkra ile kişisel verilerin korunması, bireyin özel hayatına dâhil bir temel hak olarak değerlendirilmiştir. Maddenin son cümlesinde yer alan ifade uyarınca, kişisel verilerin korunmasına ilişkin esas ve usullerin düzenlenmesi kanuna bırakılmış ve bu sayede, yalnızca kişisel verilerin korunmasına özgülenmiş bir kanunun çıkarılması zorunlu hale gelmiştir. Bu

[44] 5237 sayılı Türk Ceza Kanunu;
Madde 135: *Kişisel verilerin kaydedilmesi*
(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.
(2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.
Madde 136*: Verileri hukuka aykırı olarak verme veya ele geçirme*
(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.
(2) (Ek:17/10/2019-7188/17 md.) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.
Madde 139*: Şikayet*
(1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.

doğrultuda yapılan KVKK, 07.04.2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş olup; bu Kanun, ülkemizde kişisel verilerin korunmasına özgülenmiş genel nitelikte ilk düzenleme olması ve kişisel verilerin korunmasında, idari yaptırım mekanizması öngörmesi bakımından büyük önem taşımaktadır.

1.2.3.2.Türkiye Cumhuriyeti Anayasası

Kişisel verilerin korunması, Anayasa'nın pek çok düzenlemesi ile yakından ilgilidir. Konut dokunulmazlığı, haberleşme hürriyeti, din ve vicdan hürriyeti, düşünce ve ifade hürriyeti gibi temel hak ve özgürlükler; koruma sahaları itibarıyla belli ölçüde kişisel verilerin korunması amacına da hizmet etmektedir. Bununla birlikte Anayasa'nın, özü itibarıyla, kişisel verilerin korunması hakkına hizmet eden üç temel düzenlemesi bulunmaktadır. Bunlardan ilki, "Başlangıç" kısmında ifadesini bulan "onurlu bir yaşam sürdürme hakkı"dır. İkincisi, kişinin dokunulmazlığı ile maddi ve manevi varlığını koruma altına alan 17. maddesidir. Üçüncüsü ise daha önce çeşitli vesilelerle değinmiş olduğumuz, 20. Madde ile düzenlenen "özel hayatın gizliliği hakkı"dır[45].

Sayılan üç düzenleme, insan onurunun korunması üzerine temellenmektedir. "İnsan"ı, diğer canlılardan ayırarak onu farklı kılan özellikleri arasında yer alan akli ve ahlaki yetiler; insana kişilik değeri kazandırmakta ve onu bağımsız kılmaktadır. Bu yönüyle, hakkında, üzerinde uzlaşılmış bir tanım verebilmek ya da hakka dair sınırları çizebilmek pek mümkün görünmese de insan onurunun, en yüksek akli ve ahlaki değerler ile dokunulmaz ve kaybedilmez bir öz değerin sahibi olarak insanın, kişiliğine ve özüne ilişkin değerleri ifade ettiği söylenebilir[46]. İnsan onuru, her insanın yalnızca insan olması sebebiyle sahip olduğu değerlerin, onu korunmaya değer kılması şeklinde vücut bulurken, bu durum insana, insan olduğu için tanındığı kabul edilen ve devletlere dokunmama ödevi yükleyen temel hak ve özgürlüklerin de temelini oluşturmaktadır. Her insanın, yalnızca insan olması sebebiyle değerli olduğunun kabul edilmesi; insan hakkı düşüncesinin ve buna bağlı olarak insan haklarının da temelini oluşturduğundan, insan hakkı denildiğinde aynı zamanda insan onuru da kastedilmiş olmaktadır[47].

[45] Arslan Öncü, 2019.
[46] Bulut, Nihat. 2008, Eski Yunan'dan Aydınlanma Çağına İnsan Onuru Kavramının Gelişimine Genel Bir Bakış, s.1-2.
[47] Özdem, Berk Hasan. 2019, Alman Anayasacılığında İnsan Onuru Kavramı, s.242-243

İnsan haklarının temelinde bulunan insan onuru kavramı, kişisel verilerin korunması hakkına da temel teşkil etmektedir. Gerek uluslararası gerek ulusal düzenlemelerde sık yer verilen insan onuru kavramı; Anayasa'nın Başlangıç kısmında,[48] kendine yer bulmuştur. Buna ek olarak devletin temel amaç ve görevlerinin düzenlendiği beşinci maddede, "insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak", devlete bir görev olarak yüklenmiştir. Anayasa'nın başlangıç bölümünde yer verilen ve "temel hak ve hürriyetlerden (...) yararlanarak onurlu bir hayat sürdürme ve maddi ve manevi varlığını bu yönde geliştirme" şeklinde kaleme alınan ifade; aynı zamanda insan onurunun, kişinin maddi ve manevi varlığının geliştirilmesi ile yakın ilişki içerisinde olduğunu ifade etmektedir. İnsanın kişiliğinin korunup geliştirilebilmesi ile maddi ve manevi varlığını geliştirebilmesi bağlamında bir ölçüt olarak görülen insan onuru, bu rolü ile insanın maddi ve manevi varlığını geliştirmesini garanti eden bir misyona da sahip olmakta, "kişi varlığını" gerçekleştirmeyi ve güvence altına almayı amaçlanmaktadır[49].

İnsan onuru ile yakın ilişki içerisinde bulunan ve özü itibarıyla çerçeve bir temel hak olarak kabul edilen kişinin maddi ve manevi varlığını geliştirme hakkı, mevcut bir temel hakkın koruma alanına girmeyen genel davranış özgürlüğünün yanı sıra kişinin kendi yaşamını serbestçe belirleme ve genel eylem özgürlüğünü de bünyesinde barındırmaktadır. Özel yaşamını düzenleyebilmek ve istemediği algı ve müdahalelere tabi tutulmamak, insanın maddi ve manevi varlığı için gerekli olup[50]; maddi ve manevi varlığın korunması ve geliştirilebilmesi için önce kişinin kendisinin koruması ve geliştirmesinin desteklenmesi anlamına gelmekte ve bu durum ise kişiye kendi özel hayatında gerekli korumanın sağlanmasını gerektirmektedir[51]. Bu anlamda demokratik ve özgür bir toplumda yaşayan ve yaşamını kendi özgür iradesi ile tayin etme yeteneği bulunan bireyin, özel hayat alanına dâhil olan kişisel verilerinin de kaderini tayin edebilme hakkına sahip olması; aynı zamanda kişisel verilerin neden korunması gerektiği sorusuna da bir cevap niteliğindedir.

---

[48] Türkiye Cumhuriyeti Anayasası Başlangıç Hükümleri; *"Her Türk vatandaşının, Anayasada yer alan temel hak ve hürriyetlerden eşitlik ve sosyal adalet gereklerince yararlanarak milli kültür, medeniyet ve hukuk düzeni içinde* ***onurlu bir hayat sürdürme*** *ve maddi ve manevi varlığını bu yönde geliştirme hak ve yetkisine doğuştan sahip olduğu"* paragrafı ile.

[49] Dülger, 2018, İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması, s.107

[50] Aras, Ümit Yaşar. 2010, İnsan hakları temelinde özel hayat hakkının ulusal ve uluslararası alanda uygulamaları, s.1

[51] Gümüş, Ali Tarık. 2004, Türk Anayasasında Kişinin Maddi ve Manevi Varlığını Koruma ve Geliştirme Hakkı, s.97.

Kişisel verilerin korunması, özel hayatın gizliliği hakkının kendine has özelliklerini içinde barındıran bir kavram olarak görülmüş ve merkezi veri bankaları kurulmasından resmi makamlar tarafından kişi hakkında özel hayat alanına giren çeşitli bilgilerin toplanmasına varan pek çok uygulama, özel hayat çerçevesinde değerlendirilmiştir. KVKK'nın yürürlüğe girmesinden önce, Türk hukukunda kişisel verilerin korunmasını konu edinen genel nitelikli bir düzenleme bulunmadığından, yukarıda bir kısmına yer verilen uluslararası düzenlemelerde olduğu gibi ülkemizde de kişisel verilerin korunması, özel hayatın gizliliği kapsamında bir hak olarak yorumlanmaktaydı[52]. Anayasa'nın 20. maddesinde düzenlenen "özel hayatın gizliliği hakkı", 2010 yılında yapılan halkoylaması öncesinde; herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel ve aile hayatının gizliliğine dokunulamayacağının belirtildiği ilk fıkrayı müteakip hangi sebeplerle hakka sınırlama getirilebileceğinin belirtildiği ikinci fıkra ile sonlanmaktaydı. Bununla birlikte 2010 halkoylaması ile Anayasa'nın 20. maddesine eklenen üçüncü fıkrada[53] "kişisel verilerin korunmasını isteme hakkı" olarak ifade edilen hak, anayasal bir statüye kavuşturulmuştur[54]. Mezkûr düzenleme ile kişinin; kişisel verilerinin amaçları doğrultusunda kullanılıp kullanılmadığı hakkında bilgi edinme, kişisel verilerine erişme ve gerektiğinde kişisel verilerinin düzeltilmesini ya da silinmesini isteme hakları anayasal düzeyde koruma altına alınmıştır. Bunun yanı sıra kişisel verilerin hangi hallerde işlenebileceğine ilişkin olarak bir çerçeve çizilmiş ve kişisel verilerin, ancak ilgili kişinin açık rızasının bulunduğu durumda ya da kanunda öngörülen hallerde işlenebileceği hükme bağlanmıştır. Düzenlemenin son cümlesinde yer alan ve konuya dair esas ve usullerin kanunla düzenleneceği hususundaki ibare ile konu hakkında detaylı düzenlemelerin yer alacağı bir kanunun yapılacağı sinyalleri de verilmiştir. Anılan düzenleme, hakka temel ve ayrı bir hak alanı olarak yaklaşılması, hakkın daha detaylı düzenlemelere konu edilmesi ve ülkemizde bir veri koruma otoritesinin kurulmasına vesile olması anlamında yeni bir dönem başlatmıştır.

[52] Çelik, Yeşim. 2017, Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı, s.395.

[53] T.C. Anayasası Madde 20/3: *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığım öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*

[54] Yüksel Civelek, Dilek. 2011, Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi, s.140-141

1.2.3.3.5237 sayılı Türk Ceza Kanunu

Dijitalleşen dünya, insan hayatı üzerinde büyük değişimler yaratmış ve ortaya çıkan yeni teknolojiler hızla insan hayatına dâhil olmuştur. Değişim süreci ile verinin elde edilmesi, paylaşılması ve sair suretlerde işlenmesi faaliyetleri de oldukça kolaylaşmış; bu durum, daha fazla verinin işlenmesine yol açmış ve verinin işlenmesinde meydana gelebilecek ihlal risklerini de ciddi ölçüde artırmıştır. Bu gelişmeleri dikkate alan kanun koyucu, TCK'nin "Kişilere Karşı Suçlar" başlıklı ikinci kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde bazı fiilleri suç olarak düzenlemiş ve yaptırıma bağlamıştır[55].

Bununla birlikte, kanun maddelerinde açıkça zikredilen "kişisel veri" kavramından ne anlaşılması gerektiği noktasında bir tanım ya da açıklamaya yer verilmediği ve söz konusu hükümlerin yürürlüğe girdiği tarih itibarı ile KVKK henüz yürürlükte bulunmadığı için, suçun hangi hallerde gerçekleşeceği noktasında tereddütler ortaya çıkmıştır. TCK ile gerek gerçek gerek tüzel kişiler bakımından, ceza hukuku bağlamında yaptırım öngören bir düzenlemede, söz konusu hükümlerin uygulanması bakımından önemi bulunan "kişisel veri" kavramının tanımlanmamış olması, o dönem için önemli bir eksiklik olarak değerlendirilebilirse de KVKK'nin yürürlüğe girdiği tarih itibarıyla artık bu sorunun çözüme kavuştuğunu söylemek yanlış olmayacaktır.

1.2.3.4.4857 sayılı İş Kanunu

4857 sayılı İş Kanunu'nun 75. maddesinde, çalıştırılan her işçi için bir özlük dosyası tutulması gerektiği hüküm altına alınmaktadır. Hükme göre işverenler, çalıştırdıkları her işçi için bir özlük dosyası düzenlemek ve bu dosya içerisinde işçinin kimlik bilgilerinin yanı sıra İş Kanunu ve diğer kanunlar uyarınca işveren tarafından düzenlenme zorunluluğu öngörülen her türlü belge ve kayıtları saklamakla yükümlüdür. Bu yükümlülüğe ek olarak işverenler, işçi hakkında edindikleri bilgileri

[55] Bu fiiller; Kanun'un 135. maddesinde, "kişisel verilerin kaydedilmesi", 136. maddesinde, "verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi", 138. maddesinde, "verilerin yok edilmemesi" olarak gösterilmiştir. Kanun'un 137. maddesinde, 135 ve 136. maddelerde yer verilen suçların ağırlaştırıcı sebeplerine yer verilirken 139. maddede anılan suçların şikâyete bağlı olmadığı ve re'sen kovuşturulacağı hüküm altına alınmış; ayrıca TCK'nin 140. maddesinde bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik tedbiri uygulanacağı belirtilmiştir.

dürüstlük kuralları çerçevesinde, hukuka uygun şekilde kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlü kılınmıştır.

İşçi özlük dosyası, işveren tarafından çalıştırılan her işçi için ayrı düzenlemek koşuluyla iş ilişkisinin başlangıcı, devamı ve sona ermesine ilişkin gerek İş Kanununda gerek diğer kanunlarda öngörülen belge ve kayıtların yanı sıra kanunlara aykırı olmamak koşuluyla iş ilişkisinin gerekli kıldığı belgelerin de bulunduğu kişisel nitelikte bir dosya olarak tanımlanabilir[56]. İş Kanunu'nda özlük dosyasının içeriğinde ne olması gerektiğine sınırlayıcı şekilde yer verilmemekle birlikte, söz konusu tanımdan, işçiye ilişkin kişisel verileri de içeren kişiselleştirilmiş bir dosya olduğu açıkça anlaşılmaktadır. Bu anlamda kanun koyucunun, gerek işçi özlük dosyasının tutulması gerek işçi hakkında edinilen bilgilerin açıklanmaması bağlamında, işçiye ilişkin verilerin kullanımına bir sınır getirdiğini ve kişisel verilerin korunması amacına hizmet ettiğini söylemek mümkündür.

Bununla birlikte söz konusu hükme uygun hareket edilmemenin yaptırımının ne olduğuna ilişkin olarak özel bir düzenlemenin bulunmadığı, yalnızca İş Kanunu'nun 104. maddesinde özlük dosyası tutulmamasının idari para cezasını gerektirdiğinin belirtildiği dikkate alındığında konunun önemine binaen KVKK'de yer verilen hükümlerle yetinilmeyerek kapsamlı düzenlemelerin getirilmesi kanaatimizce uygun olacaktır. Benzer şekilde uygulamada sıkça rastlanan ve işçinin yazışmaları ile telefon görüşmelerinin işveren tarafından takip edilmesi ya da işyerindeki kamera kayıtlarının izlenmesi gibi konularda, elde edilen verilerin, hangi şartlar altında kullanılabileceği ve bunun sınırları, her ne kadar Anayasa Mahkemesi kararları ile çizilmeye çalışılsa da kanun koyucu tarafından getirilecek özel düzenlemeler ile belirlenmesi önem arz etmektedir[57].

1.2.3.5.5809 sayılı Elektronik Haberleşme Kanunu

Elektronik haberleşme, kişisel verilerin korunması ile pek çok açıdan bağlantılı bir konudur. Elektronik haberleşme sektöründe kişisel verilerin korunmasına ilişkin olarak yapılan ilk düzenleme 2004 yılında Telekomünikasyon Kurumu tarafından kabul edilen "Telekomünikasyon Sektöründe "Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" olup; Elektronik Haberleşme Kanunu

[56] Polat, Yeliz. 2011, 4857 sayılı İş Kanunu'na göre İşçi Özlük Dosyası, s.4.
[57] Uncular, Selen. 2014, İş İlişkisinde İşçinin Kişisel Verilerinin Korunması, s.112-114.

2008 yılında kabul edilmiştir. Anılan Kanun'un 6. maddesinde[58], Bilgi Teknolojileri ve İletişim Kurumuna ("BTK") bir yetki tanınarak bu kanun uyarınca verilen görevlere ilişkin yönetmelik, tebliğ ve diğer ikincil düzenlemelerin çıkarılması yetkisi BTK'ye verilmiş; ayrıca Kanun'un "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51. maddesinde, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasların belirlenmesi yetkisi, yine BTK'ye bırakılmıştır.

Danıştay İdari Dava Daireleri Kurulu, 5809 sayılı Kanunun 51. maddesini Anayasa'nın Cumhuriyetin niteliklerini düzenleyen 2., yasama yetkisini düzenleyen 7., temel hak ve özgürlüklerin sınırlanmasını düzenleyen 13. ve özel hayatın gizliliğini düzenleyen 20. maddelerine aykırı bularak, Anayasa Mahkemesi'ne ("AYM") söz konusu düzenlemenin iptali istemiyle başvurmuş; AYM vermiş olduğu kararda öncelikle "kişisel veri" kavramını tanımlayarak, "belirli veya kimliği belirlenebilir" olmak şartıyla, kişiye ilişkin bütün bilgileri kişisel veri olarak kabul etmiştir. Bu kapsamda kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler, AYM tarafından kişisel veri kapsamında değerlendirilmiştir. Esasa ilişkin yapılan değerlendirmede ise AYM, Anayasa'nın 20. maddesinin üçüncü fıkrasında belirtilen "kanunla düzenlenir" ifadesi sebebiyle, Anayasa'nın, kanun ile düzenlenmesini açıkça öngördüğü konularda yürütme organlarına düzenleyici işlem yapma yetkisi tanınamayacağı gerekçesiyle düzenlemenin, Anayasa'nın 20. maddesine aykırı olduğuna hükmederek iptaline karar vermiştir.

İptal üzerine yürürlüğe giren yeni 51. maddede ise bir sonraki bölümde ayrıntılı olarak incelenecek olan ve KVKK'nin 4. maddesinde ele alınan genel ilkelere yer verilmiş, elektronik haberleşme ve ilgili trafik verilerinin gizliliğinin esas olduğu belirtilerek mevzuat ve yargı kararlarının gerektirdiği haller dışında haberleşmeye taraf olanların tümünün rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi eylemleri yasaklanmıştır. Diğer taraftan kişisel verilerin, kanun kapsamında düzenleme altına alınan aktörler tarafından hangi hallerde ve hangi amaçlar doğrultusunda işlenebileceği ve bunun sınırları da belirlenerek düzenlemenin

[58] 5809 Sayılı Elektronik Haberleşme Kanunu
Kurumun görev ve yetkileri
MADDE 6 – (1) Kurumun görev ve yetkileri şunlardır:
….
y) Bu Kanunla verilen görevlere ilişkin yönetmelik, tebliğ ve diğer ikincil düzenlemeleri çıkarmak.

on ikinci fıkrasında mezkûr Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmecilerin sorumlu tutulduğu belirtilmiştir. Düzenlemenin onuncu fıkrasında ise soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ve bu veriler ile ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları ile abone ya da kullanıcıların rızalarını içeren kayıtlara ilişkin olarak saklama süreleri öngörülmüştür.

1.2.3.6.6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

Satıcılar bakımından hemen her yerden, kolay bir şekilde ulaşılma imkânı bulunan, çok daha fazla müşteriye ulaşarak daha fazla kazanç elde edebilecekleri, müşteriler bakımından ise çok sayıda satıcının yer aldığı, rekabetin artması ile daha uygun fiyata daha kaliteli ürün satın alabilmenin mümkün olduğu bir alan yaratan elektronik ticaret uygulamaları, buna ilişkin usul ve esasların düzenleme altına alınmasını da zorunlu kılmıştır. Bu amaçla yürürlüğe giren 6563 sayılı Kanun ("ETK"); ticari iletişimi, hizmet sağlayıcı ve aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçlarıyla yapılan sözleşmeler ile elektronik ticarete ilişkin bilgi verme yükümlülüklerini ve uygulanacak yaptırımları düzenleme altına almaktadır.

Elektronik ticaret uygulamaları kapsamında gerçekleşen kişisel veri işleme faaliyetlerine ilişkin olarak 6563 sayılı ETK'nin 10. maddesinde bir düzenleme öngörülmektedir. Buna göre hizmet sağlayıcı ve aracı hizmet sağlayıcılar, ETK çerçevesinde yapmış oldukları işlemler nedeniyle elde ettikleri kişisel verilerin saklanması ve güvenliğinden sorumlu tutulmakta ve bu aktörler tarafından kişisel verilerin, ilgili kişilerin onayı olmaksızın üçüncü kişilere iletilmesi ve başka amaçlarla kullanılması yasaklanmaktadır. Fakat önemine binaen ilgili hüküm KVKK ile elektronik ticaret mevzuatı arasındaki karışıklığı gidermek adına 2022 yılının Temmuz ayında yürürlükten kaldırılmıştır. Ayrıca 3. maddede hizmet sağlayıcılar, kendilerine ait tanıtıcı bilgileri sunmakla; sözleşme kapsamında temin edilen verilerin saklanıp saklanmayacağı ve bu verilere erişimin mümkün olup olmadığı hususları ile mümkün olması halinde erişim süresine ilişkin bilgileri vermekle ve gizlilik kuralları ile varsa alternatif uyuşmazlık çözüm yollarına ilişkin bilgilendirmeleri yapmakla yükümlü tutulmuştur.

Düzenlemede yer alan bir diğer husus da ticari elektronik ileti gönderiminin kural olarak ilgili kişinin onayına bağlanmasıdır. ETK'nin 6. maddesine[59] göre ticari elektronik iletiler, ancak alıcılarının önceden onayları alınmak suretiyle gönderilebilecek ve onayın alınmasında herhangi bir şekli şart aranmayacaktır. Bu onay KVKK ile getirilen açık rıza alma yükümlülüğünden farkı bir sistemi belirtmekte ve biri diğerinin yerini tutmamaktadır. Bununla birlikte kişinin kendisiyle iletişime geçilmesi amacıyla iletişim bilgilerini verdiği hallerde veya temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakım hususunda ileti gönderilmesine ilişkin olarak ayrıca onay verilmesi aranmamıştır. Yine esnaf ve tacirlere ileti gönderilmesi bakımından önceden onay şartı aranmadığı görülmektedir. Öte yandan bu kural, mutlak bir kural olma özelliği göstermemektedir. Nitekim ETK 8. maddesinde[60], alıcıların diledikleri zaman, gerekçe göstermeksizin ticari elektronik ileti almayı reddedebileceği, böylesi bir durumda talebi alan hizmet sağlayıcının üç iş günü içerisinde ticari elektronik ileti göndermeyi durduracağı düzenleme altına alınmıştır.

1.2.3.7.6698 sayılı Kişisel Verilerin Korunması Kanunu

İnsan haklarına saygılı, demokratik bir hukuk devleti olarak ülkemiz; AK, BM, OECD gibi uluslararası kuruluşlara üye statüsünde yer almış, AB ile ilişkilerini ise 1963'e kadar uzanan bir zaman zarfında sürdürmüştür[61]. Kişisel verilerin korunması alanında, anılan kuruluşların çalışmaları ile uyumlu bir yasal bir zeminin oluşturulabilmesi ise hemen gerçekleşememiş, bunun için 2016 yılını beklemek gerekmiştir. Bununla birlikte kişisel verilerin korunmasına ilişkin kanun çalışmalarının geçmişinin, çok daha eskiye dayandığı bilinmektedir.

---

[59] 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
Ticari elektronik ileti gönderme şartı
MADDE 6 – (1) Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz.
(2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir.

[60] 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
Alıcının ticari elektronik iletiyi reddetme hakkı
MADDE 8 – (1) Alıcılar diledikleri zaman, hiçbir gerekçe belirtmeksizin ticari elektronik iletileri almayı reddedebilir.
(2) Hizmet sağlayıcı ret bildiriminin, elektronik iletişim araçlarıyla kolay ve ücretsiz olarak iletilmesini sağlamakla ve gönderdiği iletide buna ilişkin gerekli bilgileri sunmakla yükümlüdür.
(3) Talebin ulaşmasını müteakip hizmet sağlayıcı üç iş günü içinde alıcıya elektronik ileti göndermeyi durdurur.

[61] Küzeci, 2020: 339.

Kişisel verilerin korunmasına ilişkin bir kanun yapma girişimlerinin, 1980'lerin sonlarına doğru başladığı görülmektedir. Bu kapsamda kurulan ilk komisyon, çalışmalarını tamamlayamamış, 2000 yılında oluşturulan ikinci komisyonun hazırlamış olduğu tasarı, Adalet Bakanlığı tarafından 2003 yılında açıklanmasına karşın yasalaşamamıştır. Söz konusu tasarı, 2008 ve 2014 yıllarında olmak üzere iki defa Türkiye Büyük Millet Meclisine ("TBMM") sevk edilmiş ancak her iki metin de hükümsüz kalarak yürürlüğe girememiştir. 2014 yılında sunulan metni temel alarak önemli değişiklikler getiren son tasarı ise 18 Ocak 2016'da TBMM'ye sevk edilmiş ve 24 Mart 2016 tarihinde kabul edilmiştir[62]. Söz konusu düzenleme, KVKK'nin yürürlüğe girdiği tarihte yürürlükte bulunan Direktif'i kaynak almaktadır.

[62] Küzeci, 2020: 347-348.

İKİNCİ BÖLÜM

KVKK KAPSAMINDA TEMEL KAVRAMLAR VE GENEL İLKELER, İŞLEME ŞARTLARI İLE İŞLEME FAALİYETİNİN HUKUKİ NİTELİĞİ

Gerek çevrimiçi davranışsal pazarlama uygulamalarında kullanılan kişisel verileri doğru yorumlayabilmek gerekse Türkiye'deki düzenlemelerin Avrupa düzenlemeleri ile karşılaştırılmasını yeterli şekilde yapabilmek adına öncelikle KVKK kapsamında temel kavramlar, genel ilkeler, işleme şartları ile işleme faaliyetlerinin hukuki niteliğini ayrıntılı olarak incelemenin uygun olacağı kanaatindeyiz. Bu kapsamda çalışmanın ikinci bölümü KVKK ile getirilen tanımlar ve düzenlemeleri açıklayıcı bir niteliğe sahiptir. Çevrimiçi davranışsal pazarlama uygulamaları söz konusu olduğunda özellikle kişisel verilerin korunması mevzuatı büyük önem arz etmektedir.

2.1.Kanunun Amaç ve Kapsamı

Gerek KVKK'de gerek Anayasa'nın 20. maddesinin üçüncü fıkrasında yer alan düzenlemede, "kişisel verilerin korunması" kavramı tercih edilmiş ise de KVKK, "veri"yi değil; Kanun'un 1. maddesinde de açıkça belirtildiği üzere "özel hayatın gizliliği başta olmak üzere kişilerin temel hak ve özgürlüklerini koruma"yı amaçlamaktadır. Bu anlamda KVKK'nin, kişisel verilerin korunmasını, temel hak ve özgürlüklerin kullanılmasına hizmet eden bir araç olarak gördüğü söylenebilecektir[63]. Bunun yanında KVKK, "kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenleme"yi de diğer bir amaç olarak benimsemiş; böylece işleme faaliyetlerinin belli bir disiplin altında yürütülmesi güvence altına alınmıştır.

Söz konusu amaçlar doğrultusunda Kanun'un kapsamı KVKK'nin ikinci maddesinde belirtilmiştir. Buna göre KVKK hükümleri, kişisel verileri işlenen gerçek kişiler ile kişisel verileri tamamen ya da kısmen otomatik olan yollarla ya da bir veri kayıt sisteminin parçası olmak suretiyle otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulama alanı bulacaktır. Söz konusu ifadeden, yalnızca gerçek kişilere ait verilerin KVKK kapsamında değerlendirilebileceği, tüzel kişi verilerinin ise Kanun'un kapsamı dışında bulunduğu anlaşılmaktadır. Bununla birlikte tüzel

[63] Çekin, Mesut Serdar. 2020, Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, s.23.

kişiye ait verilerin elde edilmesi ile bir ya da daha fazla gerçek kişinin kimliğinin belirlenmesinin söz konusu olduğu hallerde, gerçek kişiye ilişkin kişisel verilerin korunabilmesi amacıyla KVKK kapsamında bir korumanın sağlanabileceği kabul edilmektedir[64].

Diğer taraftan Kanun'un öngördüğü bu kapsamı somutlaştıran ve KVKK'nin uygulanıp uygulanmayacağı hususunu ortaya koyan esas unsurun, verinin işlenme yöntemi olduğu görülmektedir. Nitekim düzenleme, gerçek kişiye ait verinin işlendiği her durumu kapsamına almamakta; işleme faaliyetinin, kişisel verinin "tamamen ya da kısmen otomatik olarak gerçekleştiği" ve "veri kayıt sisteminin parçası olmak şartı ile otomatik olmayan yollarla işlendiği" haller ile sınırlamaktadır. Bununla birlikte kişisel verinin otomatik ya da otomatik olmayan yollarla işlenmesi ile neyin kast edildiği, Kanun metninde belirtilmemiştir. Konuya ilişkin olarak Kişisel Verileri Koruma Kurumu ("Kurum"), verinin otomatik ya da otomatik olmayan yollarla işlenmesi hususunda 108 sayılı Sözleşme düzenlemelerine atıf yapmaktadır. Anılan Sözleşme'nin 2. maddesinin (c) bendinde otomatik işleme; "verinin depolanması, bu verilere mantıksal ve/veya aritmetik işlemler uygulanması, değiştirilmesi, silinmesi, geri alınması veya dağıtılması işlemlerinin otomatik ya da kısmen otomatik yöntemlerle gerçekleştirilmesi" olarak ifade edilmiştir. Görüleceği üzere söz konusu tanımda kavram, yine kendisi ile tanımlandığından, otomatik işlemenin ne olduğunu anlamak güçleşmektedir. Bununla birlikte Kurum tarafından yayımlanan "100 soruda Kişisel Verilerin Korunması Kanunu" isimli rehberde, otomatik olarak veri işlenmesinin; bilgisayar, telefon, saat gibi işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyetlerini ifade ettiği belirtilmektedir[65]. Bunun anlamı ise kısmen de olsa bu veya benzer türde cihazlar tarafından gerçekleştirilmeyen işleme faaliyetlerinin, KVKK hükümlerine tabi olabilmesinin, yalnızca işlemenin bir veri kayıt sisteminin parçası olmak suretiyle gerçekleştirilmesi halinde mümkün olduğudur. KVKK'nin 3. maddesinin (h) bendinde "kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi" olarak tanımlanan veri kayıt sisteminin, ne şekilde düzenlenmesi gerektiğine ilişkin özel bir öngörü bulunmadığından veri kayıt sistemi,

[64] İmançlı, Canan. 2020, Kişisel sağlık verilerinin korun(a)mamasından doğan özel hukuk sorumluluğu, s.44.
[65] Çekin, 2020: 26-27.

veri sorumlusu tarafından belirlenecek kriter ya da kriterler doğrultusunda yapılacak bir sınıflamayı içeren, elektronik ya da fiziki ortamda tutulması mümkün olan bir kayıt türü olarak nitelendirilebilecek ve anılan şartlar dahilinde gerçekleşen kişisel veri işleme faaliyetleri de KVKK hükümlerine tabi olacaktır[66].

2.2.Kişisel Verilerin İşlenmesiyle İlgili Temel Kavramlar

2.2.1.Genel olarak

Kişisel Verilerin Korunması Kanunu, kişinin temel hak ve özgürlüklerinin korunmasını amaçlayan bir kanun olarak, veri sorumlusu ve veri işleyen gibi aktörlerle yakın bağlantı içinde olmasına karşın merkezine, korunacak asıl değerin sahibi olan "ilgili kişi"yi[67] almıştır. Tanımda yer verilen kişisel veri kavramının ne olduğu, amaç ve kapsam düzenlemelerinde yer alan "işleme"den ne anlaşılması gerektiği, verinin kimler tarafından işlenebileceği hususları da KVKK'yi doğru şekilde anlayabilmek için önem taşıdığından bu başlık altında KVKK kapsamında yer verilen kişisel veri, özel nitelikli kişisel veri, kişisel verilerin işlenmesi, veri sorumlusu ve veri işleyen kavramları ele alınacaktır.

2.2.2."Kişisel veri", "özel nitelikli kişisel veri" ve "kişisel verilerin işlenmesi" kavramları

Kişisel Verilerin Korunması Kanununda kişisel veri kavramı, 108 sayılı Sözleşme, Direktif ve GVKT başta olmak üzere birçok uluslararası düzenleme ile uyumlu şekilde ele alınmaktadır. KVKK uyarınca kişisel veri, "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"yi ifade etmekte olup; kavramın iki ana unsurunun bulunduğu anlaşılmaktadır. Bunlar; kimliği belirli ya da belirlenebilir bir kişiye aitlik ve var olan bilginin, gerçek kişiye ilişkin olmasıdır.

Kişisel veriyi oluşturan ilk unsur olan "kimliği belirli ya da belirlenebilir kişi"ye aitlik, öncelikle "kimliğin belirli ya da belirlenebilir olması" ile neyin ifade edildiğinin açıklanmasını gerektirmektedir. Kimliğin belirli olması, maddenin lafzından da anlaşılacağı üzere verinin, kime ait olduğunun açıkça belli olması durumunu ifade etmektedir. KVKK'nin gerekçesinde, kişinin belirli ya da belirlenebilir olması, "mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o

[66] Özkan, Oğulcan. 2020, Kişisel Verilerin Korunması, s.74.
[67] İlgili kişi kavramı, Kanun'un 3. maddesinin (ç) bendinde; "kişisel verisi işlenen gerçek kişi " olarak ifade edilmiştir. Bu tanımdan, bir üst başlıkta belirtilen istisna hariç olmak üzere, ilgili kişinin gerçek kişi olması gerektiği anlaşılmaktadır.

kişinin tanımlanabilir hale getirilmesi" olarak ifade edilmiş ve bilginin, kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içeriğe sahip olması ya da kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesine olanak tanıması hali bu kapsamda değerlendirilmiştir. Gerekçe metni ile madde hükmü birlikte değerlendirildiğinde; veri hakkında, kişisine aittir" denilebildiği, diğer bir deyişle, kişiyi doğrudan doğruya tanımlayabilme yetisi bulunan verilerin kimliği belirli kıldığını; doğrudan bu vasfa sahip olmamakla birlikte başka verilerle bir araya getirildiğinde kişiye işaret eden, yani dolaylı yoldan kişiyi belirli kılan verilerin ise kimliği belirlenebilir hale getirdiğini söylemek mümkündür[68]. Bu noktada önem arz eden bir husus da, belirlenebilir kılmaya ilişkin olarak herhangi bir sınır olup olmadığıdır. Konuya ilişkin olarak yasal düzeyde bir öngörü bulunmamakla birlikte; öğretide, işleme faaliyetini gerçekleştirecek olan veri sorumlusunun elinde bulunan ya da elde edebileceği ilgili kişiye ait farklı verilerin, kişiyi belirleyebilmesine ilişkin olarak kullanılmasında bir sakınca bulunmadığı, bununla birlikte verinin üçüncü kişilerden temin edileceği hallerde makul sınırlar çerçevesinde ve ölçülü olarak hareket edilmesi gerektiği kabul edilmektedir[69].

Diğer taraftan KVKK, ikinci bir unsur olarak belirli ya da belirlenebilir kişiye ait olan bilginin, gerçek kişiye ilişkin olmasını aramıştır[70]. Kişilik, Türk Medeni Hukuku çerçevesinde "sağ ve tam doğum" ile başlayan ve ölüm ya da kişinin hükmen ölümü anlamını taşıyan durumlar neticesinde kişi hakkında ölü kaydının düşülmesi ile sonuçlanan bir süreci ifade etmekte ve bu süreç içerisinde yer alan insanlar, "gerçek kişi" olarak kabul edilmektedir[71]. KVKK anlamında gerçek kişi kavramı da, yaşayan bir insana ait bilgileri ifade ettiğinden; ölmüş bir insana ait verilerin ve sağ ve tam doğumun gerçekleştiği ana kadar ceninin, KVKK kapsamında yer almadığı kabul edilmektedir.

Diğer taraftan bilginin gerçek kişiye ilişkin olması, "bilgi" kavramının değerlendirilmesini de gerektirmektedir. Kişisel verinin tanımında kendisine yer bulan bilgi, tanımdan da anlaşılacağı üzere veri kavramıyla yakın ilişki içerisindedir.

[68] Çekin, 2020: 45.
[69] Çekin, 2020: 46-49.
[70] Taştan, 2017: 32-33.
[71] Akipek, Jale; Akıntürk, Turgut; ve Ateş, Derya. 2015, Türk Medeni Hukuku- Başlangıç Hükümleri Kişiler Hukuku I. Cilt, s.241.

Günümüzde verinin, bilgi kavramı ile aynı anlama gelecek şekilde kullanılmasına rağmen verinin, bilgiden daha geniş bir kapsama sahip olduğu kabul edilmekte ve bilginin, alıcı için anlamlı olan bir formda işlenen verileri; verinin ise bilgi üretmek için işlenen ve rafine edilen hammaddeleri ifade ettiği belirtilmektedir. Bu açıdan bakıldığında "bilgi"nin kullanılması yönüyle KVKK'de daha dar bir kapsamın ifade edildiği anlaşılmaktadır. Verinin işlenerek bilgi haline dönüştüğü bir formda yer alması ve diğer şartların da sağlanması koşuluyla KVKK, hangi bilgilerin kişisel veri olduğu yönünde bir sınırlamaya gitmeyerek, geniş bir kapsamda koruma alanı sağlamaktadır. Bununla birlikte her türlü bilgi, KVKK'de yapılan tanım uyarınca Kanun kapsamında yer almamakta, bilginin, belirli ya da belirlenebilir bir gerçek kişiye ait olması beklenmektedir.

Bu bilgiler ışığında kişisel verilerin bir türü olan özel nitelikli kişisel veri kavramını açıklayabilmek daha kolay olacaktır. Özel nitelikli kişisel verilerin, kişisel verilerin bir türü olduğunun anlaşılmasına karşın, KVKK'de "özel nitelik" ile neyin kast edildiği açıklanmamıştır. Bununla birlikte özel nitelikli kişisel verilerin neler olduğu, KVKK'nin 6. maddesinin birinci fıkrasında sınırlı sayım yolu ile belirtilmektedir. Buna göre kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Söz konusu veriler ile kişisel veriler kıyaslandığında özel nitelikli kişisel verilerin, daha hassas niteliğe sahip olduğu görülmektedir. Özel nitelikli kişisel verileri, kişisel verilerden ayıran husus, açıkça belirtilmemekle birlikte "ayrımcılık tehlikesi" olarak ifade edebileceğimiz yüksek risk faktörüdür. İçerdiği yüksek risk faktörü dikkate alınarak, söz konusu verilere bazı toplumsal ve siyasi kaygılar sonucu kanun koyucu tarafından farklılık tanınmış; üçüncü kişiler tarafından öğrenilmesi halinde veri ile ilişkilendirilen kişinin mağdur olmasının önüne geçilmesi hedeflenmiştir[72]. KVKK'nin gerekçesinde de bu hususa vurgu yapılmış ve özel nitelikli olarak kabul edilen kişisel verilerin; başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olması hususu dikkate alınarak, bu türden verilerin özel nitelikli veri olarak kabul edildiği belirtilmiştir. Bu doğrultuda özel nitelikli kişisel verilerin işlenmesi, daha ağır şartlara bağlanmış; bu verilerin

[72] Dülger, 2020: 178.

işlenmesinde Kişisel Verileri Koruma Kurulu ("Kurul") tarafından belirlenen yeterli önlemlerin alınması şart tutulmuştur.

Kişisel Verilerin Korunması Kanunu bağlamında kişisel veri ve özel nitelikli kişisel veri kavramları hakkında yapılan açıklamaları müteakip, KVKK'nin uygulanmasını harekete geçiren eylem olarak "işlenme"ye de değinmek uygun olacaktır. KVKK'nin 3. maddesinin (e) bendi uyarınca kişisel verilerin işlenmesi, yukarıda açıklanan unsurlara sahip olan kişisel veri ve özel nitelikli kişisel verilerin Kanun'un 2. maddesinde belirtilen usullerle "elde edilmesi, kaydedilmesi depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem'i ifade etmektedir. Bu anlamda işleme faaliyeti; hükümde belirtilen haller ile sınırlanmamış, madde metninde belirtilenlerin dışında bir faaliyetin de işleme faaliyeti olarak kabul edilmesi mümkün kılınmıştır. Görüleceği üzere KVKK, kişisel verinin işlenmesi kavramını oldukça geniş ölçekte ele alarak, teknolojik gelişmelerin farklı işleme usullerini beraberinde getirmesi halinde dahi, Kanun'un uygulanmasına imkân sağlamıştır. Bu bakış açısı, Direktif ve GVKT ile de uyumludur. Nitekim her iki düzenlemede de kişisel verilerin işlenmesi anlamına gelebilecek fiiller örnek nev'inden sayılmakta, bu noktada kritik unsurun ise kişisel veriler üzerinde bir işlem gerçekleştirilmiş olması olduğu ifade edilmektedir.

2.2.3."Veri Sorumlusu" ve "Veri İşleyen" kavramları

Kişisel Verilerin Korunması Kanunu'nun kişi bakımından uygulanmasına ilişkin olarak karşımıza çıkan aktörlerden ilki veri sorumlusudur. İşleme faaliyetini yasal temele oturtan ana aktör olarak veri sorumlusu; hangi verilerin, hangi amaçlarla, hangi yöntemlerle kimlerden elde edileceğini, bunların üçüncü kişilerle paylaşılıp paylaşılmayacağım, paylaşılacaksa kimlerle paylaşılacağını belirleyen ve bu verilerin ne süre ile saklanacağına karar veren taraf olarak tanımlanabilir[73]. Kanun'un 3. maddesinde ise veri sorumlusu, "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi " şeklinde tanımlanmıştır.

[73] Taştan, 2017: 70.

Tanıma göre kişisel veri işleme faaliyetleri bakımından veri sorumlusunu karakterize eden iki ana unsurun varlığı göze çarpmaktadır. Bunlardan ilki, veri sorumlusunun faaliyet alanına ilişkindir. Kanun bu faaliyet alanını, "kişisel verilerin işlenme amaç ve vasıtalarını belirleme" ile "veri kayıt sisteminin kurulması ve yönetilmesinden sorumlu olma" olarak ifade etmektedir. Söz konusu tanımdan veri sorumlusunun, işleme faaliyetinin yol haritasını çıkaran ana aktör olduğu anlaşılmaktadır. Zira veri sorumlusunu karakterize eden "verinin işlenme amaç ve vasıtalarını belirleme" yetkisi, işleme faaliyetinin ana temasını belirlemekte olup; bu yetki, veri sorumlusu bakımından pek çok hususta belirleme yapabilme ve karar verebilme yetkisinin varlığına işaret etmektedir. Bu anlamda veri sorumlusunun yetkisi, öncelikli olarak hangi kişisel verilerin, hangi amaçlarla işleneceğinin tespit edilmesine ilişkindir. İşlenecek kişisel veri kategorisi belirlendikten sonra bu verilerin kimden ve hangi yöntemlerle elde edileceğinin de belirlenmesi gerekecektir. Kişisel verinin işlenme amacının belirlenip, verilerin kimden ve nasıl elde edileceği de tespit edildikten sonra bu veriler üzerinde belirlenen amaca ulaşabilmek adına ne tür bir faaliyetin gerçekleştirileceği, ne süre ile bu verilerin saklanacağının tespiti, saklama süresinin sona ermesi durumunda verinin imha edilmesi gibi, faaliyetin başlamasından sona ermesine dek gerçekleşen tüm aşamalar, veri sorumlusunun yetki alanı içinde yer almaktadır. Bununla birlikte veri sorumlusunun yetkilerinin sınırları, açık ve net şekilde ortaya konulmadığından, bir yetkinin, veri sorumlusuna ait bir yetki olup olmadığının, somut olay bağlamında ayrıca ele alınması gerekecektir.

Veri sorumlusunun görev ve yetki alanı içerisinde bulunan diğer bir konu da veri kayıt sisteminin kurulmasıdır. KVKK'nin 3. maddesinin (h) bendi uyarınca veri kayıt sistemi; "kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi" olarak tanımlanmıştır. Bir dosyalama sistemi olarak da nitelendirilebilecek veri kayıt sisteminin kurulmasına ilişkin olarak kanun koyucu özel bir usul öngörmediğinden, gerek fiziki ortamda gerek elektronik olarak oluşturulabilecek sistemlerin veri kayıt sistemi olarak değerlendirilmesi mümkündür. Böyle bir sistemin kurulması ve yönetilmesinden sorumlu olan gerçek ve tüzel kişiler, şayet kişisel verinin işlenme amaç ve vasıtalarının belirlenmesinde de aktif rol alıyorlarsa veri sorumlusu olarak nitelendirilebilecektir. Bu noktada, kişisel verilerin işlenme amaç ve vasıtalarının birden fazla kişi tarafından ortaklaşa belirlendiği ya da veri kayıt sisteminin kurulması ve yönetiminden ortaklaşa sorumluluğun söz konusu olduğu durumların da ortaya

çıkabileceğini değerlendirmek gerekmektedir. Bu hususta KVKK, özel bir öngörüde bulunmamış ve birden fazla veri sorumlusunun bulunması halini özel bir hükme bağlamamıştır. Öte yandan ilgili konu kapsamında Kişisel Verileri Koruma Kurulu tarafından 23.12.2021 tarihinde verilen 2021/1304 sayılı ilke kararı ile GVKT'nin 26. maddesine gönderme yapma vasıtasıyla "ortak veri sorumlusu" kavramından bahsedilmiş ve birden çok veri sorumlusunun aynı kişisel veriler üzerinde hakimiyeti bulunduğu hallerde birlikte sorumlu tutulacaklarına karar verilmiştir. Ortak veri sorumlularının bulunduğu durumlarda olası hukuki ve cezai yaptırımların tüm veri sorumlularına uygulanabileceğini de belirten kararın, KVKK kapsamında açıkça yer almayan bir düzenlemeye atıf yapıyor olması ve bu tanımın bir ilke kararı ile düzenlenmeye çalışılması oldukça fazla eleştiri almıştır.

Veri sorumlusunu karakterize eden ikinci unsur ise veri sorumlusunun kişiliğine ilişkindir. Yukarıda belirtilen veri sorumlusu tanımında da açıkça görüldüğü üzere veri sorumlusunun, ya bir gerçek kişi ya da bir tüzel kişi olması gerektiği belirtilmektedir. Bu bakımdan kanun koyucu, veri sorumlusunun hukuken sorumlu tutulabilmesini teminen "kişi" olması gerektiğini öngörmüştür. Bununla birlikte bu öngörü, uygulamada bazı sorunlara yol açabilecek niteliktedir. Örneğin; kişisel veri işleme amaç ve vasıtalarının belirlenmesi ya da veri kayıt sisteminin kurulmasından; adi ortaklıklarda olduğu gibi tüzel kişiliği bulunmayan bir kişi topluluğunun sorumlu olduğu hallerde ya da söz konusu faaliyetlerin devlet tüzel kişiliği üst çatısı altında teşkilatlanan ve ayrı bir tüzel kişiliğe sahip olmayan kurum ya da kuruluşlar tarafından gerçekleştirilmesi durumunda bunların "kişi" olarak kabul edilmesi mümkün olmadığından, veri sorumlusu sıfatının tespitinde sorunlar yaşanması muhtemeldir. Nitekim bu kimselerin veri sorumlusu olarak kabul edilmesi halinde kanunun lafzına aykırı hareket edilecek; veri sorumlusu olarak kabul edilmemesi durumunda ise KVKK uyarınca veri sorumlularına yüklenen görevlerin ifası ve ilgili kişilerin Kanun kapsamında yapacağı taleplere ilişkin olarak öngörülen düzenlemeler, sırf kişiliğin bulunmaması sebebiyle fiilen askıya alınmış olacaktır. Uygulamada Kurul, gerçek ya da tüzel kişi olma olgusundan ziyade kişisel verinin işlenme amaç ve vasıtalarını belirleme ve veri kayıt sisteminin kurulması konusundaki yetkinin kimde bulunduğuna ilişkin hususlara öncelik tanımaktadır. Bu anlamda Kurul'un gerçek ya da tüzel kişi olma şartını, katı bir şekilde uygulamadığı, "hayatın olağan akışı" ve "pratikte ortaya çıkan sorunların çözülebilmesi" gibi gerekçelerle geniş yorumlayabildiği

görülmektedir. Bu noktada, kanunun sözü ile özünün bağdaştırılabilmesi ve uygulama ile mevzuat arasında uyumun sağlanabilmesi adına kanaatimizce KVKK'de yer verilen veri sorumlusu tanımının, bu hususlar da dikkate alınmak suretiyle yeniden düzenlenmesi, kişisel veri işleme faaliyetlerinde ilgili kişilerin hak ve menfaatlerine hizmet edilebilmesi anlamında yararlı bir yaklaşım olacaktır.

Kanun kapsamında yer alan bir diğer aktör ise veri işleyendir. KVKK'nin 3. maddesinin (ğ) bendinde "Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi" şeklinde ifade edilen veri işleyen; faaliyetleri itibarıyla veri sorumlularının iş ve işlemlerini kolaylaştıran, işleme faaliyetlerinde veri sorumlularına destek olan bir role sahiptir. Bu anlamda veri işleyenler, veri sorumlusunun vermiş olduğu yetki çerçevesinde ve veri sorumlusu adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışında teşkilatlanmış aktörler olarak karşımıza çıkmaktadır. Veri sorumlusunun organizasyonu dışında teşkilatlanmış olma, her ne kadar KVKK'de açıkça belirtilmemiş ise de bu husus, veri işleyenin tespitinde önemli bir değerlendirme kriteri olarak karşımıza çıkmaktadır[74]. Zira veri sorumlusunun teşkilat yapısı içerisinde yer alan bir kişi ya da birimin; veri sorumlusunun emir ve talimat alanı içerisinde bulunduğu ve bu sınırlar dâhilinde hareket etmesi gerektiği açıktır. Veri sorumlusunun belirlemiş olduğu sınırlar çerçevesinde hareket eden kişilerin faaliyetleri zaten veri sorumlusuna hasredileceğinden, bu kimselerin, ayrı bir aktör olarak, başlı başına sorumlu tutulabilmesi mümkün olmayacaktır. Veri işleyen ve veri sorumlusunu ayıran bir diğer unsur ise bu aktörlerin görev alanlarıdır. Zira veri sorumlusu; kişisel verilerin toplanmasına karar veren ve bunları toplama yöntemlerini belirleyen, toplanacak veri türlerini kararlaştırarak, bunların kullanım amacını ve kimden toplanacağını tespit eden, verilerin, hangi amaçlarla kullanılacağı, bunların ne süre ile saklanacağı, paylaşılıp paylaşılmayacağı ve paylaşılmasına karar verilmesi halinde kimlerle paylaşılacağı hususlarına karar veren ve bu anlamda işleme faaliyetlerine ilişkin kritik kararları alan ana aktördür. Veri işleyen ise veri sorumlusu ile yapmış olduğu sözleşme çerçevesinde ve veri sorumlusunun talimatları ile hareket eden ve ikincil niteliği olan hususlar üzerinde yetkisi bulunan gerçek ya da tüzel kişilerdir.

Bu noktada belirtilmesi gereken bir konu, anılan sınırlar çerçevesinde hareket etmek koşuluyla bir kişinin hem veri sorumlusu hem veri işleyen olabilmesine KVKK

[74] Özkan, 2020: 80.

uyarınca bir engel bulunmamasıdır. Örneğin bir çağrı merkezi firması, firma bünyesinde istihdam edilen operatörlerin özlük dosyalarının tutulmasına ilişkin olarak veri sorumlusu iken; çağrı merkezi hizmetleri sunumuna ilişkin olarak sözleşmesel ilişki içerisinde bulunduğu bankanın, müşterilerine ait verileri üzerinde veri işleyen statüsüne sahip olacaktır. Bu iki durum arasındaki farkın önemi ise, KVKK'nin kişisel veri işleme faaliyetleri bakımından ana sorumluluğu, veri sorumlularına yüklemiş olmasından ileri gelmektedir. Gerçekten de KVKK, veri güvenliğine ilişkin yükümlülüklerin düzenlendiği 12. madde dışında veri işleyenin sorumluluğu hakkında bir hükme yer vermemiştir. 12. maddenin birinci fıkrasında; "kişisel verilerin hukuka aykırı işlenmesini/kişisel verilere hukuka aykırı olarak erişilmesini önleme ve kişisel verilerin muhafazasını sağlama amacıyla uygun güvenlik düzeyini temin etmeye yönelik olarak gerekli teknik ve idari tedbirleri alma" hususlarında veri sorumlusu ile veri işleyenin müştereken sorumlu tutulacağı hüküm altına alınmıştır. Aynı maddenin dördüncü fıkrasında ise öğrenilen kişisel verilerin, Kanun hükümlerine aykırı olarak başkasına açıklanması ya da işleme amacına aykırı şekilde kullanılması yasaklanmıştır. Bu iki husus dışında KVKK'de veri işleyenin sorumlu olduğunu hüküm altına alan bir düzenleme yer almadığından, veri sorumlusu ve veri işleyenin doğru şekilde tespit edilmesi uygulama bakımından önem arz etmektedir.

2.3.Kişisel Verilerin İşlenmesinde Uyulması Gereken Genel İlkeler

2.3.1.Genel olarak

Kişisel verilerin işlenmesine ilişkin uluslararası düzenlemelerin pek çoğunda, kişisel veri işleme faaliyetlerinde uyulması beklenen standart esaslara yer verildiği görülmektedir. İşleme faaliyetlerinde, ilgili kişilerin hak ve menfaatlerine yönelik olarak daha fazla güvence sağlanmasını amaçlayan bu ilkeler, KVKK'nin 4. maddesinde, beş ana başlık altında düzenlenmektedir. Kanun kapsamında gerçekleşen tüm kişisel veri işleme faaliyetlerinin özünde bulunması gereken ve uyulması zorunluluk arz eden genel ilkeler, "Hukuka ve dürüstlük kurallarına uygun olma", "Doğru ve gerektiğinde güncel olma", "Belirli, açık ve meşru amaçlar için işlenme", "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ve "İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" olarak

öngörülmüştür[75]. Madde metninde genel ilkelere aykırı hareket etmenin açık bir yaptırımına yer verilmemiş ise de Kurul uygulamasında genel ilkelere aykırılık; KVKK'nin 12. maddesinde yer verilen ve veri sorumlusu ile veri işleyenlerin işleme faaliyetine ilişkin teknik ve idari tedbirleri alma yükümlülüğünün ihlali olarak değerlendirilmekte ve idari para cezası uygulanmasına gerekçe olarak gösterilmektedir. Diğer taraftan söz konusu ilkelere aykırı bir işleme faaliyetinin gerçekleştirilmesi sonucunda ilgili kişilerin bir zarara uğraması halinde KVKK'nin 11. maddesinin (ğ) bendi uyarınca, söz konusu zararın giderilmesini talep etme hakkı da bulunmaktadır[76]. Anlaşılacağı üzere kişisel veri işleme faaliyetlerinde, işleme şartlarına uygunluğun yanı sıra genel ilkelere de riayet edilmesi kritik öneme sahip olup; KVKK kapsamında öngörülen genel ilkeler, aşağıda beş başlık halinde ele alınacaktır.

2.3.2.Hukuka ve dürüstlük kurallarına uygun olma

"Hukuka uygunluk" ve "dürüstlük kurallarına uygunluk" olmak üzere iki farklı unsuru bünyesinde barındıran hukuka ve dürüstlük kurallarına uygun olma ilkesi, diğer bazı ilkeleri kapsayan ya da bu ilkelere kaynaklık eden bir özelliğe sahip olması nedeniyle kişisel verilerin korunması hukukunun ilk ilkesi olarak değerlendirilebilir[77].

Hukuka uygunluk; temel itibarıyla kişisel veri işleme faaliyetlerinde gerek yasalarla gerek ikincil düzenlemelerle getirilen hükümlere riayet edilmesini ifade etmekte olup; evrensel hukuk ilkelerine uygun hareket etme gerekliliği de bu ilke kapsamda yer almaktadır[78].

Dürüstlük kuralına uygunluk ise hukuka uygunluk kavramına nazaran sınırları daha belirsiz bir kavram olup; temelde Türk Medeni Kanunu ("TMK") m. 2'de ele alınan kuralın, kişisel verilerin işlenmesi faaliyetleri esnasında ihlal edilmemesini ifade etmektedir. TMK m. 2 anlamında dürüstlük kuralı, orta zekâlı kimselerin toplum içerisinde karşılıklı güvene, ahlaka, dürüstlüğe dayalı davranışları sonucunda meydana gelmiş ve herkesçe benimsenen kuralları ifade etmektedir. Söz konusu ilke uyarınca kişinin, makul ve orta zekâda bir kimsenin göstermiş olduğu davranışı göstermesi beklendiğinden, aksi yönde davranışlar hakkın kötüye kullanılmasını teşkil

[75] Oğuz, Sefer. 2018, Kişisel Verilerin Korunması Hukukunun Genel İlkeleri, s.129.
[76] Taştan, 2017: 48.
[77] Küzeci, 2020: 228.
[78] İmançlı, 2020: 109.

etmektedir. Kişisel verilerin korunması açısından ise bu kural; veri işleme görevi ya da yetkisi veren hukuk kurallarına dayalı olarak gerçekleştirilen işleme faaliyetlerinde kuralların amacı doğrultusunda mümkün olan en az miktarda veri işlenmesi ve ilgili kişilerin öngöremeyeceği biçimde hareket edilmemesi şeklinde somutlaşmaktadır[79].

Dürüstlük kuralına uygun hareket etme ilkesi, kişisel veri işleme faaliyetlerine ilişkin şeffaflığın sağlanması ve ilgili kişilerin konuya ilişkin çıkar ve makul beklentilerinin dikkate alınması ile de yakın ilişki içerisindedir. Zira dürüstlük kuralına uygun hareket etme; kişisel verinin, yasal sınırlar dâhilinde tespit edilmiş olan amaçlara uygun şekilde işlenmesini temin eden bir araç olarak, ilgili kişilerin, işleme faaliyetinin gerçekleştirilmesi hususunda verinin gerçekten amaçları doğrultusunda kullanılıp kullanılmadığı hakkında bilgi sahibi olmasını ve gerektiğinde yasal imkânlarını kullanabilmesi anlamında önem arz etmektedir. Bu bakımdan veri sorumlularının, yasal çerçevede belirlemiş oldukları hedeflere ulaşmak üzere gerçekleştirecekleri faaliyetleri, ilgili kişilerin çıkarları ve makul beklentileri doğrultusunda gerçekleştirmesi ve ilgili kişinin beklemediği ve beklemesinin de gerekmediği sonuçların ortaya çıkmasını önleyecek şekilde hareket etmesi gerekmektedir. Bu yönüyle işleme faaliyetlerinde hesap verebilirlik ile de yakın ilişki içerisinde olan dürüstlük kuralı, aynı zamanda veri sorumluları tarafından, belirlenen amaçlar uyarınca mümkün olan en az miktarda veri işlenmesini ve ilgili kişilerin öngöremeyeceği şekilde hareket edilmemesini de gerektirmektedir.

2.3.3.Doğru ve gerektiğinde güncel olma

Kişisel verilerin doğruluğu ve güncelliği, hem ilgili kişilerin hem de veri sorumlularının menfaatine hizmet etmektedir. Nitekim verinin gerçek durumu yansıtmaması ve buna uygun şekilde işlenmemesi; belli amaçlara ulaşabilme gayesi ile kişisel verileri işleyen veri sorumlularının, söz konusu amaçlara ulaşmasını engelleyebileceği gibi, verinin ilişkili bulunduğu ilgili kişiler adına olumsuz sonuçların ortaya çıkmasına da yol açabilecek niteliktedir. Verinin işlenmesinde tüm aktörlerin menfaatine olan doğruluk ilkesi, verinin gerçekten doğru olup olmadığını kontrol noktasında ilgili kişinin işleme faaliyetine dahlini zorunlu kılmaktadır. Bu

[79] Alarslan, Fatma. 2016, Medeni Hukuk'da Dürüstlük Kuralı ve Hakkın Kötüye Kullanılması Yasağı, s.416.

yönüyle doğruluk; ilgili kişinin, kişisel verilerine erişebilmesi ve erişim hakkının aktif şekilde sağlanması ile yakın ilişki içerisindedir.

Diğer taraftan, kişisel veri işleme faaliyetinin doğruluğunun her hal ve şartta işleme faaliyetinin sıhhati açısından yeterli olamayabileceğini öngören kanun koyucu, bazı durumlarda verinin güncel olması gerektiğini de kabul ederek düzenlemeyi bu şekliyle kaleme almıştır. Güncellik, hükmün ifadesinde yerini bulan "gereklilik" unsurundan anlaşıldığı üzere, her durum bakımından aranan bir unsur olarak ele alınmamış; ancak güncelliği niteleyen "gerekme durumu"ndan ne anlaşılması gerektiği de belirtilmemiştir. Verinin doğru ve güncel olarak tutulması, veri sorumlusunun yükümlülüğünde bulunduğundan, güncelliğin ne zaman gerekli olduğunun takdiri de büyük ölçüde veri sorumlusu tarafından gerçekleştirilecektir. Bu noktada aktif özen yükümlülüğünün; özellikle, söz konusu verilere dayalı olarak ilgili kişiyle alakalı bir sonucun ortaya konulduğu durumlarda veri sorumlusuna ait olduğunun kabulü gerekmektedir. Bununla birlikte veri sorumlusunun, verinin güncelliğini sağlamak adına devamlı şekilde araştırma faaliyetlerinde bulunması, hayatın olağan akışına uygun olmadığı gibi makul bir yaklaşım olarak da değerlendirilemeyeceğinden veri sorumlularının ilgili kişinin bilgilerinin doğru ve güncel olmasını temin edecek kanalları açık tutarak, ilgili kişinin kişisel verilerine ilişkin değişikliklerin gerçekleşmesi halinde bu değişiklikleri bizzat yapabilmesine ya da veri sorumlusunu değişiklikler hakkında bilgilendirmesine imkân sağlanması gerektiği kabul edilmelidir[80].

2.3.4.Belirli, açık ve meşru amaçlar için işlenme

Veri sorumlularının, pek çok amaç doğrultusunda kişisel veri işleme faaliyetinde bulunabilmesi mümkün ise de bu amaçların önceden belirlenerek, işleme faaliyeti çerçevesinde yapılacak aydınlatma kapsamında ilgili kişinin bilgisine sunulması, ilgili kişinin kişisel verileri üzerindeki denetim hakkının bir gereğidir.

Kişisel verilerin hangi amaçlar doğrultusunda işlendiğinin bilinmemesi ya da amaçların net şekilde ortaya konulamamış olması; verilerin başka amaç ya da amaçlarla kullanılıp kullanılmadığının denetlenememesi ile sonuçlanabileceği gibi (diğer ilkelerde de olduğu üzere) tüm işleme şartları bakımından işlemenin hukuka

[80] Özkan, 2020: 88.

aykırı şekilde gerçekleşmesine sebep olabilir. Özellikle işlemenin açık rızaya dayalı olduğu hallerde, amacın belirli olması, verilecek rızanın sıhhatine etki edebileceği için ayrı bir öneme sahip olup; kişinin neye rıza verdiğini bilmesi ve veri sorumlusunun da bu amaç çerçevesinde gereken miktar kadar veri işleyebilmesini sağlama amacına hizmet etmektedir[81]. Bu bakımdan aşağıda ele alınacak olan "amaçla bağlantılı, sınırlı ve ölçülü olma" ilkesi ile de yakın ilişki içerisinde olan "belirli, açık ve meşru amaçlar için işlenme" ilkesi; amacın belirliliği bağlamında; veri sorumlusu tarafından, işleme faaliyetinin başında öngörülmediği halde, sonradan ortaya çıkabileceği düşünülen farklı amaçlar doğrultusunda kişisel veri işleme faaliyetinde bulunulmamasını amaç edinmektedir.

Bu ilke uyarınca kişisel verilerin önceden belirlenmiş ya da belirlenebilen, hukuka uygun amaç ya da amaçlar için işlenmesi asıl olsa da işleme faaliyeti esnasında farklı sebeplerle amacın değişmesi de imkân dâhilindedir; amacın belirli, açık ve meşru olması, amacın değiştirilmesini yasaklamamaktadır. İşleme faaliyeti esnasında amacın değiştiği ya da değiştirilmek istendiği durumlarda, ilke uyarınca yeni amaçların ilgili kişinin bilgisine yeniden sunulması ve ilgili kişinin, yeni durumu uygun görmeyebileceği hususu da dikkate alınarak işlemenin rızaya dayandığı durumlarda ayrıca açık rıza alınması yoluna gidilmesi gerekmektedir[82].

Öte yandan amacın kişisel veri işleme faaliyeti gerçekleştirilmeden önce belirlenmiş olması, ilkenin bir boyutu olup; diğer boyutta ise yukarıda değinilen denetim mekanizmasına işlerlik kazandırabilmek bakımından, bunun ilgili kişiye açıklanması yer almaktadır. Bu açıdan bakıldığında veri sorumlusu tarafından belirlenen amaç ya da amaçların, ilgili kişilerin anlayabileceği şekilde sunulabilmesi de gerekmekte; amacın net, anlaşılır ve somut şekilde ifade edilmesi önem arz etmektedir. Bu hususta ana kriterin ortalama bilgi seviyesine sahip kişilerin bilgi edinebilirlik düzeyi olduğunu kabul etmek kanaatimizce uygun olacaktır. Bununla birlikte işleme faaliyetinin belli bir kesime hasredildiği durumda, bu kesime dâhil ortalama bir kişinin esas alınması gerektiğinin kabulü doğrultusunda hareket edilmelidir[83].

Diğer taraftan söz konusu ilkeye uyum anlamında, amacın yalnızca belirli ve açık olması yeterli görülmemiş; belirlenen bu amaçların meşru olması da aranmıştır.

[81] Özdemir, Hayrunnisa. 2009, Elektronik haberleşme alanında kişisel verilerin özel hukuk hükümlerine göre korunması, s.141.
[82] Altındere, Murat. 2020, Kişisel Verilerin Korunması Hukuku ve Uygulaması, s.38
[83] Çekin, 2020: 75.

Amacın meşruluğu ile kast edilen, temelde, hukuk sistemi içerisinde öngörülen düzenlemelere aykırı bir amaç ile kişisel verileri işleme faaliyetinde bulunulmamasıdır. Örneğin tefecilik faaliyetinde bulunan kimsenin, alacaklı bulunduğu kişilere ait verileri barındıran bir kayıt sistemi tutmasında, bu verilerin, meşru bir amaç için tutulduğunu söylemek mümkün olamayacaktır. Bununla birlikte kanaatimizce amacın meşru olmasının, yalnızca kişisel veri işlemenin yasal bir zemine oturtulmuş olması olarak düşünülmemesi gerekmektedir; zira bu kabul, söz konusu ilkeyi, yukarıda ele alınan hukuka ve dürüstlük kuralına uygun olma ile eş tutmak anlamına gelecektir. Diğer taraftan hukuk düzen tarafından yasaklanmamış bir faaliyetin, veri sorumlusunun gerçekleştireceği somut işleme faaliyeti ile tamamen ilgisiz de olabilmesi de imkân dâhilinde olup; bu ihtimalde kişisel verilerinin işlenmesine ilişkin olarak ilgili kişinin menfaatine bir durum da kural olarak bulunmamaktadır. Bu anlamda amacın meşru olmasının, yasal sınırlar çerçevesinde olmak kaydıyla, veri sorumlusunun yapmakta olduğu iş ya da sunmakta olduğu hizmetler ile bağlantılı ve bunlar için gerekli olmasını da içerdiği kabul edilmektedir[84].

2.3.5.İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma

Bir üst başlıkta, veri sorumlusunun kişisel veri işleme faaliyetini gerçekleştirmeden önce bu faaliyetin amacını belirlemesi, daha sonra buna uygun verilerin temin edileceği kaynakları tespit etmesi ve en son verileri temin aşamasına geçilmesi gerektiği belirtilmişti. Belirlenen amacın gerçekleşmesine imkân sağlamayacak olan yahut belirlenmiş amaç ya da amaçlardan başka amaçlara hizmet etmesi beklenen verilerin, işlenmesi için geçerli bir sebep bulunmamaktadır. Özellikle belirtilen amaca, verinin işlenmesi dışındaki araçlarla ulaşılabildiği ve bu araçların temel hak ve özgürlüklere daha az müdahale ettiği ya da hiç müdahale etmediği durumlarda veri işleme faaliyetinin gerçekleştirilmemesi uygun olacaktır. Kişisel verilerin işlenmesi faaliyetinin, ilgili kişilerin hak alanına müdahale teşkil etmesi sebebiyle, amaç ile bağlantılı olarak değerlendirilse dahi her durumda gerçekleşebileceğini söylemek mümkün değildir. Nitekim kanun koyucu, düzenlemenin lafzından da anlaşıldığı üzere amaçla bağlantılı olmayı yeterli görmeyerek, aynı zamanda amaç ile sınırlı bir işleme faaliyetinde bulunulması gerektiğini hüküm altına almıştır. Sınırlılığın bir diğer

[84] Dülger, 2020: 278.

sonucu da, daha önce öngörülmemiş bir amaç doğrultusunda ya da sonradan ortaya çıkması beklenen amaçlarla işleme faaliyetinde bulunulamamasıdır.

Amaç ile uyumlu olmayan verilerin işlenmemesi gereğinin yanı sıra işlenecek verinin, öngörülen amaca ulaşma bakımından yeterli olduğu durumda daha fazlasının işlenmemesi, bu anlamda amaca ulaşmak bakımından en az miktarda verinin işlenmesi de ilkenin diğer boyutudur. Bu bakımdan ölçülülük, veri işleme faaliyeti ile gerçekleştirilmesi istenen amaç arasında makul bir dengenin kurulmasını hedeflemektedir[85].

2.3.6.İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme

Kişisel veri işleme faaliyetlerinde, veri sorumlusunun hedeflediği amaca ulaşması ile -verinin elde tutulmasını haklı kılan başkaca bir sebep bulunması dışında- işlenen verilerin muhafazasını meşru kılacak bir sebep kalmayacaktır. Artık işlenmesine gerek bulunmayan verinin saklanmaya devam edilmesi, veri sorumlusunun KVKK'nin 12. maddesi bağlamında öngörülen veri güvenliğine ilişkin yükümlülüklerini de ortadan kaldırmadığından, veri ihlaline ilişkin riskler, bertaraf edilmiş olmamaktadır[86]. Bu bakımdan verinin muhafazasını meşru kılacak bir sebebin bulunmaması halinde işleme faaliyeti derhal sonlandırılarak, veri sorumlusunun, ilgili verileri imha etmesi gerekmektedir. Verinin imhasına ilişkin olarak KVKK'nin 7. maddesinde, gerek KVKK gerek diğer kanunlara uygun şekilde işlenen kişisel verilerin, "işlenmesini gerektiren sebeplerin ortadan kalkması" halinde söz konusu verilerin "talep üzerine ya da resen", veri sorumlusu tarafından "silineceği, yok edileceği ya da anonim hale getirileceği" hüküm altına alınmaktadır. Bununla birlikte KVKK'de verinin ne zaman silineceği/yok edileceği ya da anonim hale getirileceğine ilişkin özel bir zamansal bir kısıtlama öngörülmediği, Kanun'un uygulanması bakımından işlenmeyi gerektiren sebebin ortadan kalkmasının ana kriter olarak belirlendiği anlaşılmaktadır. Bu anlamda talep üzerine verinin imhasına ilişkin olarak özel bir sürenin öngörülmediği hallerde uygulanmak üzere, veri ihlal bildirimlerinde öngörülen 72 saat kuralına benzer bir düzenleme öngörülerek, imhaya ilişkin üst bir süre sınırı getirilmesi kanaatimizce söz konusu ilkenin uygulanmasında caydırıcı bir rol üstlenecektir. İlgili

[85] Akgül, Aydın. 2014, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, s.154.
[86] Küzeci, 2020: 245.

madde çerçevesinde Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonim Hale Getirilmesi Hakkında Yönetmelik yayımlanmış ve bazı önemli tanımlamalar ilgili Yönetmelik vasıtasıyla yapılmıştır[87]. Yönetmelik'in 11 (2). maddesi uyarınca *"periyodik imhanın gerçekleştirileceği zaman aralığı, veri sorumlusu tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez"* denilerek azami süre sınırı çizilmiştir.

2.4.Kişisel Verilerin İşlenebileceği Haller

2.4.1.Genel olarak

Kişisel Verilerin Korunması Kanunu; hangi hallerde kişisel verilerin işlenebileceğini, 5. ve 6. maddelerinde açık düzenleme altına almaktadır. KVKK m. 5, Kanun tarafından özel niteliğe sahip olduğu açıkça düzenleme altına alınan veriler dışında kalan, diğer bir deyişle "genel" olarak tabir edebileceğimiz kişisel verilerin, hangi hallerde işlenmesinin hukuka uygun olacağını düzenlemekte iken; m. 6 düzenlemesi, söz konusu hususu, mezkûr maddede özel nitelikli olarak ifade edilen veri kategorileri bakımından ele almaktadır.

Bu noktada, anılan maddelerde belirtilen hallerin, sınırlı sayım yolu ile ele alındığını ve sayılan haller dışında gerçekleşecek bir kişisel veri işleme faaliyetinin, hukuka aykırılık içereceğini; KVKK'de öngörülen işleme şartları bakımından kıyas yapılabilmesi imkânı bulunmadığını belirtmek gerekmektedir. Benzer şekilde 6. madde bağlamında özel nitelikli kişisel veri kategorilerinin de genişletilebilmesi söz konusu olmamaktadır. Bu bakımdan mezkûr düzenlemelerde yer alan hallerin doğru şekilde yorumlanması, işleme faaliyetinin sıhhatine etki edebilecek nitelikte olup; aşağıda yer alan başlıklarda, bu haller detaylı olarak incelenecektir.

Kişisel verilerin işlenebilmesine ilişkin olarak belirtilmesi gereken bir diğer husus da; işleme şartları arasında bir hiyerarşi bulunmadığıdır. Madde metnine bakıldığında Kanun'un lafzi ifadesi; temel kuralın açık rıza, bunun istisnalarının ise KVKK'nin 5. maddesinin ikinci fıkrası ile 6. maddesinin üçüncü fıkrasındaki haller olduğuna işaret etmektedir. Bununla birlikte gerek Direktif gerek GVKT, açık rıza ile diğer işleme

[87] Bu kapsamdaki tanımlardan biri olan periyodik imha süreçleri ise *"Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi"* olarak tanımlanmıştır.

şartları arasında bir hiyerarşi öngörmemektedir. Nitekim uygulamada da Kurul, gerek 5. madde gerek 6. madde kapsamında gerçekleşecek işleme faaliyetlerinde, ilgili maddelerde yer alan işleme şartlarından herhangi birinin varlığı ile verinin hukuka uygun şekilde işlenebileceğini kabul etmekte ve işleme şartlarını bir bütün olarak ele almaktadır. Diğer taraftan Kurul, işleme faaliyetinin açık rıza dışında bir hukuki sebebe dayandırılabildiği hallerde diğer işleme şartlarına başvurulması gerektiğini; bu işleme şartlarına başvurmak yerine açık rıza alınması ve ilgili kişinin daha sonra açık rızasını geri çekmesi halinde diğer işleme şartlarına dayanılmasını, aldatıcı ve hakkın kötüye kullanımı niteliğinde değerlendirmektedir. Kurul'un yapmış olduğu bu yorumun diğer bir sonucu da, birden fazla işleme şartının somut olayda bir arada bulunabileceği ve işlemenin, birden fazla işleme şartına dayalı olarak gerçekleştirilebilmesinin mümkün olduğudur. Bu bakımdan, aşağıda ele alınacak olan işleme şartları; yasal anlamda öncelik-sonralık ilişkisine tabi tutulmadığı gibi bunun doğal bir sonucu olarak da KVKK ve ikincil düzenlemelerinden kaynaklı yükümlülükler de devam etmektedir. Bununla birlikte Kurul uygulamasında, açık rızanın geri çekilmesi durumunda diğer işleme şartlarına dayanılmasının aldatıcı ve hakkın kötüye kullanımı olarak değerlendirildiği dikkate alındığında işleme faaliyetinin dürüstlük kuralına uygun şekilde yürütülebilmesi anlamında fiili olarak diğer işleme şartlarına, açık rızaya nazaran öncelik verilmesi gerektiği söylenebilecektir.

2.4.2.Açık Rıza

Kişisel verilerin işlenmesinde açık rıza; ilgili kişinin, kişisel veri işleme sürecine katılmasına ve verileri üzerinde denetim sağlamasına; bu anlamda kişinin, kendi verilerinin geleceğini belirlemesi amacına hizmet etmektedir. Açık rıza bu yönüyle, kişisel verilerin korunması hakkının bir insan hakkı olduğu görüşüne etkinlik kazandırmaktadır. Konuya ilişkin olarak kişisel verilerin işlenmesine verilen rızanın, kişisel verilerin korunması hakkının kullanılmasını ifade ettiğine ilişkin görüşler ve bunun aksine, rıza beyanının, bireyin kişisel verilerinin korunması hakkından vazgeçmesi anlamına geldiği yönünde yaklaşımlar bulunsa da hangi görüş benimsenirse benimsensin açık rıza ile bireylerin kendi verileri üzerindeki denetim hakkının sağlamlaştığı bir gerçektir[88]. Bir kişisel veri işleme şartı olarak açık rızanın

[88] Yılmaz, Sabire Sanem. 2014, Tıp alanında kişisel verilerin hukuka aykırı olarak verilmesinin ceza hukuku açısından değerlendirilmesi (sır saklama yükümlülüğü kapsamında), s.86.

hukuki işlevi ise kanaatimizce diğer işleme şartlarında olduğu gibi hukuka aykırı bir faaliyet olan "işleme"yi hukuka uygun hale getirmektir.

Bu noktada önemle belirtmek gerekir ki KVKK kapsamında belirtilen açık rıza kavramı TMK ile düzenlenen rıza kavramından[89] ayrılmaktadır. KVKK kapsamında alınacak "açık" rızanın Kanun ve ikincil mevzuat ile belirlenen kriterlere uygun şekilde verilmesi gerekmektedir.

Kişisel verilerin korunması hukuku alanında kritik öneme sahip bu kavramın ne olduğunun net şekilde anlaşılması ve kavram kapsamında önem arz eden hususların değerlendirilmesi gerekmektedir. Nitekim KVKK'de, "açık rıza" şeklinde ifade edilen bu kavram; mehaz düzenleme olan Direktifte bazı yerlerde "rıza", bazı yerlerde ise "açık rıza" şeklinde ifade edilmiş ve bu yaklaşım Direktifi ilga eden GVKT'de de korunmuştur[90].

Yukarıda değinmiş olduğumuz ve genel bir uygun bulma haline işaret eden rıza kavramı, KVKK'de daha farklı bir yaklaşımla ele alınmış ve "rıza" kavramı yerine "açık rıza" kullanılmıştır. KVKK'nin 3. maddesinin birinci fıkrasının (a) bendinde açık rıza, "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" şeklinde tanımlanmıştır. Kanunun gerekçesinde; açık rıza kavramının Direktif dikkate alınarak tanımlandığı, bu kapsamda açık rızanın; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılması gerektiği belirtilmiştir.

Direktifin ikinci maddesinde "veri öznesinin rızası" şeklinde yer bulan rıza kavramı; "veri sahibinin, kendisiyle ilgili kişisel verilerin işlenmesine razı olduğu hususundaki isteğinin özgürce verilen, belirli ve bilgilendirilmeye dayanan göstergesi " olarak ifade edilmiştir. Bu haliyle KVKK'den farklı olarak "açıklık" unsuruna yer vermeyen Direktif, işlemeyi meşru hale getiren kriterlerin düzenlendiği 7. maddenin (a) bendinde, "veri sahibinin belirsizliğe mahal vermeyecek bir şekilde rıza vermesi"nden söz etmektedir. Direktifin özel veri kategorilerinin işlenmesi başlığını taşıyan 8.

[89] TMK kapsamında rıza "bir kişinin bir öneriyi veya talebi gönüllü olarak kabul etmesi"ni ifade eden hukuka uygunluk hallerinden birini tanımlamaktadır. TMK kapsamında örtülü gibi farklı şekillerde verilebilecek rıza hallerinden ayrılan açık rıza KVKK kapsamında ancak "belirli bir konuya ilişkin olma, bilgilendirilmeye dayanma ve özgür iradeyle açıklanma" koşullarını gerçekleştirdiği takdirde geçerlilik kazanacaktır.

[90] Çelikel, Serdar. 2021, Kişisel verilerin işlenmesinde, açık rıza hukuka uygunluk nedeninin, 95/46 sayılı Direktif ve GDPR'la karşılaştırılmalı olarak incelenmesi.

maddesinde ise, kişinin ırkı ya da etnik kökenini, politik fikirlerini, dini ya da felsefi inançlarını, sendika üyeliğini ve sağlığını ya da cinsel hayatını açığa çıkaracak kişisel verilerin işlenmesinin yasak olduğu belirtildikten sonra bu hükmün, veri öznesinin bu verilerin işlenmesine "açık rızasının" bulunması durumunda uygulanmayacağı belirtilmiştir.

Direktifin 8. maddesinde "explicit consent" şeklinde ve 7. maddesinde "unambiguously given consent" ifadeleri ile yer bulan rıza ile neyin kast edildiğine yer verilmemiş ise de WP 29 tarafından çıkarılan, 13 Temmuz 2011 tarihinde kabul edilen 15/2011 sayılı Görüş'te rıza kavramı detaylı şekilde incelenmiştir. WP 29'a göre ilgili kişi rızasının; işlemenin yasal bir temel dâhilinde gerçekleşebilmesi bakımından 7. madde uyarınca belirsizliğe mahal vermeden, diğer bir deyişle kesin olarak verilmesi gerekmektedir. WP 29; bu durumun ilgili kişi verilerinin işlenmesi noktasındaki niyetini, şüpheye mahal vermeyecek şekilde gösteren ve birden fazla anlama gelmeyen, tek ve hataya yer vermeyen bir sonuca yönelen, ilgili kişinin verilerinin işlenmesine gösterilen bir rıza olarak algılamaktadır. Bu anlamda "unambiguously" olarak ifade edilen ve özel niteliği bulunmayan kişisel veriler bakımından uygulama alanı bulan rızanın, veriliş şeklinden ziyade ulaşılan sonucu önemsediği söylenebilecektir. Bu hususta rızanın, telefon ile, online yollarla ya da sözlü olarak verilebileceği; rızanın verildiğinin ispatı noktasında veri sorumlularının yükümlü tutulacağına ilişkin ifadeler de önem taşımaktadır. Mezkûr Görüş'te rızanın ıslak imza, kutucuk işaretleme ve sözlü beyan gibi yollarla verilebileceğinin belirtildiği, ayrıca rızanın eylem yolu ile verilmesine ilişkin bir örneğe de yer verildiği görülmektedir. Görüş kapsamında verilen bir örnek, bir otelde yapılması planlanan fotoğraf çekimlerini konu edinmekte olup; otelde konaklayan misafirlerin, konu hakkında bilgilendirilmelerini müteakip, çekimlerde yer almak istemeyenlere ayrı bir kafeterya tahsisi sağlanması durumunda, ilgili saatlerde çekimin gerçekleştirileceği kafeteryada bulunan kişiler bakımından çekime açık rıza verildiği şeklinde bir değerlendirmede bulunulabileceği ifade edilmektedir. Bununla birlikte WP 29, her eylemin açık rıza vermeyi kapsamayacağını belirterek; bir online oyunu oynamanın, reklamcılık faaliyetleri için kişisel verilerinin işlenmesine rıza vermeyi otomatik olarak kapsamayacağını da örneklemiştir. Bu anlamda WP 29, belli bir doğrultuda hareket etmenin yalnızca kişisel verilerin işlenmesi anlamıyla yorumlanabildiği, başka bir

yorumun çıkarılmasının mümkün olmadığı şekliyle verilen rızayı açık rıza olarak kabul etmektedir.

Söz konusu Görüş ışığında Direktifin, özel nitelikli olmayan kişisel verilerin işlenmesinde rızanın açıklık unsurunu aramadığı, bununla birlikte 7. maddede rızaya verilen nitelik itibarıyla rızanın "kesin" olmasını beklediği; WP 29'un ise kişisel verinin işlenmesine verilecek rızanın, verinin işlenmesi konusunda verildiği ve bunun dışında bir anlam ile yorumlanamadığı durumlar ve şartlara hasredildiği yönünde bir değerlendirmede bulunduğu anlaşılmaktadır.

Özel nitelikli veri kategorileri bakımından ise Direktifte "rıza" yerine "açık rıza" ifadesinin doğrudan yer aldığı görülmektedir. Direktifin 8. maddesinin ikinci fıkrasının (a) bendinde "explicit consent" olarak ifade edilen bu rızanın verilmesine ilişkin olarak şekli bir şart öngörülmemiş; WP 29 tarafından, özel nitelikli kişisel veriler bakımından öngörülen açık rızanın; online işleme faaliyetlerinde elektronik ya da dijital imza ile verilebileceği gibi tıklanabilir butonlar, doğrulama e-postaları gönderilmesi vasıtasıyla da verilebildiği belirtilmiştir.

Direktifi ilga eden GVKT'de ise rıza kavramı, "ilgili kişinin kendisiyle ilgili kişisel verilerinin işlenmesi hususundaki isteklerinin; bir beyan ya da olumlu açık bir eylem ile belirtildiği; özgürce verilen, belirli, bilgilendirmeye dayalı ve kesin göstergesi" olarak tanımlanmıştır. Söz konusu tanımda da rızanın "ilgili kişinin verilerinin işlenmesi hususundaki isteğinin kesin göstergesi" ifadesinde yer verilen "unambiguous" kelimesinin bulunduğu; bununla birlikte söz konusu tanımda Direktiften farklı olarak kesin göstergenin, bir beyan ya da açık olumlu eylem yolu ile verilebileceği yer almıştır. Konuya ilişkin olarak GVKT'nin 32 numaralı Gerekçesinde, rızanın açık bir olumlu eylem yolu ile verilmesi hususunda verinin işlenmesini kabul etmeyi açıkça gösteren davranışların kapsama dâhil olduğu belirtilmiş; GVKT'de de internet ziyareti sırasında bir kutunun işaretlenmesi, bilgi toplumu hizmetleri için teknik ayarların seçilmesi gibi durumlarda açık olumlu eylemin var olduğu, bununla birlikte sessizlik, önceden işaretlenmiş kutular ya da hareketsiz kalmanın rıza teşkil etmediği ifade edilmiştir. Konuya ilişkin olarak EDPB, açık olumlu eylemin, veri sahibinin, belirli bir konu özelinde ve kasıtlı (bilinçli) şekilde gerçekleşen bir eylemde bulunması durumunda gerçekleştiğini kabul etmekte olup; ayrıca açık gösterge kavramı bağlamında rızanın; yazılı, sözlü ya da elektronik yollarla da verilebileceğini, gerekli aydınlatmalar yapıldıktan sonra kullanıcıya

sunulan ve önceden işaretlenmemiş bir kutucuğun işaretlenmesi suretiyle de gerçekleştirilebileceğini; veri sorumlularının organizasyonel yapılarına uygun rıza akışları öngörmelerinin de mümkün olduğunu, bu bağlamda fiziksel hareketlerin de açık rıza olarak kabul edilebileceğini belirtmektedir. Bununla birlikte EDPB, "genel koşullar ve şartların ya da bir sözleşme yapılmasının kişisel verilerin işlenmesi noktasında açık bir olumlu eylem olarak görülemeyeceğini yahut önceden işaretlenmiş kutucuklar, sessizlik ya da hareketsizlik durumlarının bu şekilde yorumlanamayacağını belirtmektedir.

Özel nitelikli kişisel verilerin işlenmesi hususunda ise GVKT, Direktife benzer şekilde "explicit" ifadesini kullanmaktadır. Söz konusu ifade, daha hassas korumayı gerektiren özel nitelikli veriler bakımından "unambiguous" kelimesi yerine kullanılması sebebiyle daha üstün bir koruma öngördüğü ve bu veriler bakımından daha güçlü bir koruma arandığı şeklinde yorumlanabilmektedir. Ancak GVKT bağlamında, "explicit" ifadesi, özel niteliği bulunmayan kişisel veriler bakımından aranmış olan "unambiguous" ifadesinden daha üstün bir koruma getirmekten ziyade, ilgili kişilerin rızayı ifade ediş biçimine vurgu yapmaktadır. EDPB'ye göre bu anlamıyla açık rıza, yazılı ya da imzalı beyanın yanı sıra dijital/çevrimiçi platformlar bakımından elektronik formların doldurulması, e-posta gönderilmesi, ilgili kişinin imzasını taşıyan belgenin taranarak yüklenmesi şeklinde gerçekleşebilmekte, elektronik imzalı belgeler ile yapılabildiği gibi sözlü olarak da verilebilmekte, telefon görüşmeleri ile ya da bir butona basmak suretiyle de açık rıza verilebilmektedir.

Direktif ve GVKT birlikte değerlendirildiğinde kanaatimiz, sözü edilen iki rıza türü arasında kolay anlaşılır açık bir fark bulunmadığı yönündedir. Öte yandan İngiltere Veri Koruma Otoritesi'nin ("ICO") konu ile ilgili rehber niteliğindeki görüşleri kapsamında; rızaya yönelik olarak olumlu herhangi bir eylemin kabul edildiği, örneğin e-posta adresi girilecek bir alanın altında "size özel tekliflerden haberdar olmak için e-postanızı kullanacağız" ifadesi yer aldığı takdirde ilgili kişinin e-postasını ilgili boşluğa yazması rıza kapsamını karşılarken, açık rıza niteliğinin sağlanabilmesi için ilgili kişinin rıza verdiğine dair açık bir beyan/onay vermesi gerekliliği kapsamında e-postasını ilgili bölüme girdikten sonra rıza verdiğine dair bir onay kutucuğunu da işaretlemesi gerekmektedir. GVKT'nin bu yaklaşımı esas itibarıyla benimsediği, Direktife ek olarak özel niteliği bulunmayan veriler bakımından kabul gören tanıma,

açık rızanın bir beyan ya da açık olumlu eylem ile de verilebileceği hususunu ekleyerek açık hüküm altına aldığı görülmektedir.

Kişisel Verilerin Korunması Kanunu bakımından ise her iki veri kategorisi bakımından "explicit" olarak ifade edilen açık rızanın referans alındığı, bununla birlikte kavramın yalnızca unsurları ile tanımlandığı ve açıklık ile neyin kastedildiğine yönelik bir düzenlemeye yer verilmediği görülmektedir. Kurum tarafından çıkarılan Uygulama Rehberinde de yalnızca açık rızanın, rıza veren kişinin olumlu irade beyanını içermesi gerektiğinden söz edilmekte ve mevzuatta yer verilen özel düzenlemeler saklı kalmak kaydıyla açık rızanın yazılı olmasına gerek olmadığı, elektronik ortam ya da çağrı merkezi gibi yollarla da alınabilmesinin mümkün olduğu belirtilmektedir.

2.4.3.Kanunlarda açıkça öngörülme

Kişisel verilerin açık rıza dışında işlenmesine cevaz verilen ilk hal, kişisel verilerin işlenebilmesine kanunlarda açıkça yer verilmesi halidir. Hukukun bir kaynağı olarak kanun, temel itibarıyla yasama organı tarafından anayasada öngörülen biçim ve yönteme uyularak kanun adı altında çıkarılan yazılı hukuk kurallarını ifade etmekte olup; kural olarak genel, soyut ve süreklilik arz eden metinleri ifade etmektedir[91]. Bununla birlikte kanun ifadesinin; şekli ve maddi olmak üzere iki anlamda kullanıldığı görülmektedir. Bunlardan şekli kanun, kanunların yetkili organ veya yasama meclisi tarafından, önceden kabul edilen usul ve esaslara göre yapılmış olmasını; maddi kanun ise kanunun taşıdığı anlam ve içeriğinin ne olduğu gözetilerek, işlemi yapan organ dikkate alınmaksızın soyut bir inceleme ile genel, objektif ve sürekli kural niteliğinde olduğu değerlendirilen içerikleri ifade etmektedir. Kanun, TBMM tarafından 1982 Anayasası'nda ve TBMM İçtüzüğü'nde gösterilen şekil ve esaslara uygun şekilde çıkarılan metinleri ifade etmekte olup; bu anlamda Türk Hukuku'nda şekli anlamıyla kabul edilmiştir[92].

Kişisel Verilerin Korunması Kanununun gerekçesinde, "kolluk tarafından bir suç soruşturması sebebiyle, 2559 sayılı Polis Vazife ve Salahiyet Kanununun 5 inci maddesi uyarınca şüphelilerin parmak izlerinin alınması; 5352 sayılı Adli Sicil Kanunu uyarınca Adalet Bakanlığının kişilerin ceza mahkûmiyetlerine ilişkin

[91] Sümer, Haluk Hadi. 2020, Hukuka Giriş- Kavramlar & Kurumlar, s.60-61
[92] Fendoğlu, Hasan Tahsin. 2018, Hukuka Giriş, s.95

verilerini işlemesi" örnekleri verilmiş olup; gerekçe metninde yer alan örneklerden de kanun ifadesinin şekli manada değerlendirildiği sonucuna varmak mümkündür. Bununla birlikte Kurul, vermiş olduğu bir kararında, konuya ilişkin bir değerlendirme yapmış ve "kanun" ifadesini maddi manada yorumlayarak, tebliğ hükmü uyarınca gerçekleşen kişisel veri işleme faaliyetini, kanunlarda öngörülme kapsamında kabul etmiştir. Bu noktada Kurul'un konuya yaklaşımının, kanunlarda yer verilen düzenlemeler uyarınca kişisel veri işleme faaliyetinin gerçekleştirilmesine ilişkin açık bir hükmün bulunmadığı, bununla birlikte ilgili kanun hükmünün, kişisel veri işlemeyi gerektirdiği durumlarda, düzenlemelerin detaylarının alt düzenleyici işlemler vasıtasıyla ele alındığı hallerde, alt düzenleyici işlem uyarınca gerçekleştirilen işleme faaliyetinin, kanunlarda öngörülme şartını sağladığı yönünde olduğu anlaşılmaktadır[93].

Genel hukuk kuralları uyarınca alt düzenleyici işlemlerin, normlar hiyerarşisine göre kendisinin üstünde yer alan kaynağa aykırılık içermemesi gerektiğinden, kanunlarda öngörülmemiş bir işleme faaliyetinin, alt düzenleyici işlem ile düzenlenmemiş olması esastır. Şayet alt düzenleyici işlem, kanunda düzenlenmiş bir hususu detaylandırmakta ise, işleme faaliyetinin ana dayanağı yine kanun olacağından konuya ilişkin hukuki bir sorunun ortaya çıkması kanaatimizce mümkün görünmemektedir. Bununla birlikte kanunun, kişisel veri işleme faaliyetinde bulunulabileceğine dair herhangi bir düzenleme ya da yollama öngörmemesine rağmen alt düzenleyici işlemin kişisel verilerin işlenmesine cevaz verdiği durumda, işleme faaliyetinin dayanağını hiçbir şekilde kanun oluşturamayacağından kanaatimizce işleme faaliyetinin kanunlarda açıkça öngörülme işleme şartına dayanmadığının kabul edilmesi gerekmektedir.

Öte yandan öğretide, söz konusu işleme şartına dayalı olarak gerçekleşen işleme faaliyetlerinin, istisnanın kuraldan daha geniş şekilde uygulanmasına yol açabileceği ifade edilmekte ve bu görüşün, kişisel verilerin işlenmesinde ana kuralın açık rıza verilmesi, istisnanın ise KVKK'nin 5. maddesinin ikinci fıkrası ile 6 ncı maddesinin üçüncü fıkrasında belirtilen durumların gerçekleşmesi olduğu hususu ile gerekçelendirildiği görülmektedir[94]. Gerçekten de kişisel verilerin işlenmesinde ana kuralın açık rıza olduğunun kabul edilmesi neticesinde, KVKK'de öngörülen diğer

[93] Aşıkoğlu, Şehriban İpek. 2018, Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, s.124-125.
[94] Küzeci, 2020: 375-376.

işleme şartlarının uygulanması bakımından istisna benzeri bir durum yaratılmış olmakta, böylesi bir durumda ise istisna konumunda görülen "kanunlarda öngörülme" şartının, yürürlükte bulunan pek çok düzenleme vesilesiyle uygulama alanının genişletilebileceği şeklinde bir sonuca ulaşılmaktadır. Kanaatimizce yukarıda ele alınan gerekçelerle, kanunda öngörülme şartının istisnai bir işleme şartı olarak değerlendirilmesi mümkün olamayacağından, genişletilmiş bir istisnanın varlığından da söz edilemeyecektir. Bununla birlikte konu, anılan işleme şartının bir istisna olarak değerlendirilmesinden ziyade; kişisel verinin işlenmemesinin ana kural olduğu kabulü doğrultusunda yürürlüğe giren KVKK'de öngörülen bir işleme şartı ile pek çok kanunun, işleme faaliyetine cevaz vermesine imkân tanınması açısından değerlendirilebilir. Kanaatimizce bu noktada, KVKK'nin kişisel verilerin korunması amacına hizmet eden çerçeve nitelikte bir kanun olduğunun ve pek çok kanuni düzenlemenin, kişisel verilerin işlenmesini gerektirebileceğinin göz ardı edilmemesi gerekmektedir. Nitekim öngördükleri hükümlerle kişisel verilerin işlenmesini açıkça öngören ya da bunu gerektiren kanuni düzenlemelerin hükmü genişlettiği şeklindeki bir kabul, hukuk sistemi içerisinde birçok kanuni düzenlemenin fiilen uygulanmasını imkânsız kılabileceği gibi kişisel verilerin işlenmesini gerektiren telekomünikasyon, bankacılık, sigortacılık gibi pek çok sektörü de zora sokabilecek niteliktedir. Konu bu yönüyle ve uluslararası boyutu ile ele alındığında mezkûr işleme şartının, uygulama alanını genişletmekten ziyade kişisel verilerin, gerçekten işlenmesi gereken durumlar bakımından bir sınır çizebilme amacına hizmet ettiği değerlendirilebilecektir.

2.4.4.Fiili imkânsızlık veya rızaya geçerlilik tanınmayan hallerde veri işlemenin zorunlu olması

Kişisel verilerin işlenebilmesine imkân tanınan bir diğer hal; ilgili kişinin fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunduğu ya da rızasına hukuken geçerlilik tanınmadığı bir durumda, ilgili kişinin kendisinin yahut başka bir kişinin hayatının ya da beden bütünlüğünün korunabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesidir. Kişinin hayatının ya da beden bütünlüğünün korunması amacıyla veri işlemenin zorunluluk arz etmesi hali olarak özetlenebilecek bu durumda, kişinin fiilen rızasını açıklayamayacak durumda bulunması ya da rızasına yasal olarak geçerlilik tanınmıyor olması, bir şart olarak aranmaktadır. Bununla birlikte KVKK'de rızanın hangi hallerde fiili olarak açıklanmasının mümkün olmadığı ya da hangi hallerde rızanın geçerli olarak kabul edilmediği hakkında özel bir

belirlemeye gidilmediği görülmektedir. Bu bakımdan anılan hallerin tespitinde, konuya ilişkin temel çerçeveyi çizen TMK hükümlerinin[95] kıyasen uygulama alanı bulacağını söylemek mümkündür. Kişisel verilerin korunması bağlamında fiili imkânsızlık; kişisel verileri işlenen gerçek kişinin, normal şartlar altında verilerinin işlenmesine açık rıza vermeye ehil olduğu ve bu doğrultuda kendi iradesiyle rıza verebildiği; ancak o anda gerçekleşen hal ve koşullar sebebiyle açık rıza veremediği ya da rızasının bir şekilde alınamadığı durumların somut olayda var olması şeklinde yorumlanabilir. Diğer bir deyişle ilgili kişi; normalde sahip olduğu açık rıza verebilme kabiliyetini, içinde bulunduğu hal ve şartlar sebebiyle kullanamamakta, açık rıza veremediği için kişisel verileri işlenememekte ve bu durum kendisinin ya da üçüncü bir şahsın hayati menfaatlerini ya da beden bütünlüğünü tehdit etmektedir[96].

Hükmün gerekçesine bakıldığında, rızanın açıklanamadığı ya da geçerli olmadığı hallerde, kişilerin hayat veya beden bütünlüğünün korunması için kişisel verilerin işlenmesinin öngörüldüğü belirtilmektedir. Gerekçede, kişinin şuurunun yerinde olmadığı veya akıl hastası olması sebebiyle rızasının geçerli olmadığı bir durumda, hayat veya beden bütünlüğünün korunması amacıyla, tıbbi müdahale sırasında kişisel verilerinin işlenebileceği; bu bağlamda kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar gibi verilerin, ilgili sağlık sistemi üzerinden işlenebileceği; yine hürriyeti tahdit edilen bir kişinin kurtarılması amacıyla, kendisinin veya şüphelinin taşımakta olduğu telefon, bilgisayar, kredi kartı, banka kartı veya diğer teknik bir araç üzerinden yerinin belirlenmesi için bu verilerin işlenebileceği örnek nev'inden gösterilmektedir. Madde gerekçesinde yer alan örnekler değerlendirildiğinde, verilen örneklerin sağlık verilerinin işlenmesi üzerine temellendiği dikkati çekmektedir. Bununla birlikte anılan işleme şartı, KVKK'nin 5. maddesinde düzenleme konusu edilerek, ayrı bir veri kategorisi olarak öngörülen ve farklı işleme şartlarına tabi olan özel nitelikli kişisel verileri dışlamaktadır. Başka bir ifade ile, özel nitelikli kişisel veriler ve bunların hangi hallerde işlenebileceği KVKK'nin 6. maddesinde özel olarak

[95] 4721 Sayılı Türk Medeni Kanunu
II. Saldırıya karşı / 1. İlke
Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.
[96] Badur, Emel. 2017, Tıbbi Müdahaleye Rızanın Özellik Gösterdiği Haller

ele alındığından, 5. maddede düzenlenen işleme şartlarının, kıyasen özel nitelikli kişisel veri kategorileri bakımından uygulanması mümkün değildir.

Gerekçe metninde yer verilen örnek ile, kişinin sağlığına ilişkin kişisel verilerin, 5. maddede düzenlenen bir işleme şartı bağlamında işlenebileceği şeklinde bir değerlendirme yapılmış olmaktadır. Bununla birlikte kanun sistematiği değerlendirildiğinde, kişisel veriler ile özel nitelikli kişisel verilerin işlenme şartlarının ayrı maddelerde düzenlendiği, bu kategoriler için ayrı işleme şartlarının öngörüldüğü, özellikle sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesinde daha özel bir korumanın söz konusu olduğu ve iki veri kategorisinin net çizgilerle birbirinden ayrıldığı dikkate alındığında; gerekçede belirtilen örneklerin, anılan işleme şartının sistematik itibarıyla yanlış yerde düzenlenmesinin bir sonucu olabileceği ya da kanun koyucunun hem kişisel veriler hem de özel nitelikli kişisel veriler açısından ayrı düzenlemeler yapmayı ihmal etmiş olabileceği sonucuna işaret etmektedir. Bu konuya ilişkin kanaatimiz, kanun koyucunun, hem kişisel veriler hem de özel nitelikli kişisel veriler bakımından anılan işleme şartına yer vermek niyetinde olduğu, bununla birlikte özel nitelikli kişisel verilerin işlenmesine ilişkin olarak düzenleme sevk edilmesinin ihmalen gerçekleştirilemediği yönündedir. Nitekim kanun koyucunun amacının, yalnızca kişisel verilerin işlenmesini sağlamak olduğu varsayımında sağlık verilerinin işlenmesine işaret etmemesi gerekecek, yalnızca hayati menfaatlerin korunmasını sağlamak üzere sağlık verilerinin işlenmesini amaçlaması halinde ise anılan işleme şartının 6 ncı maddede düzenlenmesi ile bu amaca ulaşılabilecekti. KVKK'de yer alan düzenlemenin lafzi ifadesi, her ne kadar insan yaşamını tehdit eden durumlara ve buna bağlı olarak özel nitelikli kişisel verilerin işlenmesine yönelmekte ise de kanaatimizce hükmü, yalnızca insan yaşamını tehdit eden durumlar ve hassas veriler ile sınırlayıcı bir çerçevede değerlendirmek uygun olmayacaktır. Temel itibarıyla anılan görüş doğru olarak değerlendirilse de, her somut olay bakımından böyle bir kabul doğrultusunda ilerlemenin kişisel verilerin korunması bağlamında yanlış kabul ve sonuçlara yol açabileceğini de dikkate almak gerekmektedir. Bu nedenle hükmün, kişiliğe sıkı sıkıya bağlı olan ve kişinin maddi ve manevi varlığına tesir edebilecek niteliği bulunan temel hak ve özgürlüklere halel getirebilecek ve bu doğrultuda rıza vermesini engelleyebilecek türden saldırıları kapsayacak şekilde düzenlenmesi kanaatimizce daha uygun bir yaklaşım olacaktır.

Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması halinde kişisel verilerin işlenmesi durumu, öğretide bazı yazarlar tarafından "özel nitelikli üstün yarar" kavramı kapsamında değerlendirilmekte ve kişisel verilerin işlenmesi halinde ilgili kişinin bu konuda rızası bulunmasa dahi veri işleme faaliyetinin hukuka aykırılık teşkil etmeyeceği savunulmaktadır[97]. Ancak diğer bir görüş; hayati menfaatlerin varlığı halinde kişisel verilerin işlenmesinde kişinin imkânının olması halinde rıza vermesinin muhakkak olması gerektiği, bu nedenle kişinin sağlığına tekrar kavuştuğunda kendisinin somut rızasına başvurulması gerektiği; aksi takdirde yapılan işlemin hukuka aykırı olacağını belirtmektedir. Kanaatimizce KVKK'nin yapmış olduğu düzenleme ile anılan tartışma artık anlamını kaybetmiştir. Nitekim KVKK'nin 5. maddesi, kişisel verilerin işlenme şartlarını açıkça düzenlemiş ve madde kapsamında yer verilen şartlardan herhangi birinin somut olayda var olması halinde kişisel verilerin işlenmesini hukuka uygun kabul etmiştir. Fiili imkânsızlık halinin ortadan kalkması durumunda, yeniden açık rıza arayışına gidilmesi hukuki açıdan faydasız olduğu gibi kanunda yer verilen veri işleme şartları arasında da bir hiyerarşi olduğunu kabul etmek anlamını taşıyacaktır. Oysa 5. maddede düzenlenen veri işleme şartları bakımından bir üstünlük sıralaması öngörülmemiş; her bir veri işleme şartına eşit değer addedilmiştir. Bu nedenle kanaatimizce, anılan veri işleme şartına dayalı olarak kişisel verilerin işlenmesi halinde yeniden bir rıza arayışına girmeye gerek bulunmamaktadır.

Madde kapsamında düzenlenen diğer bir durum da ilgili kişinin rızasına hukuki geçerlilik tanınmaması halidir. Yukarıda detaylı olarak ele aldığımız açık rıza kavramı ve açık rızanın unsurları ile yakın ilişkisi bulunan bu hususta; açık rızanın geçerliliğine etki edebilecek yaş küçüklüğü, akıl hastalığı, akıl zayıflığı ile ayırt etme gücünü geçici veya sürekli olarak kaldıran diğer haller sebebiyle rıza geçersiz kılınabilecek ve böylesi bir durumda ilgili kişinin veya bir başkasının hayati menfaatlerinin ya da beden bütünlüğünün korunması için veri işlemenin zorunlu olması halinde, kişisel verilerin işlenmesinin hukuka uygun kabul edilecektir.

[97] Başar, Cemal. 2019, Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, s.60

2.4.5.Sözleşme ilişkisi çerçevesinde veri işlemenin gerekli olması

Sözleşme, tarafların karşılıklı ve uyumlu davranış biçimlerinden bir borç kaynağının doğduğu ilişkileri ifade etmektedir[98]. Sözleşme ilişkisi; alacaklı bakımından borcun ifası noktasında bir talep hakkının doğmasına, borçlu bakımından ise bir ifa yükümlülüğünün ortaya çıkmasına zemin hazırlamakta olup; KVKK m. 5/2 (c) uyarınca anılan hakkın kullanılması ya da borcun ifası, kişisel verilerin işlenmesi ile mümkün olmaktadır. Bu anlamda kanun koyucu, sözleşmenin kurulması ya da ifası ile doğrudan ilgili olan hususlarda, taraflara ait kişisel verilerin işlenmesine imkân tanıyarak bu durumda kişisel verilerin işlenmesini tarafların açık rızalarına bağlı olmaktan kurtarmış ve sözleşme ilişkisinin sekteye uğramasını engelleme amacı gütmüştür.

Sözleşme ilişkisi çerçevesinde genel kural, tarafların irade serbestisi olup; anılan işleme şartı bakımından taraflar arasında kurulan sözleşmenin niteliği de önem taşımaktadır. Nitekim bir sözleşme bakımından gerekli ya da zorunlu olarak değerlendirilen bir kişisel verinin, başka bir sözleşme türü bakımından da gerekli ya da zorunlu olduğunu söylemek her durumda mümkün değildir. Örneğin kişinin, örnek bir fotoğrafına dayalı olarak bir portre yaptırmak istemesi halinde fotoğraf, sözleşmenin ifası bakımından gerekli bir kişisel veri olarak değerlendirilebilecek iken, buzdolabı satın almak isteyen kişi bakımından bu verinin işlenmesinin gerektiği söylenemeyecektir. Hatta ifaya konu edimin niteliği dikkate alındığında aynı sözleşme türü içerisinde dahi işlenmesi gereken kişisel verilerin farklılık arz edebilmesi mümkündür. Bu bakımdan, söz konusu işleme şartının; somut sözleşme ilişkisinin dinamikleri göz önüne alınarak, sözleşmenin kurulması ya da ifası noktasında işlemenin gereklilik arz edip etmediğinin değerlendirilmesi önem taşımaktadır.

2.4.6.Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması

Veri sorumlularının, yapmış olduğu hukuki işlemler ile bağlantılı olarak ya da mevzuatta öngörülen düzenlemeler neticesinde bazı hukuki yükümlülüklerin muhatabı olması söz konusu olabilmektedir. Örneğin, 1136 sayılı Avukatlık Kanunu'nun 163. maddesi ve devamı hükümleri uyarınca kurulan bir vekâlet ilişkisi çerçevesinde avukatın, müvekkilinin haklarını korumak üzere gerçekleştireceği işlemler için

[98] Kılıçoğlu, Ahmet M. 2013, Borçlar Hukuku Genel Hükümler, s.52

müvekkiline ait kişisel verileri elde etmesi, mesleki sorumluluğunu yerine getirmesi bakımından zorunluluk arz etmektedir. Benzer şekilde 213 sayılı Vergi Usul Kanunu'nun 236. maddesi uyarınca serbest meslek erbapları, mesleki faaliyetlerine ilişkin olarak yapacağı her türlü tahsilat için serbest meslek makbuzu düzenlemekle yükümlü tutulmuş olup; Kanun'un 237. maddesinde söz konusu makbuzda müşterinin soyadı, adı veya unvanı ile adresinin bulunması gerektiği hüküm altına alınmıştır. Serbest meslek erbabı veri sorumlusunun, yapacağı tahsilata ilişkin olarak serbest meslek makbuzu düzenleyebilmesi için gerçek kişi müşteriye ait kişisel verileri işlemesi gerekecektir. Bu noktada belirtilmesi gereken husus; veri sorumlusunun tabi bulunduğu yükümlülüğün, veri sorumlusunun takdirine bırakılmamış olması gerektiğidir. Diğer bir deyişle veri sorumlusu, gerek hukuki ilişkinin niteliğinden kaynaklı olarak gerek kanun gerek ikincil düzenlemelerle, kendi isteği ya da iradesinden bağımsız olarak hukuken bir yükümlülüğün muhatabı haline getirilmiş olmalıdır. Bu bakımdan veri sorumlusunun hukuken bir yükümlülük altına girdiği ve bu yükümlülük neticesinde kişisel veri işleme faaliyetinde bulunması gereken durumlarda, anılan işleme şartına dayalı olarak kişisel verileri işlemesi mümkün olacaktır.

2.4.7.İlgili kişinin kendisi tarafından alenileştirilmiş olması

Kişisel verilerin korunması hukuku bağlamında alenileştirme, ilgili kişinin kişisel verilerinin herkesçe bilinebilecek bir hale getirilmesi olarak ifade edilebilir[99]. Kurum nezdinde alenileştirme ise "ilgili kişi tarafından kişisel verilerinin kamuoyuna açıklanması" şeklinde kullanılmaktadır. Bununla birlikte gerek KVKK'nin gerekçesinde gerek KVKK ve ikincil düzenlemelerde "alenileştirme" kavramı ile neyin kast edildiği, kamuoyundan ne anlaşılması gerektiği, verinin kamuoyuna açıklanmış olması ve bu anlamda alenileştiğinin kabul edilebilmesi için verinin, kaç kişilik bir kitleye açıklanmasının gerektiği gibi hususlar başta olmak üzere, anılan veri işleme şartının çerçevesinin oluşturulmasına yönelik bir belirlemeye gidilmediği görülmektedir. Diğer taraftan Kurul uygulamasında, verilen kararlar ile alenileştirmeye ilişkin daha fazla detay içeren açıklamaların yapıldığı ve bu anlamda konunun, Kurul uygulaması ile şekillendirildiği anlaşılmaktadır.

[99] Küzeci, 2020: 398.

Kurum tarafından yayımlanan 16.12.2020 tarihli kamuoyu duyurusunda alenileştirmenin, ilgili kişinin kişisel verilerinin kendisi tarafından kamuoyuna açıklanması anlamına geldiğinden söz edilerek, alenileştirmenin, ilgili kişinin alenileştirme iradesi ve amacı ile bağlantısına dikkat çekilmiş ve herhangi bir açıklamanın ya da herhangi bir şekilde kişisel verinin kamuoyuna açık hale gelmesinin, KVKK kapsamında alenileştirme olarak kabul edilemeyeceği vurgulanmıştır[100]. Anılan ifadeden öncelikle, ilgili kişinin alenileştirmenin gerçekleşmesine yönelmiş bir iradesinin bulunması ve bu iradenin, kişinin alenileştirmedeki amacı ile bağlantılı olması gerektiği anlaşılmaktadır. Bu bakımdan alenileştirme, ilgili kişilerin, hangi amaçlar ile kişisel verilerini kamuoyuna açıkladıklarının önceden belirlenmiş olmasını gerektirmekte olup; ilgili kişilerin belirledikleri bu amaca aykırı şekilde gerçekleştirilecek işleme faaliyetleri, anılan işleme şartı kapsamında değerlendirilemeyecektir. Diğer taraftan ilgili kişilerin, belirledikleri amaç ya da amaçlar doğrultusunda kişisel verilerinin kamuoyuna açıklanması yönünde bir iradeye sahip olmaları ve bu irade doğrultusunda verinin kamuoyuna sunulması da gerekmektedir. Verinin kamuoyuna açıklanmasında ilgili kişi iradesinin dışında faktörlerin rol oynadığı durumlarda, verinin ilgili kişinin hür iradesi ile açıklandığı söylenemeyeceğinden KVKK anlamında bir alenileştirmeden de söz edilemeyecektir.

Bu açıklamalardan yola çıkılarak alenileştirmenin; ilgili kişinin kişisel verilerini, belirlemiş olduğu amaç ya da amaçlar doğrultusunda ve bu amaçların gerçekleştirilebilmesini teminen, kendi iradesiyle, amaç ile bağlantı içerisinde olan kişilerin erişimine açık halde bulundurması olarak ifade edilmesi mümkündür. İlgili kişinin belirlemiş olduğu amaç doğrultusunda kişisel verilerini alenileştirmesi ve bu amaçlar doğrultusunda kişisel veri işleme faaliyetinin gerçekleştirilmesi halinde, işleme faaliyeti hukuka uygun; bu amacı aşan ya da bu amaçtan başka amaçlarla işleme faaliyetinin gerçekleştirilmesi halinde ise alenileştirme iradesinin başka bir amaca yönelmesi sebebiyle faaliyet, hukuka aykırı olarak kabul edilecektir. Bu yaklaşım, yukarıda ele almış olduğumuz işleme faaliyetinin amaç ile bağlantılı, sınırlı ve ölçülü olması ilkesi ile de uyum içerisinde olup; ilgili kişinin, farklı amaçlarla kişisel verilerinin işlenmesine ve suistimallerin gerçekleşmesine engel oluşturabilecek niteliktedir.

[100] Aşıkoğlu, 2018: 133.

2.4.8.Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması

Hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması sebebiyle kişisel verilerin işlenmesi; öncelikle hakkın müstakbel sahibi ya da hak sahibi olarak hakkı kullanacak yahut hakkın korunması için talepte bulunabilecek konumda olan kişinin, belli bir hak ile ilişki içerisinde olmasını gerektirmektedir. Bu konuda kanun koyucunun, özel bir belirlemede bulunmadığı; diğer bir ifade ile hakkın türüne ilişkin bir sınırlamaya gitmediği anlaşılmaktadır. KVKK'nin beşinci maddesinin gerekçesinde de anılan düzenlemeye ilişkin olarak "bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması" ve "kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması" örnekleri verilerek, mezkûr şart kapsamında bir işleme faaliyeti gerçekleştirilebilmesi için öncelikle meri mevzuat kapsamında bir hak ile ilişki içerisinde bulunulması gerektiği vurgulanmıştır. Buna ek olarak ilgili kişinin, kendisine belirli bir hak tesis edilecek olan ya da bu hakkın sahibi olarak hakkı ya da hakkın korunmasına ilişkin yolları kullanabilecek bir kişi olması gerekmektedir. Hakkın tesisi; esasen belli bir hakka henüz sahip olmayan kimsenin, yasal ya da iradi işlemler neticesinde ya da mevzuat gereği belli bir hakka sahip olabilmesi olarak ifade edilecek olursa, ilgili kişinin, bu hakkın sahibi olabilmesi adına kişisel verilerinin işlenmesi halinde, işleme faaliyetinin hukuka uygun şekilde gerçekleştiği söylenebilecektir.

Bu noktada, hakkın tesisinin iradi ya da yasal bir işlem ile gerçekleşmesi halinde, sözleşmenin kurulması ya da ifası bakımından veri işlemenin zorunlu olması ya da kanunlarda öngörülme başta olmak üzere, hakkın tesisi/kullanılması/korunması işleme şartının, diğer işleme şartları ile birleşme durumuna değinmek gerekir. Yukarıda da belirtildiği üzere somut olaylar bağlamında bir işleme şartının, başka bir işleme şartı ya da birden fazla işleme şartı ile birleşebilmesi imkân dâhilindedir. Kişisel veri işleme faaliyetinin, birden fazla işleme şartına dayanması, işleme faaliyetinin KVKK hükümleri bağlamında birden fazla dayanağının olması anlamına gelmekte olup; bu durumun gerçekleşmesine yasal anlamda bir engel bulunmamaktadır. Böylesi bir durumda önem arz eden husus, diğer işleme şartları var iken açık rızaya başvurulmamasıdır.

Hakkın kullanılması ve korunması ise, yukarıda da belirtildiği üzere öncelikle hak sahipliğini gerektirmekte olup; söz konusu hakkı korumak ya da bu hakkı kullanmak üzere kişisel verilerin işlenmesinin gerektiği durumlarda veri işleme faaliyeti hukuka uygun olacaktır. Bu kapsamda, örneğin nama yazılı bir senedin hamili olan kişi; senet, kendi namına yazılmamış ise hangi hukuki sebep ile senedin şahsına devredildiğini ispatlamak mecburiyetinde bulunmaktadır. Bu anlamda nama yazılı senedin sahibinin, söz konusu hakkını ispatlamak ve senedi tahsil edebilmek, yani hakkını kullanabilmek amacıyla senet devrini ispatlayan ve kişisel veriler içeren devre ilişkin sözleşmeyi, anılan işleme şartına dayalı olarak sunabileceğini söylemek mümkün olacaktır.

2.4.9.İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

Kişisel Verilerin Korunması Kanunu'nun 5. maddesi uyarınca işleme faaliyetinin gerçekleştirilebileceği son hal, veri sorumlusunun meşru menfaatleri uyarınca işlemenin zorunluluk arz etmesidir. Bu veri işleme şartında, veri sorumlusunun meşru menfaatlerine bir sınır çizilerek, meşru menfaatlerin ilgili kişilerin temel hak ve özgürlüklerine zarar veremeyeceği açık hüküm altına alınmıştır. Bununla birlikte meşru menfaat kavramının belirsizliği ve sınırlarının net şekilde tayin edilebilmesinin zorluğu, anılan veri işleme şartının uygulanmasında sorunlara yol açabilecek niteliktedir. Olası sorunların önüne geçilebilmesi ve şartın doğru şekilde anlaşılabilmesi bakımından Kurul'un söz konusu şarta bakış açısı ve somut başvurular bağlamında meşru menfaat kavramını ne şekilde yorumladığının anlaşılmasının önemli olduğu değerlendirilmektedir.

Kurum tarafından yayımlanan Uygulama Rehberi'nde; veri sorumlusunun meşru menfaatinin, gerçekleştirilecek işleme faaliyeti neticesinde elde edilecek çıkar ve faydaya yönelik olduğu, bu faydanın meşru olmasının yanı sıra ilgili kişinin temel hak ve özgürlükleri ile yarışabilecek düzeyde etkin, belirli ve hâlihazırda mevcut olması gerektiği, ayrıca veri sorumlusunun gerçekleştirdiği güncel aktiviteler ile ilişkili ve yakın gelecekte fayda sağlayabilecek nitelikte olması gerektiği belirtilmiştir. Bu noktada veri sorumlusunun meşru menfaatinin, KVKK'nin amaç ve ruhuna uygun olarak yorumlanması gerektiği belirtilerek öncelikle veri sorumlusunun meşru bir menfaati olup olmadığının tespit edilmesi gerektiği, akabinde ilgili kişinin temel hak ve özgürlüklerinin neler olduğu belirlenerek veri sorumlusunun meşru menfaati ile

ilgili kişinin temel hak ve özgürlükleri arasında bir denge testi yapılması gerektiği ifade edilmektedir[101].

Kurul'un konuya ilişkin olarak yayımlamış olduğu 25/03/2019 tarihli ve 2019/78 sayılı kararında[102], petrol piyasasında dağıtıcı lisansı ile faaliyet gösteren bir şirketin, satış hareketlerini sorgulama imkânı sağlayan, araç plakası ile yakıt türü eşleştirilmek suretiyle hatalı yakıt verilmesini engellemeyi amaçlayan, şirketin anlık erişimine açık bir otomasyon sistemi kapsamında işleme faaliyetinde bulunulmasının, veri sorumlusunun meşru menfaati çerçevesinde değerlendirilip değerlendirilemeyeceği konu edilmiştir. Başvuruya ilişkin olarak Kurul, meşru menfaat kapsamında bir işleme faaliyetinin söz konusu olabilmesi için bazı kriterler ortaya koymuştur. Bu kriterler; "kişisel verinin işlenmesi sonucunda elde edilecek menfaatin, ilgili kişinin temel hak ve hürriyetleri ile yarışabilir düzeyde olması ve söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi", "meşru menfaatin hâlihazırda mevcut, belirli ve açık olması", "meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması", "meşru menfaat ile beklenen yararın, çok sayıda kişiyi etkilemesi, yalnızca ekonomik yarara yönelik olmaması, söz konusu yararların tespitinde şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması", "ilgili kişinin, temel hak ve hürriyetlerinin zarar görmesini engellemek amacıyla öngörülebilir, açık ve yakın her türlü tehlikeden uzak tutulması", "kişisel verilerin bir veri kayıt sisteminde, amaçla sınırlı olarak hukuka uygun işleyişinin temini ile zararı ve ihlalleri engellemek için her türlü teknik ve idari tedbirin alınması", "kişisel verilerin işlenmesinde genel ilkelere uygunluğun sağlanması" ve "kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması" olarak ifade edilmiştir. Başvuru konusu bakımından ise ilgili araca, talep edilen dışında bir yakıt verilmesinin araç arızalarına yol açabileceği ve bu durumun tüketici aleyhine zarar oluşturabileceği, bu zararların tazmini bakımından dağıtıcı şirketin de işletici ile müteselsilen sorumlu tutulacağı gerekçe gösterilerek dağıtıcı şirketin, söz konusu sistemin kurulması ve sistem içerisinde kişisel verileri işlemesinde meşru menfaati bulunduğuna karar verilmiştir.

[101] Kişisel Verileri Koruma Kurumu, 2019: 78.
[102] https://www.kvkk.gov.tr/Icerik/5434/2019-78

Kişisel Verileri Koruma Kurulunun 11/02/2020 tarihli ve 2020/108 sayılı kararı[103] uyarınca, ilgili kişinin eski işvereni tarafından, yeni işverenine veri aktarımında bulunulduğu iddiası ile Kurul'a yapılan bir diğer başvuruda ise başvuruya; yeni işveren konumunda bulunan şirketin kurumsal hesabından, ilgili kişi ile çalışılmaya başlandığının duyurulması ve bu duyuruda, ilgili kişinin çalıştığı eski pozisyonu ile ilgili olarak yanlış bilgilerin yer aldığını eski işverenin fark etmesi üzerine, eski işveren tarafından ilgili kişinin hangi tarihler arasında hangi iş pozisyonunda çalıştığı ve ilgili kişinin işten ayrılma nedenine ilişkin bir e-posta gönderilmesi konu edilmiştir. Konuya ilişkin olarak Kurul; aktarımın sınırlı bilgilere ilişkin olarak yapıldığını belirterek, işverenlerin yanlış bilgi verilmek suretiyle yanıltılması ve veri sorumlusu tarafından gerçeği yansıtmayan bilgilerin düzeltilmesinin, kişinin makul beklentisine aykırı olup olmadığı, temel hak ve hürriyetlerini ihlal edip etmediği ve yeni işverenin yanıltılması sebebiyle iş mevzuatından kaynaklı hakların kullanılabilmesi hususlarını da incelemiş ve söz konusu aktarım faaliyetinin, veri sorumlusunun meşru menfaati kapsamında işlendiğinin kabul edilebileceğine karar vermiştir.

Söz konusu kararlardan da görüleceği üzere veri sorumlusunun meşru menfaati uyarınca kişisel verilerin işlenmesi; veri sorumlusunun her türlü menfaati olarak değerlendirilmesi mümkün olmayan, daha dar çerçevede ve ilgili kişinin temel hak ve özgürlükleri ile yarışabilecek düzeyde ciddi, somut olay bağlamında incelenmesi ve değerlendirilmesi gereken, buna bağlı olarak da diğer veri işleme şartlarına nazaran daha hassas bir değerlendirmeyi gerektiren bir işleme şartı olarak öngörülmüştür. Bu bakımdan anılan işleme şartına dayalı olarak kişisel veri işleme faaliyetinde bulunulmasında ilgili kişi ve veri sorumlusunun menfaatleri arasındaki dengenin hassasiyetle değerlendirilmesi ve diğer işleme şartlarına gidilemediği durumlarda kişisel verilerin işlenebileceği torba bir işleme şartı olarak görülmemesi kanaatimizce önem arz etmektedir.

2.4.10.Özel nitelikli kişisel verilerin işlenme şartları

Kişisel Verilerin Korunması Kanunu, bazı kişisel verileri, yukarıda detaylı şekilde ele almış olduğumuz kişisel verilerden ayırarak, bu veri türleri için özel işleme şartları öngörmüş ve bunları özel bir korumaya tabi tutmuştur. "Özel nitelikli" olarak ifade edilen kategorilere dâhil veriler, esas itibarıyla, öğrenilmesi halinde ilgili kişinin

[103] https://www.kvkk.gov.tr/Icerik/6921/2020-108

mağdur olmasına ya da ayrımcılığa maruz kalmasına sebep olabilecek niteliğe sahip bulunmakta ve bu itibarla daha hassas ve sıkı bir korumayı gerektirmektedir[104].

Kanun koyucu, bu verileri; kişinin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi ya da diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri olarak, sınırlı sayım ilkesi doğrultusunda belirlemiştir.

Özel nitelikli kişisel verilerin işlenmesi de, özel niteliği bulunmayan kişisel verilerin işlenmesinde olduğu gibi bazı şartlara tabi tutulmuştur. Bu şartların belirlenmesinde kanun koyucunun, özel nitelikli kişisel verinin türüne göre bir ayrıma gittiği göze çarpmaktadır. Bu şartlara değinmeden önce, tüm özel nitelikli kişisel veri türleri bakımından açık rızanın bir işleme şartı olarak öngörüldüğünü belirtmek gerekmektedir. Bununla birlikte açık rızanın bulunmadığı bazı durumlarda da verinin işlenmesi gerekebileceğinden yola çıkılarak farklı işleme şartları da öngörülmüştür. Bu işleme şartları; sağlık ve cinsel hayata ilişkin veriler ile diğer özel nitelikli kişisel veriler arasında farklılık göstermekte olup; sağlık ve cinsel hayat dışında kalan özel nitelikli kişisel veriler için kanunlarda öngörülme halinde işlemeye cevaz verilebileceği, sağlık ve cinsel hayata ilişkin verilerin ise; kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amaçları ile sınırlı olmak kaydıyla, sır saklama yükümlülüğü altında bulunan kişiler ya da yetkili kurum ve kuruluşlar tarafından açık rıza bulunmaksızın işlenebileceği hüküm altına alınmıştır[105].

Özel nitelikli kişisel verilerin de işleme şartları arasında bulunan açık rıza hakkında detaylı incelemeler, yukarıda ayrıntılı şekilde açıklandığından bu bölümde ayrıca değerlendirme konusu edilmeyecektir. Yine "kanunda öngörülme" hususuna ilişkin olarak, yukarıda yapılan açıklamalara yollamada bulunmakla yetineceğiz. Bununla

---

[104] Kişisel Verileri Koruma Kurumu, 2019: 80.

[105] 6698 Sayılı Kişisel Verilerin Korunması Kanunu
Özel nitelikli kişisel verilerin işlenme şartları
…
MADDE 6/3 Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. 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.

birlikte "kanunlarda öngörülme" hususunda, 5. madde düzenlemesinden farklı olarak, özel nitelikli kişisel verilerin işleme şartlarını düzenleyen 6. maddede "açıklık" unsuruna yer verilmemiş olması dikkati çekmektedir. KVKK'nin tasarı metninin gerekçesine bakıldığında, "...kanunlarda açıkça öngörülen hallerde özel nitelikli kişisel veriler işlenebilecektir." ifadesine yer verildiği görülmekte ise de söz konusu unsura, gerekçe metninde yer verilmesinin özel bir anlamının olmadığı, söz konusu farklılığın bir ihmal sonucu ortaya çıkarıldığı kanaatindeyiz[106].

Sağlık ve cinsel hayata ilişkin verilerin işlenebileceğinin belirtildiği dört başlığa bakıldığında, belirtilen hallerin "kamu sağlığı", "koruyucu hekimlik", "tıbbi bakım", "sağlık hizmeti/finansmanının planlanması/yönetimi" gibi sınırları kolayca tespit etmenin mümkün olmadığı hallerin öngörüldüğü göze çarpmaktadır. Temel itibarıyla, bu durumlardan kamu sağlığının; sağlığın toplum genelinde geliştirilmesi ve hastalıkların önlenmesini sağlama adına yapılan faaliyetleri, koruyucu hekimliğin ise hastalıkların meydana gelmemesi için gerekli önlemlerin alınması, bulaşıcı hastalıklarla mücadele, hastalık sonrası rehabilitasyon gibi konularda yürütülen hekimlik faaliyetlerini ifade ettiği söylenebilir. Bireyde var olduğu düşünülen fiziksel ya da psikolojik bir rahatsızlığın olup olmadığını anlama, var ise bu rahatsızlığın ne olduğunu bulma amacıyla tıp bilimine uygun şekilde gerçekleştirilen faaliyetler ise teşhis; hastalığın iyileştirilmesi, hafifletilmesi veya ortadan kaldırılması süreci ile bu kapsamda gerçekleştirilen tıbbi, cerrahi ve psikolojik faaliyetler ise tedavi olarak nitelendirilmekte ve tedavi sürecinin, bakım evresini de kapsadığı kabul edilmektedir. Sayılan amaçlar doğrultusunda gerçekleştirilen faaliyetlerin, özel nitelikli kişisel verilerin işlenmesini gerektirdiği hallerde, söz konusu işleme faaliyetinin hukuka uygun olacağını söylemek mümkün olacaktır. Benzer şekilde, bireyi hastalığın finansal yükünden korumak amacıyla, sağlık hizmetlerinin maliyetlerinin karşılanabilmesi için gerekli kaynakların yaratılması olarak ifade edebileceğimiz sağlık finansmanını planlamak yahut yönetmek için özel nitelikli kişisel verilerin işlenmesinin gerektiği hallerde de işleme faaliyeti hukuka uygun olacaktır. Bununla birlikte söz konusu işleme faaliyetinin, sır saklama yükümlülüğü altında bulunan kimselerce gerçekleştirilmesi gerektiği hüküm altına alınmış olup, mevzuatımızda "sır

[106] Özkök Gökmen, Başak. 2020, Patent hakkının sınırları ve istisnaları (kamu sağlığı gerekçesi özelinde incelenmesi), s.127-128.

saklama" yükümlülüğü altında bulunan kişilerce ve yukarıda ifade edilen amaçlarla özel nitelikli kişisel verilerin işlenmesi, KVKK uyarınca hukuka uygun olacaktır[107].

2.5.Kişisel Verilerin Hukuka Aykırı İşlenmesinin Kişisel Verilerin Korunması Kanunu Bakımından Sonuçları

Kişisel Verilerin Korunması Kanunu hükümleri uyarınca, bir işleme faaliyetinin hangi durumlarda kanuna uygun olacağı, yukarıda ele alınmıştı. Anılan hükümlere aykırı şekilde gerçekleşen bir işleme faaliyeti kanuna aykırılık arz etmekte ve hukuk sistemi tarafından müsamaha görmemektedir. KVKK'nin 5 ve 6. maddelerinde düzenleme altına alınan işleme şartları, "sınırlı sayım" ilkesi doğrultusunda ele alındığından, buradan ulaşılacak sonuç, ancak kanunda sayılan hallerde işlemenin yasal temele dayandırılabileceğidir. Bunun tersinden çıkan anlam ise, kişisel veri işleme faaliyetinin kural olarak hukuka aykırı bir faaliyet olduğu; ancak KVKK'de gösterilen hallerden birinin bulunması halinde hukuka aykırı bu faaliyetin hukuka uygun hale gelebileceğidir[108].

Kişisel verilerin işlenmesi faaliyetinin hukuken ne şekilde değerlendirileceği önemli bir soru olarak karşımıza çıkmaktadır. Zira kişisel verilerin korunmasını isteme hakkı, belli yönleriyle özel hukuku belli yönleriyle de kamu hukukunu ilgilendirmekte olup; bu anlamda birçok kavram ve hukuki müessese ile iç içe bulunmaktadır. Özel hukuka ve kamu hukukuna dair, birbirinden bağımsız görünen bu kavramlar; temelde "insan hakkı"na vurgu yapmaktadır. Bununla birlikte bu durum, yalnızca hakkın hukuki niteliğini açıklayabilmekte, konumuz açısından önemi olduğunu değerlendirdiğimiz kişisel veri işleme faaliyetinin hukuki niteliğini ise tek başına açıklayamamaktadır. Oysa çalışmanın ana konusunu teşkil eden ve işleme şartları arasında yer alan açık rızanın ve buna bağlı olarak açık rıza verebilme ehliyetinin tespit edilebilmesi, öncelikli olarak kişisel veri işleme faaliyetinin hukuki niteliğinin değerlendirilmesini gerektirmektedir.

Kişilik hakkı, insan hakları kavramı ile sosyal devlet akımının ürünü yeni bir haktır. Bu hak; klasik ayni haklar ve alacak hakları gibi malvarlıksal kavramlar yerine, doğrudan doğruya insanın maddi ve manevi varlığını ilgilendirmesi sebebiyle ayrı bir

[107] Basan, Nuri Mehmet ve Bilir, Nazmi. 2016, Koruyucu sağlık hizmetlerinde önleme çelişkisi ve nedenleri. TAF Preventive Medicine Bulletin, 15 (1), s.45.
[108] Avcı Braun, Cihan. "Kişisel Verilerin İşlenmesinde Rıza", YÜHFD, C.XV, 2018/1, s.15.

öneme sahiptir. Bu anlamda kişilik hakkı; bireyi birey kılan, kişinin kişiliğini oluşturan ve bu itibarla korumaya değer görülen, başta yaşam hakkı olmak üzere kişinin bedensel ve ruhsal bütünlüğü, cinsel dokunulmazlığı, sağlığı, onuru, saygınlığı, özel yaşamının gizliliği, özgürlüğü, sözleri, resmi, ismi gibi insana ait, bireysel ve kişisel değerleri konu edinmektedir. Yukarıda bazı örnekleri verilen bu hakların, ihlal edilmesine ilişkin risk arttıkça kişiliği koruyan düzenlemelerin ve bireylere tanınan hakların da sayısı artmakta, kişilik haklarına dâhil değerler de genişlemektedir. Bu bakımdan temel hak ve özgürlükler de kişilik hakkı kavramına dâhil değerler olarak karşımıza çıkmaktadır[109].

Anayasa'nın "Temel hak ve hürriyetlerin niteliği" başlıklı 12. maddesinde herkesin kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahip olduğu; bu temel hak ve hürriyetlerin, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva ettiği belirtilmiştir. Takip eden 13. maddede ise "temel hak ve hürriyetlerin; özlerine dokunulmaksızın yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği", "bu sınırlamaların, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeni ve lâik Cumhuriyetin gerekleri ile ölçülülük ilkesine aykırı olamayacağı" vurgulanmıştır. Bahsi geçen Anayasa hükümlerinden; temel hak ve özgürlüklerin bireyin kişiliğine bağlı değerler olarak devlete "dokunmama" ödevi yüklediği, bu özgürlüklerin, belli şartlar dâhilinde ve ancak "kanun" şeklinde mevzuata dâhil edilen normlarla sınırlandırılabileceği; bu itibarla Anayasal teminat altında bulunan hakların özel bir korumaya tabi tutulduğu anlaşılmaktadır. Anılan temel haklar arasında yer alan kişisel verilerin korunmasını isteme hakkı, Anayasa'nın "Temel Hak ve Ödevler" başlığını taşıyan ikinci kısmının, "Kişinin hakları ve ödevleri" bahsinde, "Özel hayatın gizliliği" başlığı altında ele alınmış; bu itibarla "negatif statü hakkı" olarak da ifade edilen ve kişinin devlet tarafından aşılamayacak ve dokunulamayacak özel alanının sınırlarını çizen, kişiyi devlete ve topluma karşı koruyan aynı zamanda devlete karışmama ödevi yükleyen bir hak olarak öngörülmüştür[110]. Anayasa'nın 20. maddesinin son fıkrasında yer alan "Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü uyarınca çıkarılan KVKK, bu amacın gerçekleştirilmesine hizmet ederek

[109] Serozan, Rona, 2018, Medeni hukuk- Genel bölüm/ Kişiler hukuku (8. Bası), İstanbul: Vedat Kitapçılık. s.454
[110] Tunç, Hasan. 2019, Anayasa Hukuku Genel Esaslar, s.212.

kişisel verilerin korunması hukuku alanına ilişkin temel çerçeveyi çizmekte ve konuya ilişkin genel bir kanun niteliği taşımaktadır.

Yukarıda değinildiği üzere kişisel verilerin korunmasını isteme hakkının, Kıta Avrupası hukuk sistemlerinde kişilik hakkı alanına dâhil olduğunun kabul edilmesi sebebiyle; hukuka aykırı bir işleme faaliyetinin gerçekleştirilmesi, aynı zamanda kişilik hakkının da ihlal edilmesi anlamını taşıyacaktır. Kişilik hakkının ihlal edilmesi durumuna ilişkin olarak ise hukukumuzun farklı alanlarında, ihlalin tespiti ya da giderilmesine ilişkin farklı mekanizmalar öngörülmekte olup; KVKK'de de kişilik hakkının ihlaline ilişkin hükümlere yer verildiği görülmektedir. Bu düzenlemelere değinmeden önce, KVKK'de yer alan ve kişisel verilerin işlenmesine ilişkin olarak öngörülen hükümlerin ihlali halinde, Kanun'un 17 ve 18. maddeleri gereğince veri sorumluları bakımından idari ve cezai sorumluluk doğacağının açık hükme bağlandığını belirtmek gerekmektedir. Bununla birlikte KVKK hükümlerinin ihlal edilmesi suretiyle bir kişisel veri işleme faaliyetinin gerçekleştirilmesi halinde özel hukuk bağlamında sorumluluğun ne olacağına ilişkin ayrı bir düzenlemeye yer verilmediği; yalnızca mezkûr kanunun "İlgili kişinin hakları" başlıklı 11. maddesi [111]ile "Kurula şikâyet" başlıklı 14. maddesinin üçüncü fıkrasında[112], kişilik haklarının ihlali halinde genel hükümlere göre tazminat haklarının saklı kalacağına ilişkin bir düzenlemeye yer verilerek genel hükümlere göndermede bulunulduğu dikkati çekmektedir. Konuya ilişkin olarak, gerek mehaz düzenleme olan Direktifte gerek GVKT'de sorumluluğa ilişkin daha detay düzenlemelere yer verildiği görülmektedir.

Veri sorumlusunun tazminat yükümlülüğü, Direktifin 55 numaralı gerekçesi ile 23. maddesinde düzenlenmekte idi. 55 numaralı gerekçede; veri sorumlularının, ilgili kişi haklarını ihlal ettiği durumlara ilişkin olarak yerel mevzuatta bir yargı yolu sağlanması gerektiği, aynı zamanda, veri sorumlusunun bu zararı tazmin edeceği, bununla birlikte zararın ortaya çıkmasında kusurun ilgili kişiye ait olduğu ya da mücbir sebeplerin bulunduğu hallerde veri sorumlusunun sorumluluktan kurtulabileceği düzenleme

---

[111] *İlgili kişinin hakları*
MADDE 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;
…
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

[112] *Kurula şikâyet*
MADDE 14-
…
(3) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır.

altına alınmakta idi. Benzer şekilde Direktifin 23. maddesinde, Direktif uyarınca kabul edilen iç hukuk düzenlemelerinde yer alan hükümlerle bağdaşmayan ya da yasa dışı mahiyeti bulunan bir işleme faaliyetinin gerçekleşmesi durumunda zarara uğrayan kişinin veri sorumlusundan tazminat isteme hakkı bulunduğu, veri sorumlusunun zarara yol açan olaylarda sorumlu olmadığını kanıtlaması halinde ise bu yükümlülüğün kısmen ya da tamamen kalkabileceği belirtilmişti.

Mülga Direktifte belirtilen hususlar, GVKT'nin 146 numaralı gerekçesi ile 82. maddesinde ele alınmaktadır. Direktiften farklı olarak GVKT'nin 146 numaralı gerekçesinde veri sorumlularının yanı sıra veri işleyenlerin de tazminatın tamamı bakımından sorumlu olacağına ve rücu ilişkisine ilişkin düzenlemeye yer verilmiş, zarar kavramının Adalet Divanı içtihatları doğrultusunda geniş bir şekilde yorumlanması gerektiğine değinilmiş, tazminat davası bakımından mahkemelerin hükmedecekleri tazminatı, sorumluluklarına göre veri sorumlusu ve veri işleyen arasında paylaştırabileceği ifade edilmiştir. 82. maddede ise veri işleyenlerin sorumluluklarına ilişkin daha detay bir düzenlemeye yer verilerek veri işleyenlerin, GVKT ile kendilerine yüklenen sorumluluk ve yükümlülüklerine uyum göstermediği ya da veri sorumlusunun hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde sorumlu olacağı belirtilmiştir.

Kişisel Verilerin Korunması Kanunu'nda ise konuya ilişkin özel bir düzenlemenin bulunmadığı, 11 ve 14. maddelerde "zararın giderilmesi" ve "tazmin yükümlülüğü"ne atıfta bulunulmakla yetinildiği ve bu yönüyle düzenlemenin Direktif ve GVKT'den önemli ölçüde ayrıldığı görülmektedir. Bununla birlikte İsviçre'de yürürlükte bulunan "Veri Korunmasına İlişkin Federal Yasa"da da KVKK'ye benzer şekilde kişiliğin korunmasına ilişkin Medeni Kanun hükümlerine gönderme yapılmaktadır[113]. KVKK'de yer alan hükümlerin ilgili kısımlarında[114] da görüleceği üzere KVKK'nin 11 ve 14. maddelerinde yalnızca tazminattan ve zararın tazmininden söz edilmekte; tazminin dayanağının ne olduğuna ya da biçimine ilişkin herhangi bir hükme yer verilmemektedir. Kanaatimizce konuya ilişkin özel bir düzenlemeye KVKK'de yer

[113] Gürpınar, Damla. 2017, Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk, s.688)

[114] *"İlgili kişinin hakları*
MADDE 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;
(...)
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."
"Kurula şikâyet MADDE 14- (...)
(3) Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır."

verilmeyerek, söz konusu tazmin yükümlülüğünün özel hukuk uyarınca öngörülen genel hükümler doğrultusunda sağlanacağı değerlendirilmelidir. Bu noktada ise sorumluluğun hangi hükümlere dayandırılacağının belirlenmesi gerekecektir. Hukukumuzda kişilik haklarının ihlalinde tazminat yükümlülüğünü düzenleyen iki ana düzenlemenin bulunduğu görülmektedir. Bu düzenlemeler ise TMK'nin 24 ve 25.[115] maddeleri ile TBK'nin 58.[116] maddesi ile belirlenen hükümlerdir. O halde kişisel verilerin işlenmesi esnasında gerçekleşecek ihlal durumlarında KVKK'nin 11 ve 14. maddeleri bağlamında öngörülen tazmin sorumluluğunun dayanağını TMK m. 24-25 ve TBK m. 58 hükmünde aramak gerekmektedir[117].

Öte yandan tazmin yükümlülüğünden farklı olarak Kurul tarafından verilen kararlar incelendiğinde veri sorumlusu veya veri işleyenlerin KVKK ve ikincil mevzuat kapsamında sebep oldukları hukuka aykırılık hallerinde sıklıkla idari para cezasına çarptırıldıkları kimi zaman ise ihlalin giderilmesi ve/veya söz konusu durumun düzeltilmesi konusunda talimatlandırıldıkları görülmektedir. Kurul kararları uyarınca veri sorumlusu veya veri işleyenlere verilen idari para cezası miktarlarının hangi kriterlere göre belirlendiği henüz Kurul tarafından net bir şekilde açıklığa kavuşturulmamış olmakla beraber, Kurum tarafından 5326 sayılı Kabahatler Kanununun 17. maddesi uyarınca idarî para cezalarının miktarı belirlenirken söz

---

[115] *II. Saldırıya karşı*
1. İlke
Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir.
Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.
2. Davalar
Madde 25- Davacı, hâkimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.
Davacı bunlarla birlikte, düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabilir.
Davacının, maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın vekâletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunma hakkı saklıdır.
Manevî tazminat istemi, karşı tarafça kabul edilmiş olmadıkça devredilemez; miras bırakan tarafından ileri sürülmüş olmadıkça mirasçılara geçmez.
Davacı, kişilik haklarının korunması için kendi yerleşim yeri veya davalının yerleşim yeri mahkemesinde dava açabilir.

[116] *Kişilik hakkının zedelenmesi*
MADDE 58- Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir.
Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.

[117] Aytın, Sinem. 2017, Televizyon yoluyla kişilik hakkı ihlalinden doğan manevi tazminat davası, s.12

konusu kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunun birlikte değerlendirileceği hükmü ile kişisel verilerin korunması mevzuatı kapsamında her somut olayın özelinde ayrı bir değerlendirme yapılacağı ve bu değerlendirmede aykırılığın nasıl gerçekleştiği, etkilenen kişi sayısı ve etkilenen verilerin niteliği gibi kriterlerin de göz önüne alınacağı açıklanmıştır[118].

[118] Kişisel Verileri Koruma Kurumu (2022). 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2

ÜÇÜNCÜ BÖLÜM

ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMA VE UYGULAMALARI

3.1.Çevrimiçi Davranışsal Pazarlama ve Kapsamı

Bu bölümde, çevrimiçi davranışsal pazarlama ("ÇDP") kavramından, dijital reklam uygulamalarındaki yerinden, öneminden, aktörlerinden ve rollerinden bahsedilecektir.

3.1.1.Kavramsal Açıdan Çevrimiçi Davranışsal Pazarlama ve Reklamcılık

Günümüzün dijital dünyasında, pazarlama faaliyeti yürüten taraflar, müşteri kitlelerine sundukları reklamları kişiselleştirmek ve hedeflemek için tüketiciler hakkındaki çevrimiçi verileri kullanma fırsatını yakalamıştır. Bu tür veriler, ziyaret edilen web sitelerini, okunan makaleleri, izlenen videoları ve ayrıca bir arama motoruyla aranan her şeyi içerebilmektedir. ÇDP, tüketicilerin web gezinme alışkanlıklarını takip ederek onlara özelleştirilmiş, ilgi alanlarına ve ihtiyaçlarına uygun reklamlar sunma yaklaşımıdır. Bu yöntemde, genellikle "çerezler" adı verilen bilgi parçaları aracılığıyla bir kullanıcının çevrimiçi davranışlarını izleyen ve analiz eden teknolojiler kullanır. ÇDP'nin temel amacı, kullanıcının ilgisini çeken ve ihtiyacına yönelik reklamlar sunmaktır. Bu teknik vasıtasıyla, pazarlama yapan taraflara, bir kullanıcının ilgisini çeken belirli ürün ve hizmetleri belirleme ve kullanıcıyı daha etkili bir şekilde hedefleme yeteneği sağlanabilmektedir.

Çevrimiçi davranışsal pazarlama ve çevrimiçi davranışsal reklamcılık genellikle birbiriyle çok yakından ilişkilidir ve bu terimler kimi zaman birbirinin yerine de kullanılmaktadır. Ancak, bu iki kavram arasındaki mevcut fark şöyle tanımlanabilir;

ÇDP genellikle bir kullanıcının çevrimiçi davranışlarına[119] dayanarak kişiselleştirilmiş ve hedeflenmiş pazarlama stratejilerinin ve taktiklerinin geliştirilmesini ifade etmektedir. Bu, e-posta üzerinden gerçekleşen pazarlama kampanyaları, özelleştirilmiş web içerikleri, sosyal medya stratejileri ve daha fazlasını içerebilecektir.

[119] Örneğin; ziyaret edilen siteler, arama geçmişi, satın alınan ürünler vb.

Öte yandan, çevrimiçi davranışsal reklamcılık, genellikle davranışsal verileri kullanarak reklamları kişiselleştiren ve hedefleyen spesifik bir dijital pazarlama taktiğidir. Genellikle kullanıcının çevrimiçi alışkanlıklarını ve ilgi alanlarını izleyen çerezler aracılığıyla gerçekleştirilir ve ilgili bilgiler daha sonra, kullanıcının ilgisini çekebilecek reklamları göstermek için kullanılmaktadır.

Kısacası, ÇDP daha geniş bir stratejiyken, çevrimiçi davranışsal reklamcılık daha spesifik bir uygulamadır. Çevrimiçi davranışsal reklamcılık, genellikle ÇDP stratejilerinin bir parçası olarak karşımıza çıkmaktadır. Bundan sonra bahsedilecek olan ÇDP hakkındaki bilgiler, durumlar ve örnekler; çevrimiçi davranışsal reklamcılık uygulamalarını da içerisinde barındırıyor olacaktır.

Basit bir ÇDP örneğinde, bir reklam ağı[120] bir tüketicinin web sitesi ziyaretlerini izlemektedir. Bir tüketici arabalarla ilgili birkaç web sitesini ziyaret ederse, ağ tüketicinin arabalarla ilgilendiğini varsaymaktadır. Ağ daha sonra araba reklamlarını yalnızca arabalarla ilgilenen (ya da ilgilendiği varsayılan) kişilere göstermektedir. Sonuç olarak, iki kişi aynı anda aynı web sitesini ziyaret ettiğinde, biri araba reklamlarını görebilirken, diğeri (mobilya ile ilgili web sitelerini ziyaret etmiş olan) mobilya reklamlarını görmektedir. Reklam verenler, ÇDP'yı hedeflenen kitlelere ulaşmanın en önemli yeni yollarından biri olarak görmektedir.

Tüm bunlarla birlikte, ÇDP uygulamaları aynı zamanda kişisel verilerin toplanmasını, kullanılmasını ve paylaşılmasını da içermekte ve bu nedenle tüketici mahremiyetiyle ilgili endişeleri artırmaktadır[121].

Bu alanda aktif rol oynayan McDonald ve Cranor'a göre; hedefli pazarlama stratejilerinin bir türü olan ÇDP stratejileri, hangi reklamın gösterileceğini seçmek için bir bireyin çevrimiçi etkinlikleri hakkında veri toplama uygulamasını da kapsamaktadır. Davranışsal reklamcılık, çeşitli farklı veri türlerine ve bu verilerden çıkarılan çıkarımlara dayalı olarak internet kullanıcıları için profiller oluşturmaktadır. Üçüncü taraf tanımlama bilgileri, davranışsal reklamcılığı mümkün kılmak için kullanılan birkaç mekanizmadan biridir. Binlerce web sitesindeki reklamlara sahip merkezi bir reklam ağı, belirli bir kullanıcının ağdaki herhangi bir siteyi her ziyaret edişini not ederek tanımlama bilgilerini ayarlayabilmekte ve okuyabilmektedir.

[120] Çok çeşitli web sitelerinde reklam hizmeti veren şirketler
[121] Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius. "Online behavioral advertising: A literature review and research agenda" 2017, s.363

Reklam verenler, bireyin hangi siteleri ziyaret ettiğini, hangi reklamların tıklandığını, yaş aralığı ve cinsiyetle ilgili çıkarımları ve bilgisayarın IP adresine dayalı yaklaşık coğrafi konumları ile ilişkilendirerek, o kişinin özelliklerinin ve olası ilgi alanlarının profillerini oluşturmaktadır. Çevrimiçi ortamlar, muazzam ölçekte büyük veri toplamaya bağlı olarak, oldukça fazla davranışsal reklam süreçleri bulunan kitle iletişim aracı biçimleridir. Yahoo! reklam sunucusu her ay yarım milyardan fazla benzersiz kişiye ulaşarak pazarın %9,7'sini oluşturmaktadır. Google'ın DoubleClick ve AdSense reklam sunucuları ise toplam pazarın %56'sına sahiptir ve her ay en az 1,5 milyar tekil kullanıcıya ulaşmaktadır. Google web işaretçileri, örneklenen yaklaşık 400.000 web sitesinin %88'inde ve en popüler 100 sitenin 92'sinde bulunmaktadır. Google'ın küresel boyutta internet kullanıcılarının yaklaşık %90'ını izlediği bildirilmektedir.

Turow bu noktada dijital profilleme ve kişiselleştirmenin yükselişinin çok ciddi sonuçları olabilecek toplumsal ayrımcılık ve mahremiyet sorunlarına yol açacağını belirtmektedir. Ona göre dijital ortamın birçok büyük avantajı var ise de şirketlerin insanları takip etmesi ve onların verilerini kullanarak reklam göndermesinin henüz tam olarak netleşmeyen sonuçları olabilmektedir. Ortaya çıkabilecek en olası sonuç, insanları reklamlar yoluyla sınıflandırmaktır[122].

Bu reklam ağı şirketleri, kişisel olarak tanımlanabilir bilgileri değil, yalnızca belirlenebilir[123] verileri izledikleri için ÇDP'nin kişisel mahremiyete müdahale etmediğini iddia etmektedir. Hatta ÇDP'nin tüketiciler için faydalı olduğunu çünkü onlara kendileriyle gerçekten alakalı daha fazla bilgi sağladığını da belirtmektedirler[124].

Buna karşılık; Turow ise bu iddiaların anlamlı olmadığını şu şekilde ifade etmektedir; *"Bu iddialara cevaben, reklam ağı şirketlerinin gerçekten de bireyleri tanımlayabildiği, ancak bireysel çevrimiçi gezinme geçmişini izleyip derledikleri konusunda tüketicileri aktif olarak bilgilendirmediği ve izleme için tüketiciden izin talep etmediği ileri sürülmektedir; buna göre, pek çok tüketici davranışsal izleme*

[122] Turow, Joseph. 2015, İzleniyoruz: Yeni Reklam Sektöründeki Kimliğimiz ve Değerlerimiz, s. 21
[123] Örneğin; belirli bir tüketicinin tanımlayıcı bilgileri olmadan çevrimiçi davranış verileri
[124] Ham, Chang-Dae. 2017, "Exploring How Consumers Cope With Online Behavioral Advertising." International Journal of Advertising, s.632

uygulamasının farkında değildir ve yalnızca nispeten küçük bir kısmı özel reklam mesajlarının nasıl iletildiğini bilmektedir."[125].

3.1.2.Çevrimiçi Davranışsal Pazarlama Stratejilerinin Dijital Reklam Uygulamalarındaki Yeri ve Farklılığı

ÇDP stratejilerinden çevrimiçi davranışsal reklamcılık, çeşitli tanımlarda başlı başına bir reklam uygulaması olarak kabul edilirken; aynı zamanda bir sistem, özel bir hedefli reklamcılık biçimi, yeni bir reklam biçimi olarak da adlandırılabilmektedir[126].

Çevrimiçi reklam şirketleri tarafından üretilen reklamları, bireylerin çevrimiçi etkinliklerini düzenlemek için kullanılan gelişmiş bir çevrimiçi takip mekanizması olarak tanımlamak yerinde olacaktır[127].

Çevrimiçi davranışsal reklam, dijital reklam stratejilerinin önemli bir parçasıdır ve genel dijital reklam pratiklerinden çeşitli şekillerde farklılık gösterir.

1. Kişiselleştirme: Çevrimiçi davranışsal reklam, kullanıcının web'de geçirdiği süre boyunca toplanan verilere dayanarak reklamları kişiselleştirmektedir. Bu, kullanıcının belirli bir ürün veya hizmetle ilgilenip ilgilenmediğini anlamak için gezinme geçmişi, arama geçmişi, satın alma geçmişi vb. gibi çeşitli faktörleri içerir. Bu tür bir kişiselleştirme, diğer dijital reklam taktiklerinde nadiren görülmektedir.

2. Davranışsal Segmentasyon: Çevrimiçi davranışsal reklam, kullanıcıları belirli davranışsal özelliklere ve eğilimlere göre segmentlere ayırmaktadır. Bu, kullanıcılara en uygun ve ilgi çekici içeriği sunmak için kullanılmaktadır. Diğer dijital reklamcılık tekniklerinde genellikle demografik veya coğrafi özelliklere dayalı segmentasyon kullanmaktadır.

3. Gelişmiş Hedefleme: Çevrimiçi davranışsal reklam, kullanıcıların geçmiş davranışlarına ve ilgi alanlarına dayanarak çok özelleştirilmiş ve hedeflenmiş

[125] Turow, 2015: 21

[126] Smith, Edith G.; Noort, Guda Van ve Voorveld, Hilde A. (2014). "Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe."; McDonald, Aleecia M., and Lorrie Cranor. "An Empirical Study of How People Perceive Online Behavioral Advertising (CMU-CyLab-09-015)." (2009). Pittsburgh: Carnegie Mellon University; Kim, Yoojung. (2014). "Consumer Privacy Concerns and Responses to Online Behavioral Advertising: A Cross-Cultural Comparison of Americans and Koreans.", 2014

[127] Leon, Pedro Giovanni; Cranshaw, Justin; Cranor, Lorrie Faith; Graves, Jim; Hastak, Manoj; Ur, Blase ve Xu, Guzi (2012). What Do Online Behavioral Advertising Disclosures: s.1

reklamlar sunma yeteneğine sahiptir. Bu, tüketicilere daha alakalı ve kişisel reklamlar sunarak dönüşüm oranlarını artırma potansiyeli sağlamaktadır.

4. Dinamik İçerik: Çevrimiçi davranışsal reklam, kullanıcıların eylemlerine yanıt olarak dinamik olarak değişebilen reklamlar sunabilir. Bu, kullanıcının belirli bir eylemi gerçekleştirmesi (örneğin, bir ürünü sepete eklemesi veya bir web sitesini ziyaret etmesi) sonucunda reklamın içeriğinin veya görüntülenme sıklığının değişmesi anlamına gelmektedir.

Bu bağlamda bu farklılığın temel nedeni biçimsel bir tür değil, bağlamsal bir tür olmasıdır. Hedefleme, belirli kriterlere (yer, zaman, demografi, çevrimiçi davranış vb.) dayalı olarak tüketicilere reklam gönderme yöntemidir. En iyi sonuçlar, hedefleme ile belirlenen belirli bir hedef kitleye yönelik reklamcılıkla elde edilmektedir. Çevrimiçi davranışsal reklamcılığın dijital reklamcılığın oluşumundaki yeri, bir hedefleme yöntemi olmasından kaynaklanmaktadır. Çeşitli hedefleme türlerinden biri olan ve çevrimiçi davranışsal reklama temel teşkil eden davranışsal hedefleme, en basit ifade ile "*bir kullanıcının web tarama davranışından yararlanarak, reklamın etkinliğini artırmasıdır*"[128].

Bunun bir örneği, bir internet kullanıcısının ilgisini yansıtacak şekilde yayınlanan bir banner reklamdır. Davranışsal reklamcılık aynı zamanda hedef kitlelere farklı bir odaklanma getirmiştir. Artık reklamcılık grupları değil, insanları etkilemeyi amaçlamaktadır. Yani reklamda bireyselleşme var olmaktadır. Schultz bu durumu, "*medya, bugün kitle iletişim araçlarının kullandığı daha geniş ve daha genel demografik gruplardan ziyade satıcılara / reklam verenlere hitap edecek benzersiz izleyiciler oluşturmaya daha fazla odaklanacaktır*" şeklinde ifade etmektedir[129]. Bu aşamada pazarlama ortamındaki güç dinamiği de değişmekte ve firmalar sadece agresif rakiplerle değil, aynı zamanda dikkati sınırlı müşterilerle de uğraşmak zorunda kalmaktadır[130].

Bu nedenle günümüzde dikkati sınırlı müşterilere ancak reklamlar hedeflendiği takdirde ulaşılabildiği görülmektedir. Bu kapsamda ÇDP uygulamaları da özellikle

[128] Chen, Jianqing ve Stallaert, Jan. "An Economic Analysis of Online Advertising Using Behavioral Targeting, 2014, s.430
[129] Schultz, Don. "The Future of Advertising or Whatever We're Going to Call It." Journal of Advertising, 2016, s.281
[130] Kumar, V. ve Gupta, Shaphali: "Conceptualizing the Evolution and Future of Advertising." Journal of Advertising, 2016, s.302

hedef kitleyi tanımlamaya yönelik değerli veriler sağladığı için her geçen gün daha fazla önem kazanmaktadır. Ancak bu durum mahremiyet sorunlarını da beraberinde getirmektedir. Kullanıcıların çevrimiçi davranışları üzerinde derinlemesine gözlem yapılması, bazı durumlarda kullanıcıların gizlilik haklarını ihlal edebileceği anlamını taşımaktadır. Bu nedenle, bu tür reklam uygulamaları dikkatli bir şekilde yönetilmeli ve kullanıcıların gizlilik haklarına saygı gösterilirken, yasal düzenlemelere uyumun sağlandığından da emin olunmalıdır.

3.1.3. Çevrimiçi Davranışsal Pazarlama'nın Aktörleri ve Rolleri

ÇDP sektöründe birçok oyuncu bulunmaktadır ve reklam sürecinde paydaş olan tüketiciler, reklamcılar, ajanslar, medya ve yasal kuruluşlar ile benzerlik göstermektedir[131]. Çünkü reklamın görünümü her şeyden önce ona ihtiyacı olan reklam verenin, reklamı hazırlayan bölümün veya reklam ajansının varlığına ve tasarlanan mesajların hedefe ulaşması için bir iletişim kanalı olarak medyanın varlığına bağlıdır[132]. Dolayısıyla benzer şekilde çevrimiçi davranışsal reklamcılık dünyasının paydaşları da reklam veren, yayıncılar, reklam ağları ve kullanıcılar olarak ifade edilmektedir[133].

Bu süreçte rol oynayan aktörler ise aşağıdaki şekilde özetlenebilecektir;

> ***1. Kullanıcılar (Tüketiciler):*** Kullanıcılar, çevrimiçi etkinliklerini sürdürürken çeşitli veriler üretmektedir. Bu veriler, çevrimiçi davranışsal pazarlama süreçlerinde kullanılır. Kullanıcılar, belirli bir ürün veya hizmet hakkında bilgi ararken, çevrimiçi alışveriş yaparken, sosyal medya hesaplarını kullanırken veya bir blog veya haber sitesini okurken ÇDP uygulamalarına bilgi akışını sağlamaktadırlar.
>
> ***2. Web Sitesi Sahipleri/İçerik Sağlayıcılar:*** Web sitesi sahipleri ve içerik sağlayıcılar, kullanıcıların çevrimiçi davranışları hakkında bilgi toplamakta ve bu bilgileri reklam verenlere veya üçüncü taraf platformlara iletmektedirler. Ayrıca, web sitesi sahipleri genellikle çerezleri ve benzeri teknolojileri

[131] Yaman, Fikret. Reklamcılık Sektöründe Reklam Etiği Algılamasının Değerlendirilmesi, 2009, s.30-36.
[132] Peltekoğlu Balta, Filiz, Kavram ve Kuramlarıyla Reklam, 2010, s.98
[133] Keser Berber, Leyla. Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması, 2014, s.15

kullanarak kullanıcıların çevrimiçi davranışlarını izler ve bu bilgiler sonrasında kişiselleştirilmiş reklamlar sunmak için kullanır.

3. Reklam verenler: Reklam verenler, çevrimiçi davranışsal pazarlama stratejilerini oluşturan ve uygulayan işletmelerdir. Kullanıcı verilerini kullanarak, hedef kitlesiyle en etkili şekilde nasıl iletişim kuracaklarını belirlemektedirler. Reklam verenler genellikle üçüncü taraf platformlara[134] bu hedefleme bilgilerini ileterek süreci yürütürler.

4. Üçüncü Taraf Platformlar / Reklam Ağları: Üçüncü taraf platformlar ve reklam ağları, reklam verenler ve web sitesi sahipleri arasında köprü görevi görmektedir. Bu platformlar, reklam verenlerin belirlediği hedefleme kriterlerine göre kullanıcıların online davranışlarına dayanarak kişiselleştirilmiş reklamlar sunmaktadır. Bu tür hizmetleri sağlayan ve en bilinin platformlar arasında Google ve Facebook gibi büyük platformlar yer almaktadır.

5. Veri Analitik Şirketleri: Bu aktörler, çevrimiçi davranışsal pazarlamada önemli bir rol oynamaktadır. Online kullanıcı verilerini toplayan, analiz eden ve bu bilgileri reklam verenlere sağlayan taraf olarak karşımıza çıkmaktadırlar. Veri analitik Şirketleri tarafından sağlanan bu bilgiler, daha etkili ve kişiselleştirilmiş reklam kampanyaları oluşturmak için kullanılmaktadır.

3.2.Çevrimiçi Davranışsal Pazarlama Stratejilerinin Çalışma Prensibi

Yukarıda açıklandığı gibi, ÇDP stratejileri, çeşitli şekillerde elde edilen verilerin kullanılması vasıtasıyla kişilerin ilgi alanlarını ve ihtiyaçlarını belirleyerek kişiselleştirilmiş reklam göndermenin bir yoludur. Kişiselleştirilmiş reklamların gönderilmesi, reklam verenler ve reklam ajansları için oldukça avantajlı olsa da, kişinin davranışlarının takip edilmesi ve çeşitli hedeflemeler sağlanması nedeniyle eleştirilmektedir. Kritik noktalar, bu tür bir reklamın nasıl veri elde ettiğini de önemli kılmaktadır.

[134] Örneğin; Google AdWords, Facebook Ads vb.

3.2.1.Çevrimiçi Davranışsal Pazarlama Uygulamalarında Veri Edinme Teknikleri

ÇDP uygulamalarında kullanılan verilerin nasıl elde edildiği ve kullanıldığı oldukça büyük önem arz etmektedir. Tüketicilerin ilgi alanlarını, tercihlerini, yönelimlerini ve ihtiyaçlarını belirlemede veri toplamaya yönelik çeşitli mekanizmalar vardır. Bazı yaygın veri toplama teknikleri aşağıdaki şekilde sıralanabilir;

1. Çerezler (Cookies): Çerezler, kullanıcıların internet tarayıcılarına yerleştirilen küçük veri dosyalarıdır. Çerezler, kullanıcıların bir web sitesindeki aktivitelerini takip etmek ve bir dizi kullanıcı bilgisini saklamak için kullanılmaktadır. Çerezler genellikle kullanıcıların site tercihlerini, oturum bilgilerini ve tercih edilen diğer verileri saklamak için kullanılmaktadır.

2. Web İşaretçileri (Web Beacons): Web işaretçileri (veya pixel etiketleri), genellikle e-posta pazarlama kampanyalarında kullanılmaktadır. Kullanıcının bir e-postayı açıp açmadığını, hangi bağlantılara tıkladığını ve tercih edilen diğer eylemleri izlemek için kullanılabilmektedir.

3. Log Dosyaları: Web sunucuları, kullanıcıların bir web sitesinde gerçekleştirdiği her etkinliği otomatik olarak kaydeder. Bu bilgiler, kullanıcıların web sitesinde ne zaman ne yaptıkları hakkında ayrıntılı bilgiler sağlamaktadır.

4. Clickstream Verileri: Clickstream verileri, bir kullanıcının web sitesinde gerçekleştirdiği her bir tıklamayı kaydeder. Bu, kullanıcının sitede ne zaman ne yaptığı ve hangi sayfalara gittiği hakkında ayrıntılı bir kayıt sağlamaktadır.

5. Veri Madenciliği (Data Mining): Veri madenciliği, genellikle büyük veri setlerindeki desenleri ve ilişkileri keşfetmek için kullanılmaktadır. Bu teknik, kullanıcının çevrimiçi davranışlarını ve tercihlerini anlamak için oldukça tercih edilen bir yöntemdir.

6. Sosyal Medya İzleme: Sosyal medya izleme stratejileri, hangi ürünlerin ve hizmetlerin kullanıcılar arasında popüler olduğunu, kullanıcıların belirli konular hakkında ne düşündüğünü ve kullanıcıların kimlerle etkileşimde bulunduğunu anlamak için kullanılabilmektedir.

7. Cihaz ve Tarayıcı Ayırt Edici Özellikler: Cihazın IP adresi, işletim sistemi, tarayıcı türü, ekran çözünürlüğü ve diğer ayırt edici özellikler de kullanıcı hakkında veri toplamak için kullanılabilmektedir.

Konu bütünlüğünü bozmamak adına yukarıda sayılan veri toplama tekniklerinden yalnızca çerezler ve veri madenciliği kapsamında büyük verinin tanımı aşağıda daha detaylı olarak incelenmektedir.

3.2.1.1.Çerezler (Cookies)

Çerezler, web sitelerinin kullanıcıların bilgisayarlarına veya diğer cihazlarına yerleştirdiği küçük metin dosyalarıdır. Bir kullanıcı bir web sitesini ziyaret ettiğinde, site bir çerez oluşturabilir ve bu çerezi kullanıcının cihazına kaydedebilir.

20 Haziran 2022 tarihinde Kurum tarafından yayımlanan Çerez Uygulamaları Hakkında Rehber ile çerez tanımı yapılmıştır[135].

Çerezler, kullanıcıların bir web sitesini ziyaret ettikleri sırada tarayıcılarına yerleştirilir ve genellikle bir kullanıcının o siteyi daha sonra tekrar ziyaret etmesi durumunda kullanıcıyı hatırlamak için kullanılmaktadır. Çerezler, kullanıcının kimlik bilgilerini, oturum bilgilerini, site tercihlerini, alışveriş sepeti bilgilerini ve tercih edilen diğer bilgileri saklayabilmektedir. Çerezler aracılığıyla elde edilen veriler, kişisel veri niteliği taşımayan bilgilerden (tercih edilen dil ayarları gibi) oluşabileceği gibi; IP adresi, kullanıcı adı veya e-posta adresi gibi kişisel verilerden de oluşabilecektir. IP adreslerinin kullanımı sayesinde ilgili kişilerin isim-soyisim bilgisi bulunmasa dahi belirlenebilir olacaktır. Bu nedenle, çerezler kişisel verilerin korunmasıyla doğrudan ilişkili olmaktadır[136].

---

[135] Kişisel Verileri Koruma Kurumu, Haziran 2022 *"Çerez, internet sitesi operatörleri tarafından kullanıcı cihazına yerleştirilen bir tür metin dosyası olup HTTP(S)3 (Hiper Metin Transferi Protokolü) talebinin bir parçası olarak aktarılır. Diğer bir tanıma göre ise çerezler, bir internet sayfası ziyaret edildiğinde kullanıcılara ilişkin birtakım bilgilerin kullanıcıların terminal cihazlarında depolanmasına izin veren düşük boyutlu zengin metin biçimli text formatlarıdır."*

[136] Aksoy, Hüseyin Can ve Halıcıoğlu, Mesut. AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme, 2021

Çerezler, kaynaklarına, saklanma sürelerine ve kullanım amaçlarına göre sınıflandırılabilir[137].

Kaynaklarına göre çerezler, *"birinci taraf çerezleri*" ve "*üçüncü taraf çerezleri*" olarak ikiye ayrılmaktadır. Birinci taraf çerezler, kullanıcının ziyaret ettiği web sitesi tarafından oluşturulur ve web sitesinin sahibiyle doğrudan ilişkilidir. Üçüncü taraf çerezlerde ise web sitesinin sahibi, üçüncü kişilerin oluşturduğu çerezlere izin vermekte ve bu çerezler aracılığıyla kullanıcı takip etmektedir[138].

Çerezler ayrıca kullanım sürelerine göre "*oturum çerezleri*" (geçici süreli çerezler) ve "*kalıcı çerezler*" olarak da sınıflandırılmaktadır. Oturum çerezleri, kullanıcının web sitesini ziyaret ettiği süre boyunca işlemde kalan ve web sitesi kapandığında otomatik olarak silinen çerezlerden oluşmaktadır. Kalıcı çerezler ise web tarayıcısı kapatılsa bile silinmeyen ve kullanıcının tercihlerine, ilgi alanlarına ve kimlik doğrulama gibi bilgilerine erişim imkanı sağlayan çerezleri tanımlamaktadır. Bu çerezler aracılığıyla kullanıcının dijital bir profil oluşturulması mümkün kılınmaktadır.

Son olarak, çerezler ihtiyaçlarına/amaçlarına göre "*zorunlu çerezler*", "*işlevsellik çerezleri*" (ihtiyaca yönelik çerezler), "*performans çerezleri*" (analitik çerezler) ve "*reklam/pazarlama çerezleri*" olarak dört gruba ayrılır. Zorunlu çerezler, bir web sayfasının doğru şekilde çalışabilmesi, web sayfasında gezinebilmeyi ve içeriğinden faydalanmayı sağlamak için gerekli ve hatta zorunlu olan çerezlerdir. İşlevsellik çerezleri, kullanıcının geçmiş tercihlerini hatırlayarak web sitesinin içeriğini kişiselleştirmek için kullanılmaktadır. Performans çerezleri, kullanıcının web sitesini nasıl kullandığını tespit etmek için anonim olarak kullanılmakta ancak kişinin kimliğini tespit etmek amacıyla kullanılmamaktadır. Öte yandan reklam/pazarlama çerezleri ise kullanıcılar hakkında veri toplayarak, hedeflemeye yönelik işlemleri gerçekleştirmeye ve kullanıcılara ilgi çekici içerik ve reklamlar sunmaya fayda sağlayan çerezlerdir.

Genel anlamda çerezlerin ilgili kişilerin verilerini ihlal riski taşıdığını söylemek izahtan varestedir. Bu kapsamda veri sorumlusu ve veri işleyenlere bu verileri hangi

[137] Doğan, Başak ve Bozkurt, Tuğçe. Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle, 2020

[138] Skouma Georgia ve Leonard Laura. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Reforming European Data Protection Law (C. 1-20, C. Privacy and Data Protection, 2015, s.15-22.

yöntemlerle topladığı, ne amaçlarla kullandıkları, nasıl sakladıkları varsa aktarım tarafları gibi süreçler ile yerel ya da gerektiğinde uluslararası mevzuata uyumluluk konusunda büyük sorumluluklar düşmektedir.

Çalışmanın devamında ÇDP uygulamaları hakkında getirilen hem ulusal hem de uluslararası düzenlemelere ayrıca değinilecek olup, bu çalışmanın esasını oluşturan Türk hukukundaki eksiklikler ve getirilmesi beklenen düzenlemeler hakkındaki görüşlerimiz de ayrıca paylaşılacaktır.

3.2.1.2. Veri Madenciliği Kapsamında Büyük Veri ve Çevrimiçi Davranışsal Pazarlama ilişkisi

Çevrimiçi davranışsal pazarlama ve büyük veri, birbiriyle yakından ilişkili olup, birlikte kullanıldığında, pazarlamacılara daha kişiselleştirilmiş ve etkili pazarlama stratejileri oluşturma imkanı sağlayan bir uygulamadır[139].

Büyük veri, ÇDP uygulamalarında kritik önem taşımaktadır. Pazarlamacılar, büyük veriyi vasıtasıyla, kullanıcıların çevrimiçi davranışlarını, alışkanlıklarını, tercihlerini ve ilgilerini analiz edebilir, bu sayede kullanıcılara daha kişiselleştirilmiş ve alakalı reklamlar ile içerik sunma yeteneğine sahip olurlar.

Büyük veri terimi, bir kuruluşun çok büyük veri kümeleri ve depoları oluşturmasını, değiştirmesini ve yönetmesini sağlayan araçları, süreçleri ve prosedürleri ifade etmektedir[140]. Diğer bir deyişle terim, geleneksel veri işleme araçlarının kaydedemediği, depolayamadığı ve analiz edemediği devasa veri bloklarını ifade etmektedir[141]. Bu veri kümeleri genellikle insanların dijital ayak izlerini, alışkanlıklarını, tercihlerini ve etkileşimlerini içermekte ve sosyal medya etkileşimleri, satın alma geçmişi, web sitesi tarama geçmişi, coğrafi konum verileri ve daha pek çok kaynaktan elde edilebilmektedir.

Büyük veri ilk başta endüstri analisti Doug Laney tarafından günümüzde de yaygın şekilde kullanılan 3V (hacim, hız ve çeşitlilik) tanımı ile ifade edilmiştir. Hala birçok kaynakta Laney'in bu 3V tanımlaması bulunmasına rağmen, daha sonra eklemelerle doğruluk (veracity), değer (value), değişkenlik (variability), sanallık (virtual), görselleştirme (visualization) ve karmaşıklık (complexity) tanımları da büyük veri

[139] Çekin, 2016.
[140] Knapp, Maureen. "Big Data." Journal of Electronic Resources in Medical Libraries, 2013, s.215
[141] Lokke, Eirik. Mahremiyet: Dijital Toplumda Özel Hayat, 2018. s.60

özelliklerine dahil edilmiştir. Ancak büyük ölçüde kabul edilen V'ler; hacim (volume), hız (velocity) çeşitlilik (variety), doğruluk (veracity) ve değer (value) olarak görülmektedir[142].

Dolayısıyla gelecekte veriye sahip olacak ve onu iş süreçlerinde daha iyi kullanacak kişilerin çok daha değerli kurum/firma/birey olacağı ve dolayısıyla rakiplerine göre ciddi bir değere sahip olacağı anlaşılmaktadır. Günlük hayatın dijitale yönelmesinin yanı sıra iş hayatının dijitalleşmesi de büyük veri kullanımını önemli kılmaktadır. İş hayatında inovasyona dönüşen bu yönelim, geleneksel işletme yönetiminden farklı olarak görülmektedir. Benzer şekilde, büyük veriler geleneksel verilerden farklıdır ve ayrı olarak depolanmaktadır. Çünkü büyük veri, klasik veri tabanı sistemlerinin yeterli olmadığı durumlarda ortaya çıkan bir problem olarak ifade edilmektedir[143].

Özellikle büyük kuruluşlarda veri bilimcileri, iç çözümler için üst düzey yöneticilere danışmanlık sunumları hazırlamak yerine tüketiciler için ürün ve hizmetler hazırlama eğilimindedir. Örneğin, Linkedin CEO'su Reid Hoffman, şirket için tanınacak insanlar, beğenilecek gruplar, ilgi uyandırmak için iş ilanları gibi ürünler yaratan bir veri bilimci ekibi kurmuştur. Büyük veri şirketi olan Google, arama ve reklam algoritmalarını uygulamak için veri bilimcilerini kullanmaktadır[144].

Büyük veri, e-postaları, metinleri, belgeleri, videoları, sesleri, görüntüleri, tıklama akışlarını, sistem günlüklerini, arama sorgularını, sosyal medya etkileşimlerini, tıbbi kayıtları, bilimsel verileri, kamu ve özel sektör kayıtlarını, sensörler ve akıllı telefon kayıtlarını ve daha fazlasını içermektedir. Bu bileşenler aracılığıyla elde edilen bilgilerin birleştirilmesi çok farklı sonuçlara yol açabilmektedir. Çünkü 1854 yılındaki kolera salgını sırasında yapılan ve büyük bir veri tabanı olarak ifade edilen haritalama artık arama motorları tarafından yapılabilmektedir. Bölgedeki çevrimiçi aramaların yoğunluğuna bağlı olarak çok çeşitli tür verilere ulaşılabilmektedir[145]. Dolayısıyla Google'ın kimin neyi, nerede aradığını kaydederek, resmi sağlık kuruluşları ile aynı anda, hatta daha erken dönemde hastalıkların yayılımını tespit etme potansiyeline sahip olduğu bile söylenebilecektir. Büyük veri birçok alanda farklı amaçlar için

[142] Patgiri, Ripon ve Ahmed, Arif. "Big Data: The V"s of the Game Changer Paradigm." 18th International Conference on High Performance Computing and Communications, 2016, s.17-18
[143] Terzi, Ramazan.; Sağıroğlu, Şeref. ve Demirezen, Umut. Büyük Veri ve Açık Veri: Temel Kavramlar. Şeref Sağıroğlu, Orhan Koç (Ed.), Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar içinde, 2017, s.16
[144] Davenport, Thomas. Big Data @ Work: Efsaneye Son Vermek, Fırsatları Keşfetmek, 2014, s.23
[145] Lokke, 2018: 61

kullanılabilmekte ancak sorun da zaten burada ortaya çıkmaktadır. Her saniye büyüyen verilerin anlamlı hale getirilmesi gerekmekte, bu da bazı zorluklar yaratmaktadır[146]. Dolayısıyla veriye sahip olmak yerine onu işlemek, anlamlandırmak ve süreçteki zorluklar temel problemler olarak ortaya çıkmaktadır. Veri büyüdükçe, yeni algoritmalar, yaklaşımlar, tek kelimeyle, verilerin toplanması, depolanması, işlenmesi ve değerlendirilmesi için yeni yöntem ve teknolojilere ihtiyaç duyulmaktadır[147].

Bu aşamada veri madenciliği teknikleri önemlidir, veri madenciliği büyük veri araştırmaları için doğru sonuçlara sahip olabilecek ve veri setinden çeşitli örüntüler, kurallar ve eğilimler çıkarabilecek, yöntemleri içermekte ve önemli bilgilerin kullanılmasına izin vermektedir[148].

Veri madenciliği; istatistik, veri yönetim sistemleri ve makine öğrenmesi gibi tekniklere dayanarak veriden bilgiyi elde etmeyi amaçlayan sistemlerdir[149]. Teknik olarak çok detaylı ve bu çalışmanın kapsamı dışında çok geniş bir alanı temsil eden veri madenciliği, tüketim ve pazarlama alanında oldukça etkin bir şekilde kullanılmaktadır.

Pazarlama alanındaki veriler çeşitli kaynaklardan elde edilmektedir. Bunlar[150], öncelikli olarak, 1980 sonrasında hızla yaygınlaşan barkod sistemlerinden elde edilen verilerin, ERP28 ve SCM29 yazılımları ile kombine edilmesine dayalı verilerdir. İkincisi; demografi, satın alma geçmişi, reklam yanıt geçmişi, tercihler, ürün iade geçmişi, e-posta kampanyalarına ilgi gibi bilgilerden elde edilen tüketici kimlik verileridir. Üçüncü bir potansiyel veri kaynağı olarak; tüketicilerin çeşitli sitelere girerken gönüllü olarak verdikleri sosyal medya bilgilerinden elde edilen veriler ile son olarak; tüketici tercihlerini ve satın alma eğilimlerini ortaya çıkarmak için konum bilgilerinden elde edilen veri kaynaklarıdır. Büyük veri analitiğinin yüksek potansiyel değerinin en önemli nedeni, depolama alanı genişledikçe ve işleme yetenekleri genişledikçe verilerin yeniden kullanım olasılığının arttırılmasıdır. Bu, dijital dünyada bırakılan elektronik ayak izlerinin ve belirli bir amaç için toplanan ve saklanan

[146] Acharjya, Debi Prasanna, ve Ahmed, Kauser. "A Survey on Big Data Analytics: Challenges, Open Research Issues and Tools, 2016 s.512-513.
[147] Terzi; Sağıroğlu; Demirezen, 2017: 23
[148] Şeker, Şadi Evren "Sosyal Ağlarda Veri Madenciliği, 2015 s.30
[149] Fayyad, Usama; Piatetsky-Shapiro, Gregory ve Smyth, Padhraic, "From Data Mining to Knowledge Discovery in Databases, 1996, s.39
[150] Bradlow, Eric; Gangwar, Manish; Kopalle, Praveen ve Voleti, Sudhir. "The Role of Big Data and Predictive Analytics in Retailing." 2017, s.8-14

verilerin başka amaçlar için (büyük olasılıkla kişilerin rızası olmadan) kullanılabileceği anlamına gelmektedir[151].

Bu bağlamda ÇDP uygulamaları, büyük veriyi çeşitli yöntemlerle işleyerek reklamcıların kullanımına hazır hale getirmektedir. Ayrıca veri madenciliği, hızla büyüyen ÇDP endüstrisine ekonomik değer sağlamaktadır. Bu nedenle, daha fazla reklam geliri, tüketicilerin daha fazla çevrimiçi reklamcılığa ve veri madenciliğine maruz kaldığını göstermektedir[152]. Basitçe ifade etmek gerekirse; çevrimiçi reklamlar, artık ÇDP ve veri madenciliğine dayanmaktadır.

3.2.2.Çevrimiçi Davranışsal Pazarlamanın İşleyişi

Çevrimiçi medya ve reklam endüstrisi şu an 'gerçek zamanlı açık arttırma' anlamına gelen 'Real Time Bidding' sistemini kullanmaktadır. Dr. Johnny Ryan, sistemin çalışma şeklini detaylı bir şekilde "*Behavioural advertising and personal data*" başlıklı raporunda ortaya koymaktadır[153].

Ortaya çıkan veriler, birçok reklam platformunda çeşitli görevleri yerine getiren reklam teknolojisi şirketleri arasında paylaşılmaktadır. Bu sistemi kullanan ÇDP uygulamaları, kişisel verilerin korunması nerdeyse mümkün olmayacak şekilde kişisel verileri kullanmaya devam ederken, web sitelerinde bir kullanıcı her web sayfası yüklediğinde bu işlem gerçekleşmeye devam etmektedir. Çevrimiçi davranışsal reklamcılık, bu verileri nasıl elde ettiklerine göre; kendisi, taraflı ve üçüncü şahıslar olmak üzere 3'e ayrılmaktadır[154].

Bu nedenle, veri toplama, ÇDP işleyişinin merkezinde yer almaktadır. Uygulayıcılar, kendilerini birey olarak tanımlamadıklarını, sadece birkaç kullanıcı olduklarını, bu nedenle güven sorunu yaratabilecek bir durum olmadığını iddia etmektedirler. Özellikle bu tür reklamların kişilerin rızasına bağlı olduğu ve istemeyen kişilerin bunu kolayca bildirebileceği iddiası en sık kullanılan açıklamadır.

---

[151] Lokke, 2018: 63

[152] Hunt, Matthew K. "Cookie Consumer: Tracking Online Behavioural Advertising in Australia. 2016, s.57-59

[153] www.brave.com,19/09/2022

[154] McStay, Andrew, Profiling Phorm: An Autopoietic Approach to The Audience-as- Commodity., 2011, s.311-312.

3.2.2.1.Hedefleme Nedir ve Hedefleme Türleri Nelerdir?

İnternette gezinen, arama yapan, çeşitli içerikleri görüntüleyen, alışveriş yapan, haber okuyan ve daha birçok işlemi gerçekleştiren tüketiciler, bilgi alarak kendileri hakkında da bilgi bırakmaktadırlar. Bu bilgiler, dijital ayak izlerini ve pazarlama uygulamalarını belirlemek için kullanılmaktadır. Artan küresel rekabet, pazarlama iletişimi profesyonellerini belirli hedef tüketici gruplarına odaklanmaya zorlamaktadır[155]. Günümüzde tüketiciler çevrimiçi ortamlarda eriştikleri içerikler için ödeme yapmak istememektedirler. Anderson bu durumu şu ifadelerle açıklamaktadır:

> "*Tüketicilerin içeriklere ulaşması için ödeme yapmalarının istendiği ilk birkaç yılın ardından, dijital ekonomi ile savaşmanın imkânsız olduğu görülmüş ve ücretsiz içerikler üretilmeye başlanmıştır (2009: 16). ...Dolayısıyla ücretsiz yayın yapan radyo, televizyon, gazete gibi geleneksel medyadan, çoğunluğu internet olan dijital medyanın birçoğuna kadar arkasında reklam destekli medya bulunmaktadır. Reklam destekli ücretsiz içerik yüzyılın en önemli iş modelidir*"[156].

Reklamları ise yanlış kişilere hedeflemek pazarlamacılar için her zaman zor olmuştur. Geleneksel olarak medya planlamasının amacı, bir kategoride aktif olmayan tüketicilere gönderilen reklam miktarını azaltarak doğru tüketiciye ulaşmaktır. Aslında firmalar, müşteri kişiliğini ve müşterinin geçmiş davranışlarını birleştiren standart yöntemlere güvenmektedirler, ancak müşteri sosyal profillerini analiz etmek, hedefleme ve iletişim için en uygun stratejiyi belirlemeyi de kolaylaştırmaktadır[157]. Dolayısıyla firmaların, müşterilerin tercihleri ile medya alışkanlıklarını biliyor olmaları firmalara bir pazardaki belirli segmentleri hedefleme yeteneği sunmaktadır. Hedefleme esas olarak "pazar bölümlendirmesine" dayanmaktadır. Pazar bölümlendirme; pazarın benzer özelliklere sahip tüketici gruplarına bölünmesi ve hizmet için en uygun hedefin seçiminde ifade edilmektedir. Bu anlayışa dayalı ilişkisel pazarlama faaliyetleri, yeni müşteriler edinmeden önce mevcut bir müşterinin sadakatini kazanarak pazarlama ve tanıtım faaliyetlerinin bu doğrultuda düzenlenmesi anlamına gelmektedir[158]. Bu nedenle, bir reklam amacı için uygun bir grubu seçerek hedefleme, aslında belirli bir mevcut müşteri grubuna yönelik pazar bölümlendirme

[155] Roberts, Marilyn S. ve Ko, Hanjun, "Global Interactive Advertising." 2001, s.19
[156] Anderson, Chris; Free: The Future of Radical Price, 2009, s.114
[157] Kumar ve Gupta, 2016: 309
[158] Yılmaz, Recep ve Erdem, Nur. 150 Soruda Geleneksel ve Dijital Reklamcılık, 2016, s.260

veya promosyon faaliyetlerinin dijital sürecinde yeni bir form olarak tanımlanabilmektedir. Bu noktadan hareketle hedeflemeyi ifade etmek gerekirse; demografik bilgiler, tarama geçmişi, anket bilgileri ve coğrafi bilgiler gibi tüm reklam veren bilgileriyle birlikte benzersiz çevrimiçi reklam bileşenleri kullanılarak oluşturulan uygulamalardır.

DÖRDÜNCÜ BÖLÜM

ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMA UYGULAMALARININ YASAL DÜZENLEMELER KAPSAMINDA DEĞERLENDİRİLMESİ

4.1 Çevrimiçi Davranışsal Pazarlama Uygulamalarının Yasal ve Etik Bağlamı

Bir önceki bölümde detaylı olarak açıklandığı üzere ÇDP uygulamaları, internet üzerindeki kullanıcıların davranışlarını analiz ederek, kişiselleştirilmiş pazarlama stratejileri geliştirmek amacıyla kullanılan bir yöntemdir. Bu durum da yasal ve etik sorunları beraberinde getirmektedir.

ÇDP uygulamaları, kişisel verilerin işlenmesini gerektirmekte ve bu nedenle veri koruma mevzuatıyla yakından ilişkili olmaktadır. Özellikle Avrupa Birliği'nde, GVKT gibi düzenlemeler, ilgili kişi verilerinin toplanması, saklanması ve işlenmesi konusunda sıkı kurallar getirmiştir. Bu kurallar, kullanıcılara bilgilendirme yapılmasını ve gereken hallerde rızalarının alınması hakları sağlamakta, verilerin güvenliği ve gizliliği konusunda birçok farklı önlem alınmasını zorunlu kılmaktadır. Veri sorumluları, bu mevzuata uygun olarak veri toplama ve işleme faaliyetlerini gerçekleştirmek zorundadır. Ayrıca, kullanıcılara sağlanan tercih ve iptal imkanları da yasal zorunluluklar arasındadır.

Öte yandan ÇDP uygulamaları bazı etik sorunları da ortaya çıkarabilmektedir. Kullanıcıların çevrimiçi davranışlarının takip edilmesi ve kişisel tercihlerinin kullanılması; gizlilik ihlalleri ve kişisel özgürlüğe müdahale olarak algılanabilecektir. Bu nedenle, ilgili uygulamaları kullanan taraflar, etik kurallara uymak ve kullanıcıların mahremiyetini korumak için ekstra çaba göstermelidir. Kullanıcıların verilerini güvenli bir şekilde korumak, şeffaf olmak, açık ve anlaşılır bir şekilde bilgilendirme yapmak, tercihlerine saygı göstermek, kullanıcılara kontrol imkanları sunmak gibi etik prensipler önemlidir.

ÇDP, kullanıcıların tercihlerine uygun ve kişiselleştirilmiş deneyimler sunmak amacıyla kullanılan etkili bir pazarlama yöntemidir. Ancak, yasal ve etik kurallara uyum sağlanması, kullanıcıların veri güvenliği ve mahremiyetinin korunması büyük önem taşır. ÇDP uygulamalarını kullanacak taraflar, mevzuata uygun hareket etmeli, şeffaf ve etik bir yaklaşım sergileyerek, kullanıcıların güvenini kazanmalıdır.

Çalışmanın bundan sonraki kısmında ÇDP uygulamalarına yönelik kişisel verileri koruma mevzuatı kapsamındaki yasal düzenlemeler karşılaştırmalı olarak gösterilecek ve Türk hukukundaki eksiklikler değerlendirilerek ilerleyen süreçlerde uygulanması beklenen mevzuatsal değişiklikler belirtilecektir.

4.2. Çevrimiçi Davranışsal Pazarlama Uygulamalarında Etik Durumun İncelenmesi

ÇDP uygulamaları konusunda her ne kadar etik durum yasal durumdan pek ayrılamaz olsa da, ayrı bir başlık altında etik durumun kısaca incelenmesinin de uygun olacağı görüşündeyiz.

Cunningham'a göre reklam etiği, reklamcılıkta neyin doğru ve iyi olduğunun tanımıdır. Bu sadece yasal olarak ne yapılması gerektiği ile ilgili değil, aynı zamanda ne yapılması gerektiği ile de ilgilidir[159]. Bu nedenle, yasal zorunluluk, ÇDP uygulamalarının yalnızca bir yönüdür. Etik yönü de çok önemli ve değerli görülmektedir. Çünkü etik değerler otorite tarafından oluşturulamaz ve dışarıdan dayatılamaz, ancak bu mesleği icra edenlerin olağan uygulamalarıyla şekillenerek geçerli olabilmektedir[160].

Bu nedenle, ÇDP sürecine dahil olan şirketlerin de etik kaygıları olması gerekse de araştırmalara göre ilginç bir şekilde, çoğu reklam verenin yalnızca yasal zorunlulukları önemsediği görülmektedir[161].

ÇDP uygulamalarının etik bağlamı, kullanıcı gizliliği, veri güvenliği, şeffaflık ve kullanıcı kontrolü gibi yasal bağlamda da değerlendirilecek olan önemli konuları içermektedir. Pazarlamacılar, etik prensiplere uygun davranış sergileyerek, kullanıcıların güvenini kazanmalı ve kişisel verilerin doğru ve sorumlu bir şekilde kullanılmasını sağlamalıdır. Kullanıcıların gizlilik haklarına saygı göstermek ve onların tercihlerini önemsemek, ÇDP uygulamalarının etik sınırlarının korunması için kritik öneme sahiptir.

[159] Minette E. Drumwright & Patrick E. Murphy. The Current State of Advertising Ethics: Industry and Academic Perspectives, Journal of Advertising 2009, s.83
[160] Girgin, Atilla. Yazılı Basında Haber ve Habercilik Etiği, 2003, s.146
[161] Davis, Joel J., Ethics in Advertising Decisionmaking: Implications for Reducing the Incidence of Deceptive Advertising, 1994, s.380

4.3. Çevrimiçi Davranışsal Pazarlama Uygulamalarında Yasal Durumun İncelenmesi

Gizlilik ve veri koruma hukuku, bir tarafta işletmelerin hedef kitlelerini daha etkin bir şekilde anlamalarını ve hizmetlerini iyileştirmelerini sağlarken, diğer yanda kullanıcıların kişisel bilgilerinin kötüye kullanılmasını önlemeye çalışır. Bu denge, özellikle ÇDP söz konusu olduğunda karmaşık bir durum yaratmaktadır.

Avrupa Birliği'nde GVKT bireylerin kişisel verilerinin nasıl ve ne amaçla kullanılacağı konusundaki düzenlemeler için önemli bir kaynak olup bir reform niteliğine de sahiptir. GVKT, şeffaflık, bilgi edinme hakkı, verilerin silinmesi (unutulma hakkı) gibi prensipler üzerine kurulmuştur. ÇDP uygulamaları bu çerçevede kullanıcıların açık rızasını almak ve kullanıcıların veri toplama, işleme ve depolama uygulamaları hakkında bilgilendirmek zorundadır. Yine Avrupa Birliği'nde elektronik haberleşme sektöründeki hususları düzenleme amacıyla e-Gizlilik Tüzüğü ("EGT") taslağı yayınlanmış, ancak EGT henüz nihai hâlini almamış olup geçiş süreci ile birlikte 2025 yılının sonunda yürürlüğe girmesi beklenmektedir. Bu tüzükte, ÇDP kapsamında çerez uygulamaları da önemli bir konu olarak öne çıkmaktadır[162].

Amerika Birleşik Devletleri'nde ise her eyalet kendi veri koruma kanunlarını çıkarırken, bazı federal kanunlar da var olmaktadır. Kaliforniya Tüketici Gizlilik Yasası ("CCPA"), tüketicilere kişisel verilerini satmayı reddetme veya silebilme hakkı tanırken, çok sayıda diğer eyalet benzer yasaları kabul etmiştir.

Bununla birlikte, birçok ülke ÇDP uygulamalarını düzenleyen yasalara sahip bulunmamakta veya ilgili yasalar bulunsa dahi çoğu eksikliğin göz ardı edildiği durumlar gözlemlenmektedir. Bu durum, çevrimiçi etkinliklerin uluslararası niteliği göz önüne alındığında, hukuki belirsizlikler ve zorluklara yol açmaktadır.

Hem işletmeler hem de tüketiciler için çevrimiçi davranışsal pazarlama uygulamalarında yasal düzenlemelerin anlaşılması ve uygulanması büyük önem arz etmektedir. Bu, hem gizlilik haklarının korunmasını hem de veri temelli hedefleme ve pazarlamanın etkin kullanımını sağlamaktadır.

Ayrıca, devletlerin ve yasa koyucuların, teknolojinin sürekli gelişmesi ve değişmesi göz önünde bulundurulduğunda, bu konudaki yasaları ve yönetmelikleri güncel ve

[162] Aksoy ve Halıcıoğlu, 2021.

etkin tutma ihtiyacı da bulunmaktadır. Bu şekilde, ÇDP hem tüketicilere hem de işletmelere fayda sağlarken, aynı zamanda gizlilik ve veri koruma hakkına da saygı göstermiş olacaktır.

4.3.1.ABD'deki Yasal Durum

Federal Ticaret Komisyonu'nun ("FTC") ÇDP uygulamalarında veri koruma düzenlemeleri bağlamında aldığı öncü kararlar, ABD'deki yasal durumun incelenmesi bakımından büyük önem arz etmektedir. FTC 1914 yılında ABD hükümeti tarafından kurulmuştur ve amacı tüketicileri korumak ve rekabeti teşvik etmektir[163].

1990'ların başında, internet ve dijital teknolojilerin yaygınlaşmasıyla birlikte, kişisel veri korunması Amerika Birleşik Devletleri'nde önemli bir konu haline gelmiş ve bu dönemde, FTC tüketicilerin kişisel bilgilerinin korunmasına öncülük eden bir dizi önemli girişimde bulunmuştur.

1990'ların ortalarına kadar serbest piyasa ve rekabet koşullarına göre hareket eden ve internet ile dijital reklamcılığın gelişmesiyle birlikte tüketicinin korunması kapsamındaki konuları da ele alan Federal Ticaret Komisyonu, bu çerçevede çevrimiçi davranışsal pratiği inceleme konusunda da aktif rol almıştır[164].

1995'te FTC, çocukların çevrimiçi gizliliğini koruma konusuna odaklanmış ve bir dizi kamuoyu oturumu düzenlemiştir. Bu oturumlar sonucunda, 1998'de Çocukların Çevrimiçi Gizliliğini Koruma Yasası ("COPPA") kabul edilmiştir. COPPA, 13 yaşın altındaki çocukların çevrimiçi kişisel bilgilerini toplayan ve kullanabilen şirketlerin ebeveynlerden açık rıza almasını zorunluluğunu düzenlemektedir. COPPA'nın uygulanması ve düzenlenmesinden sorumlu ana kurum FTC olarak belirlenmiştir.

1999'un başlarında, FTC çevrimiçi profil oluşturma uygulamaları hakkında bir soruşturma başlatmış ve 2000 yılında mevcut kuralların uygulanmadığını belirtmiştir. 2000'li yıllarda, Gramm-Leach-Bliley Yasası uyarınca finansal kuruluşların, tüketicilerin kişisel bilgilerini nasıl kullandığına ve paylaştığına ilişkin düzenlemelerin denetlemesi yoluna gidilmiş ve finansal kuruluşlara tüketicilere gizlilik politikalarını bildirme zorunluluğu getirilmiştir.

[163] www.ftc.gov.tr,19/09/2022
[164] Keser Berber, 2014: 79

Ancak dot-com balonunun ardından reklamlarda yaşanan hızlı düşüş bu süreci yavaşlatmış ve 2007 yılında konu ile ilgili bir dizi çalışma yürütülmüştür[165].

Bu süreçte, tüketicilerin zamanla daha bilinçli hale gelmesi ve veri toplamanın güvenilirliği ile ilgili sorunların fark edilmesiyle FTC'nin çalışmaları hızlanmıştır. 2009 tarihli bir raporda, hedefli reklamcılık tüketicilere fayda sağlarken, ücretsiz içeriği desteklerken ve çevrimiçi pazarı harekete geçirirken, şirketlerin bu verileri nasıl topladığı, bir araya getirdiği, ifşa ettiği ve yok ettiği konusundaki belirsizliğin tüketiciler için önemli etkileri olduğunu belirtilmektedir. Yine aynı raporda, sektörün güçlü bir öz denetim uygulaması gerektiğini ve bu düzenleme aracılığıyla dinamik bir çevrimiçi pazarda tüketici gizliliğini koruduğunun ve koruyacağının açıkça ortaya koyulması ihtiyacı belirtilmektedir[166].

Kasım 2010'da FTC, "*Hızlı Değişim Çağında Tüketici Gizliliğini Savunmak"* başlıklı yeni bir rapor yayınlamış ve bu rapor; tüketici verilerini toplayan, depolayan, paylaşan veya başka bir şekilde kullanan çevrimiçi ve çevrimdışı ticari kuruluşların bu verilerin gizliliğini nasıl koruduğuna ilişkin kapsamlı ve yaygın olarak uygulanabilir bir çerçeve sağlamayı amaçlamıştır. Özellikle, raporun ana temalarından biri, verilerin toplanması, kullanılması ve açıklanmasına ilişkin tüketici tercihlerinin basitleştirilmesi ihtiyacıdır. Ancak, bu tüketicileri bilgilendiren ve seçim yapmalarına izin veren bir model, tüketicilerin genellikle okuyamadığı veya anlayamadığı uzun, katı yasal gizlilik politikalarıyla sonuçlanmıştır. Çünkü "Gizlilik Politikalarını Okumanın Maliyeti" başlıklı bir çalışma, tüm gizlilik politikalarını okumanın kullanıcılara günde ortalama 40 dakikaya mal olduğunu göstermiştir[167]. Bu araştırma sonuçlarının üzerine FTC yayınlanan raporları revize etmiş ve 2012'de "Privacy Framework" adlı nihai bir rapor yayınlanmıştır. Şirketler, gizlilik savunucuları, teknoloji uzmanları ve bireysel tüketicilerden daha önce yayınlanan 2010 raporuna yapılan 450 yoruma dayanarak, Federal Ticaret Komisyonu, önceki rapordaki temel ilkeleri dikkate alarak ve revize ederek nihai gizlilik çerçevesini oluşturmuştur[168]. Bu rapor, şirketlere, gizlilik hakkında tüketicileri nasıl bilgilendirecekleri ve tüketicilerin

[165] Nill, Alexander ve Aalberts, Robert J., Legal and Ethical Challenges of Online Behavioral Targeting in Advertising, 2014, s.130
[166] Leibowitz, Jon, Self-Regulatory Principles for Online Behavioral Advertising, 2009, s.1
[167] McDonald, Aleecia M. ve Cranor, Lorrie F. "Beliefs and Behaviors Internet Users" Understanding of Behavioral Advertising.", 2010.
[168] Rosch, J. Thomas, Protecting Consumer Privacy in an Era of Rapid Change, 2012, i.

kişisel bilgilerini nasıl kontrol edebilecekleri konusunda rehberlik etmek amacıyla tasarlanmıştır.

ABD sınırları dâhilinde kişisel verilerin korunması alanındaki en göze çarpan gelişme ise 2018 yılında Kaliforniya'da Tüketici Gizlilik Yasası kabul edilişi ile gerçekleşmiştir. Kaliforniya'da Tüketici Gizlilik Yasası, tüketicilere kişisel verilerini silebilme ve bu verilerin hangi amaçlarla kullanılacağını öğrenme hakkı vermiş ve tüketicilere kişisel bilgilerinin satılmasını reddetme hakkını da tanımıştır. Ek olarak 2020 yılında kabul edilen Kaliforniya Gizlilik Hakları Yasası ile de tüketicilere verilerini düzeltme, sınırlama ve taşınabilirlik hakları sağlanmıştır.

Bahsedilen bu düzenlemelere rağmen özellikle ÇDP uygulamaları konusunda aşağıda detaylı açıklanacak olan Avrupa Birliği düzenlemelerine kıyasen oldukça eksik kalan ABD düzenlemeleri günümüzde gelişen teknolojilere ayak uydurma sürecine devam etmektedir.

4.3.2. AB'deki Yasal Durum

Uluslararası arenada kişisel verilerin korunmasının gerekliliği ilk olarak Avrupa Birliği ülkelerince kabul edilmiştir. Avrupa Birliği, üye ülkelerin hukuk sistemlerinde hiyerarşik olarak en üst seviyede yer alan, anayasal statüde sayılan, tüm üye ülkeleri bağlayıcı bir hukuk sistemi oluşturmuştur. Üye ülkelerin hukuk sistemlerinde yer alan düzenlemelerin ve uluslararası alanda insan haklarını düzenleyen belgelerin kişisel verilerin korunmasına yeterli olup olmadığının incelenmesi için 1968'de Avrupa Konseyi Bakanlar Komitesi toplanmıştır. Avrupa Birliği'nin asıl amacı bilgiyi halk ile buluşturmaktır. Bu nedenle de bilgiye ulaşmak için tüm imkanlarını seferber etmişlerdir. Ancak bilgiye ulaştıkça özellikle e-ticaret arttıkça bireylere ait kişisel verilerin korunması da daha büyük önem kazanmıştır. Kişisel verilerin korunmasının ulusal ve uluslararası düzenlemelerle sağlanarak e-ticaretin yaygınlaşmasıyla ekonominin gelişmesi hedeflenmektedir[169].

Tüm bu gelişmeler Avrupa Birliği'ne üye ülkeleri de etkilemiş ve 1970'te Almanya'da merkezi bir veri bankasının kurulması ile ilgili kanun ile kişisel verilerin korunmasına ilişkin hükümler içeren kanun çıkarılmıştır. İsveç 1973'te ilk ulusal kanunu yayınlamıştır. Bu ülkeleri 1976 ve 1978 yılları arasında İspanya, Avusturya ve

[169] Tene, Omer, & Polonetsky, Jules, "To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising", 2012, s.307-308

Portekiz takip ederek kişisel verilerin korunması hususunda ülkelerinde anayasal koruma sağlamışlardır[170]. Avrupa Konseyi tarafından çıkarılan 108 sayılı Sözleşme her ne kadar Avrupa Konseyi'ne üye Avrupa Birliği'ne üye ülkelerce kabul edilmişse de bu ülkeler kişisel verilerin korunması hususunda ayrı bir düzenleme yapma ihtiyacı hissetmiştir. Çünkü Avrupa Birliği'ne üye ülkeler, kişisel verilerin korunmasına ilişkin yasalarındaki farklılıkları kaldırmak ve aralarındaki veri akışını belli kurallara bağlamak istemişlerdir. Bu nedenle de 95/46 sayılı Direktif kabul edilmiştir[171].

Avrupa Birliği 95/46 sayılı Direktif haricinde kişisel verilerin korunması hususunda Temel Haklar Şartı'nı, 2006/24/EC sayılı Direktif'i ve 2009/136/EC sayılı Direktifler'i de kabul etmiştir. Kişisel verilerin korunmasında gelinen noktada 95/46 sayılı Direktif'in de yetersiz kaldığının farkına varan Avrupa Birliği, Avrupa Konseyi ve Avrupa Komisyonu ile birlikte 2016 yılında EU 2016/679 sayılı GDPR'yi kabul etmiştir. Bu tüzük 95/46 sayılı Direktif'i 25 Mayıs 2018 tarihinde ilga ederek yürürlüğe girmiştir[172].

Kişisel verilerin korunması alanında Avrupa'da yaşanan tüm bu gelişmeler ÇDP uygulamaları kapsamındaki düzenlemeleri de beraberinde getirmiştir. Uzun yıllardır yürürlüğe konulan bu düzenlemelerden ÇDP uygulamaları kapsamında özellikle çerez uygulamaları bakımından önem arz edenleri aşağıda daha detaylı olarak incelemek Türk hukuku bakımından eksiklikleri anlayabilmek adına büyük önem taşımaktadır.

4.3.2.1 Genel Veri Koruma Tüzüğü (GVKT)

GVKT daha önce de bahsedildiği üzere Avrupa Birliği'nde (AB) 25 Mayıs 2018'de yürürlüğe giren ve kişisel verilerin işlenmesini düzenleyen bir tüzüktür[173]. ÇDP uygulamaları ve özellikle çerezlerin kullanımı genellikle kişisel verilerin toplanmasını içermekte ve bu nedenle GVKT'nin kapsamına girmektedir.

Öncelikle GVKT kapsamını ayrıntılı olarak açıklamanın uygun olacağı kanaatindeyiz.

[170] Keser Berber, 2014: 33
[171] Gare, Elisson. Profiling and Online Behavioural Advertisement Under the GDPR Has the New Regulation Succeed in Ensuring the Protection of Fundamental Rights without Hindering innovation and Economic interests in the Digital Economy?, 2016, s.18
[172] Legge, Adam. "Online Behavioural Advertising: A Comparative Study of Regulation Between the EU and Hong Kong.", 2015, s.425
[173] Küzeci, 2020: 221-222

Genel Kapsam

Bazı kişisel veriler, kötüye kullanımları halinde, ilgili kişinin, özellikle mahremiyetinin korunmasına veya ayrımcılık yasağına ilişkin temel haklarına daha fazla zarar gelmesi ihtimalinin bulunması sebebiyle, "özel nitelikli kişisel veriler" olarak adlandırılmaktadır. Özel nitelikli kişisel veriler, diğer kişisel verilerden bu bağlamda ayrılarak, onlara nazaran daha üst bir korumadan yararlanmaktadır. Nitekim özel nitelikli kişisel veriler, yalnızca yasalar kapsamında yetkilendirilen özel kurum ya da kamu kurumları tarafından, istisnai hallerde, sınırları çizilerek belirlenmiş amaçlarla, özel koşullar altında, işlenebilmektedir. Birlik hukukunda, özel nitelikli kişisel verilere ilişkin, ilk açık düzenleme, mülga 95/46 sayılı Kişisel Verilerin Korunması Direktifi'nin "Özel Veri Kategorilerin İşlenmesi" başlığı altındaki III. Kısım madde 8'de yapılmıştır. Bu madde ile üye devletlerin özel nitelikli kişisel verilerin, istisnalar dışında işlenmelerini yasaklamaları gerektiğinin altı çizilerek, bu verilerin işlenebilmelerinin, ancak ve ancak ilgili kişinin hiçbir tereddüde yer bırakmayan açık rızasının bulunması durumunda mümkün olabileceği belirtilmiştir. Mülga 95/46 sayılı Direktif'in kapsamından ise "ırksal veya etnik kökene, siyasi fikirlere, dini veya felsefi inançlara, ticaret birliği üyelikleri de dahil olmak üzere, dernek, vakıf, sendika üyeliği gibi iş ilişkilerine, adli ya da cezai soruşturma ve kovuşturmaya veyahut mahkumiyete, idari yaptırımlara, işyeri performansına, siyasi parti üyeliğine, ekonomik duruma, fiziksel ya da psikolojik sağlık durumuna, biyometrik ve genetik bilgilere, cinsel hayata ilişkin verilerin" özel nitelikli kişisel veriler olarak kategorize edildiği anlaşılmaktadır[174].

2016/679 sayılı Tüzük'ün 9/1.maddesi kapsamında, özel nitelikli kişisel verilerin, nitelikleri gereği, daha özel ve yüksek bir yasal koruma altına alınarak, bu verilerin işlenmelerinin kural olarak yasaklandığının altı çizilmiştir. Kişisel verilerin bu özel kategorisine sağlanan hassas ve özel korumanın nedeni, bu verilerin ilgili kişinin, bir ya da daha fazla belirli amaca yönelik olarak işlenebilmesi için vereceği "açık rızası" dışında yahut özel olarak verilen bu açık rızanın amacına aykırı olarak işlenerek kullanılmaları halinde, veri sahibinin "ayrımcılığa uğrama" ihtimalinin çok yüksek olmasıdır. Diğer bir ifade ile, Birlik hukuku kapsamında özel nitelikli kişisel verilere

[174] Article 29 Data Protection Working Party, (2011) "Advice Paper on Special Categories of Data ("Sensitive Data")", Ref.Ares (2011)444105 – 20.04.2011, https://www.pdpjournals.com/docs/88417.pdf adresinden 02 Haziran 2022 tarihinde erişilmiştir, s.3-8.

erişimin ve bunların işlenmesinin yasal düzenlemelerle, yasada sayılan istisnalar dışında yasaklanması vasıtasıyla, özellikle dini ve felsefi inanca, siyasi görüşe, ırk, cinsiyet, milliyet ve sağlık durumuna, cinsel eğilimlere ilişkin özel nitelikli kişisel verilerin kullanılması sonucu çeşitli şekillerde doğrudan ayrımcılık yapılması ihtimalinin önlenmesi amaçlanmaktadır. Bu sebeple de özel nitelikli kişisel verilerin ihlal edilmesinin önlenmesi babında daha yüksek bir koruma ve özen gösterilmesi gerektiği açıktır. Özel nitelikli kişisel verilerin kullanılmasıyla yapılan doğrudan ayrımcılığa örnek olarak sağlık verileri, medikal geçmiş, ya da hastalık riski gibi verilerin kötüye kullanımı verilebilir. Şöyle ki, belli bir coğrafi bölgede yaşayan insanlarda yüksek sağlık riski bulunması halinde, sigorta şirketlerinin bu bölgenin posta kodundan yola çıkarak burada yaşayan kişilere sigorta yapmamaları; bölgeyi ve bu muhitte yaşayan insanları kara listeye almaları; yahut, sigorta prim uygulamalarında aşırı fiyatlandırma yapmaları halleri, özel nitelikli kişisel veriler kullanılarak yapılan doğrudan ayrımcılığa açık örnek teşkil edebilmektedirler. Bu da özel nitelikli kişisel verilerin korunmasına özel önem verilmesi gerektiğini kanıtlar niteliktedir[175].

Avrupa Birliği Genel Veri Koruma Tüzüğü 5.maddesinde de, mülga 95/46 sayılı Direktif'te sayılan, kişisel verilerin işlenmesinde göz önüne alınması gereken ilkeler, pekiştirilip eklemeler yapılarak sıralanmıştır. Tüzük madde 5/1 (a) ile, kişisel verilerin yasal düzenlemeler çerçevesinde ve adil bir şekilde işlenmesi gerektiğine ilişkin "adil ve yasal işleme (Lawfulness & Fairness)" ilkesine ek olarak, ilgili mülga 95/46 sayılı Direktif'in giriş, kısmında bahsedilmekle birlikte, madde kapsamında yer almayan "şeffaflık (Transparency)" ilkesi de getirilmiştir[176]. Şeffaflık ilkesine göre, kişisel verilerin işlenmesine ilişkin yapılacak her türlü bildirim ve iletişimin herhangi bir yanlış, anlaşılmaya izin vermeyecek şekilde açık, sade, kolay ve anlaşılır bir dille yapılması gerekmektedir[177].

Başlangıçtan İtibaren Mahremiyet İlkesi (Privacy by default) ise, tasarlanan iş yapma süreçleri kapsamında yapılacak veri işleme faaliyetlerinin, yalnızca ilk başta belirlenerek ilgili kişilere bildirilen toplanma amacıyla sınırlı olarak yapılmasını sağlayacak nitelikteki mahremiyet dostu teknik mekanizmaların oluşturularak, bu

[175] Zarsky, Tal, Incompatible: The GDPR in the Age of Big Data, 2017, s.1012-1013
[176] Article 29, 2011: 5
[177] GDPR, Beyanlar 39

uğurda gereken önlemlerin alınmasını ifade etmektedir[178]. Tasarımla Mahremiyet İlkesi (Privacy by design) ilkesinin, kişisel verilerin korunmasında göz önüne alınması gereken "Veri Minimizasyonu" ve "Amaç ile Sınırlılık" temel ilkeleri ile doğrudan bağlantılı olduğundan ve bu bağlamda da kişisel veriler üzerinde ilgili kişilerin kontrolünün artırılmasına katkıda bulunduğundan şüphe yoktur[179].

GVKT'nin 25.maddesi kapsamında, gerek Tasarımla Mahremiyet, gerekse de Başlangıçtan İtibaren Mahremiyet ilkeleri ile veri sorumlularına kişisel verilerin korunması bağlamında oluşturacakları mekanizmalar ve kullanacakları yöntemler açısından önemli görev ve sorumluluklar yüklenmiştir[180]. Bu ilkeler vasıtasıyla, kişisel verilerin, hem tasarım aşamasından itibaren alınacak önleyici tedbirler kapsamında oluşturulacak sistemler aracılığıyla güven içinde işlenmesi, hem de amaçla sınırlı olma hususunda gereken hassasiyetin gösterilmesi garanti altına alınmaya çalışılmıştır. Alınacak bu tedbirlerle de Avrupa dijital tek pazarına duyulan güvenin yükseltilip, dijital işlemler bağlamındaki güvensizlik bariyerinin kaldırılarak, yapılacak işlem sayı ve çeşitliliğinin artırılması ve dijital ekonominin güçlendirilmesine katkı sağlanması hedeflenmiştir[181].

GVKT kapsamında işlenecek kişisel verilerin güvenliğinin, özellikle bulut bilişim gibi ileri teknoloji sistemleri dâhilinde gerçekleşebilecek güvenlik ihlal ve zaafları karşısında, en üst seviyede sağlanarak, korunabilmesi için kullanılabilecek teknik uygulamalardan bir diğeri de "Şifreleme (Encryption)" yöntemidir. Bir veri güvenliği yöntemi olan şifreleme ile, kişisel verilerin kime ait olduğuna ilişkin belirleyici olabilecek veri ve bilgilerin, gizli bir algoritma, kod veya kripto anahtarı kullanılarak gizlenmesi yoluna gidilerek, erişime yetkili olmayan herhangi bir kimsenin anlayamayacağı hale getirilen veriler ile mahremiyetin korunması hedeflenmektedir. GVKT, şifreleme (encryption) yöntemine ilişkin açık bir tanımlama getirmemekle birlikte, veri güvenliğinin ve işlemenin yasallığının sağlanabilmesi bağlamında, çeşitli maddeler kapsamında bu yöntemin kullanılmasının gereğini işaret etmektedir[182]. Şifreleme yönteminin de, kişisel verilere yetkisiz erişimin engellemesi bağlamında,

[178] Bulut Çimen, İpek. Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları, 2020.
[179] Sanchez, Noain. Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users', 2016, s.124
[180] Bulut, 2020
[181] Wachter, Sandra. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR, 2018, s.17-21.
[182] GDPR Beyanlar 83

veri güvenliğinin artırılmasına katkı sağlayacağından, tüketici güvenini artırarak, Avrupa dijital tek pazarının gelişimine katkıda bulunması beklenmektedir.

İlgili kişi rızasının, işleme faaliyetine geçmeden önce, ilgili kişi işbu işlemenin amaç, kapsam ve niteliğine ilişkin bilgilendirilmesine müteakip, alınması gerektiği unutulmamalıdır. Zira ilgili kişinin bilgilendirilmesi hususu, GVKT'ye göre, rızanın usulüne uygun verilebilmesinin esaslı unsuru niteliğindedir. Diğer bir ifade ile rızanın, ilgili kişinin serbest iradesini yansıtabilmesinin bir koşulu da, ilgili kişinin kişisel verilerinin hangi amaç ve kapsamda işleneceği ve bu işlemeye ilişkin haklarının neler olduğuyla ilgili bilgilendirilmesidir. Ayrıca rızanın geçerli sayılabilmesi için de bilgilendirmenin, en azından, "veri sorumlusunun kimlik bilgileri; işlemenin ne amaçla yapılacağı; ilgili kişiye ilişkin olarak ne çeşit verilerin toplanıp kullanılacağı; ilgili kişinin rızasını geri çekme hakkının bulunduğu; ilgili verilerin ne çeşit otomatik karar verme işlemlerinde kullanılacağı; yapılacak veri transferi faaliyetlerine ilişkin olası risklerin neler olduğu" bilgilerini içermesi gerekmektedir. Tüzük'ün Giriş (32) sayılı paragrafına göre, kişisel verilerin islenmesine ilişkin gerekli bilgilendirmeler yapıldıktan sonra ve fakat veri işleme faaliyetinden önce talep edilmesi gereken rıza, yazılı şekilde verilebileceği gibi, sözlü olarak da verilebilmektedir. Ancak yazılı beyanın ispat kolaylığı sağlayacağı da unutulmaması gereken bir husustur. Rıza, ayrıca, "bir web sitesi ziyareti sırasında onay kutucuğunun işaretlenmesi" veya "bir bilgi toplumu hizmeti sunulması esnasında teknik ayarların kullanılması" şeklinde de yapılabilen açık ve olumlu bir eylemde bulunulması vasıtasıyla elektronik ortamda da verilebilir. Ancak ilgili kişinin, bu bağlamda sessiz ya da hareketsiz kalmasının ya da önceden işaretlenmiş kutucukların bulunmasının, işbu Tüzük dâhilinde hiçbir şekilde rıza beyanı olarak kabul edilemeyeceğinin de altı yine Tüzük'ün 32.paragrafı kapsamında çizilmiştir. Özellikle elektronik ortamda ilgili kişiye yönlendirilen rıza talebinin açık olması, kısa ve öz bilgiler içermesi ve kullanılacak hizmet bağlamında ilgili kişiyi gereksiz yere rahatsız edecek, zorlayacak nitelikte bulunmaması da gerekmektedir. Yine rızanın, yapılması planlanan işleme faaliyetlerine ilişkin tüm amaçları açık bir şekilde kapsar nitelikte olması da önemlidir[183].

[183] Article 29 Data Protection Working Party (2017). "Guidelines on Consent under Regulation 2016/679, Adopted on 28.11.2017", WP259rev.01, as last revised and adopted on 10.04.2018, https://ec.europa.eu/newsroom/article29/ite-mdetail.cfm?item_id=623051 adresinden 02 Haziran 2022 tarihinde erişilmiştir.

Rızanın GVKT kapsamında geçerli kabul edilebilmesi için, veri işleme faaliyetinin başlamasından önce, açık, kesin ve olumlu bir beyan ya da eylem vasıtasıyla verilmesi gerektiğinden, ilgili kişinin rızasını geri çekme eyleminin herhangi bir şekilde geçersiz sayılması ile veri sorumlusu tarafından rızanın alınmış varsayılması da mümkün değildir[184].

Rıza, ilgili kişinin bireysel özgürlüğünün ve bilginin geleceğini belirleyebilme hakkının bir dışa vurumu olarak da nitelendirilebilir. Tüzük'ün Giriş (43) sayılı paragrafında, somut olay kapsamında, ilgili kişi ile veri sorumlusu arasında, ilgili kişi aleyhine açık bir güç dengesizliğinin bulunduğu hallerde, ilgili kişinin bireysel özgürlüğünün baskı altında olabileceği hususu da göz önüne alınarak, verilecek rızanın niteliği açıklanmıştır. Buna göre, ilgili kişi aleyhine açık bir güç dengesizliğinin bulunduğu ve özellikle de veri sorumlusunun bir kamu otoritesi olduğu hallerde, verilen rıza, somut olayın özelliklerine göre, kişisel verilerin yasal olarak işlenebilmesi için gereken geçerli rıza kapsamında addedilemeyebilecektir. Aynı paragrafta, birbirlerinden ayrı rızaya dayanması gereken, farklı kişisel veri işleme faaliyetlerine zorunlu olarak, tek seferde rıza verilmesi şeklinde düzenlenen işlemler neticesinde alınan rızanın da serbestçe verilmiş, geçerli bir rıza sayılamayacağının da altı çizilmiştir[185].

Tüzük madde 7/4'e göre, ilgili kişinin rızasının serbestçe verilip verilmediğinin tespitinde, göz önüne alınması gereken bir diğer husus da, kişisel verilerin işlenmesine ilişkin alınan rızanın, ilgili kişiye bir hizmet sunulmasını da kapsayabilen bir sözleşmenin ifası bakımından alınırken, rıza alınan hangi işleme faaliyetlerinin bu sözleşmenin ifası için gerçekten gerekli, hangilerinin gereksiz olduğunun tespitidir. Zira ilgili sözleşmenin ifa edilebilmesi için gerekli olmayan bir veri işleme faaliyetine, sözleşme kapsamında alınan rıza, serbestçe verilmiş, rıza kapsamından çıkabileceğinden, böyle bir rıza ile yapılan işleme faaliyeti de, somut olayın özelliklerine göre, meşruiyetini kaybederek, yasal işleme kapsamında sayılamayabilecektir. Tüzük madde 7/4 çerçevesinde engellenmeye çalışılan bu durum, literatürde kimi yazarlar tarafından "paketleme (bundling)", Türk hukukunda ise battaniye ya da şemsiye rızalar olarak ifade edilmektedir. Paketleme (bundling),

[184] Politou, Eugenia, Alepis, Efthimios ve Patsakis, Constantinos, Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions, 2018, s.6-7
[185] Article 29, 2017: 5-6

bir sözleşme kapsamında kişisel verilerinin işlenmesi amacıyla ilgili kişinin rızasının alınması için hazırlanan metne, bu sözleşmenin ifası için gerekli olmayan başka amaçların da eklenerek, bunlar açısından da ilgili kişinin rızasını vermeye zorlanması olarak da tanımlanabilir[186]. Eğitim hizmeti alınmasına ilişkin imzalanan hizmet sözleşmesi kapsamında, ilgili kişinin kişisel verilerinin aynı zamanda reklam faaliyetlerine ilişkin olarak da işlenmesini kapsayan rızasının alınması hali bu duruma örnek gösterilebilecektir.

GVKT, kişisel verilerin korunması ve serbest dolaşımlarının sağlanması bağlamında, ilgili kişinin bizzat kendisinin kullanabileceği hakları da düzenlemektedir. İlgili kişiye kişisel verilerine ilişkin olarak bahşedilen ve aşağıda detaylı şekilde ele alınacak olan bu haklar, "erişim hakkı, düzeltme hakkı, işlemenin kısıtlanmasını talep hakkı, itiraz hakkı, profilleme de dahil tamamen otomatik olarak yapılan herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama hakkı, veri taşınabilirliği hakkı, unutulma (silme) hakkı" şeklinde sıralanabilir. İlgili kişilere sağlanan bu haklar ile bireylerin kendi kişisel verileri üzerindeki kontrollerinin artırılması hedeflenirken, bu yolla veri sorumlularının ellerinde bulunan asimetrik gücün, ilgili kişiler lehine çevrilerek güçler dengesinin kurulması amaçlanmaktadır[187]. İlgili kişiye tanınan bu haklar ile ayrıca, eksik, yanlış, veya hatalı bir kişisel veriye dayanılarak işlem yapılmasının; yasal işleme ilkesi dışına çıkılarak kişisel verilerin işlenmesinin; ya da, yetkisiz kişilerce işleme yapılmasının önüne geçilerek; bu yolla ilgili kişinin zarara uğramasının, bizzat ilgili kişinin kendisi tarafından, birinci elden engellenebilmesi hedeflenmiştir.

Tüzük'ün 22.maddesi kapsamında ise ilgili kişinin kendisi bakımında yasal etki ve sonuç doğurabilecek nitelikte bulunan ve insan müdahalesinden uzak bir şekilde "Profilleme de dâhil, tamamen otomatik olarak yapılan, herhangi bir işleme faaliyetine dayalı olarak alınan karara tabi olmama hakkı[188]" düzenlenmiştir. Salt otomatik işleme sonucu alınan bir karara tabi olmamaya ilişkin olarak ilgili kişiye tanınan bu hak, özellikle ilgili kişiye ilişkin bir takım yasal sonuçlar ortaya koyarak, onu önemli ölçüde etkileyebilecek nitelikteki, otomatik işleme faaliyetlerine karşı kullanılabilir. İlgili

[186] Kostic, Bojana ve Penagos, Emmanuel Vargas. The Freely Given Consent and the "Bundling" Provision under the GDPR, 2017, s.217-218
[187] Goddard, Michelle. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact, t.y.
[188] Right not to be subject to a decision based solely on automated processing, including profiling

kişinin iş performansını, ekonomik durumunu, sağlık durumunu, kişisel tercihleri ve ilgi alanlarını, davranışlarını, konum ve hareketlerini içeren kişisel verilerinin tamamen otomatik bir şekilde işlenmesi halleri bu kapsamda örnek olarak sayılabilir. Bu gibi durumlarda kişisel verilerin yapay zekâlar aracılığıyla otomatik işlenmesi neticesinde ortaya konulan işleme sonuçlarına, insan müdahalesi yapılarak, nihai yorumlamanın yetkili kişilerce gerçekleştirilmesi, ilgili kişinin otomatik işleme sonucu katlanmak zorunda kalabileceği olumsuz etkilerin bertaraf edilebilmesi bakımından önem arz eder[189].

Tüzük'ün getirdiği önemli değişikliklerden bir diğeri de 20. madde kapsamında düzenlenmiştir. Bu maddeye göre, ilgili kişinin bizzat kendisinin kullanabileceği haklardan biri de "Veri Taşınabilirliği Hakkı[190]" dır. Bu hak kapsamında ilgili kişi, bizzat kendisinin veri sorumlusuna aktardığı kişisel verilerini, yaygın bir şekilde kullanılan ve makinalar tarafından yeniden okunmaya elverişli olarak yapılandırılmış, bir formatta hazırlanarak, bir başka veri sorumlusuna iletilmek üzere, kendisine teslim edilmesini yahut teknik anlamda mümkünse, elektronik ortamda, doğrudan ilgili kişinin kendisinin belirlediği yeni veri sorumlusuna gönderilmesini talep edebilir[191].

Veri taşınabilirliği hakkının, ilgili kişinin kendi kişisel verileri üzerindeki kontrolünü artırma hedefine yönelik olarak atılmış, önemli bir adım olduğunu söylemek yanlış, olmayacaktır. Bu noktada veri sorumlularının, veri taşınabilirliği hakkının kullanımını kolaylaştıracak nitelikte, birlikte çalışabilirliğin sağlandığı, kullanışlı formatlar geliştirme çalışmaları yapmaları teşvik edilmelidir[192]. Netice itibarı ile veri taşınabilirliği hakkı içeriğinde, kişisel verilerin bir kopyasının veri sorumlusundan aktarıma uygun bir formatta alınması hakkı ile bu verileri bir sorumludan, diğerine aktarabilme hakkı şeklinde tanımlanabilen, ilgili kişinin kullanabileceği iki önemli hak barındırarak, ilgili kişinin bu bağlamda kendi verileri üzerindeki kontrolünü artırmaktadır. Bu hak, günlük hayatta, kişisel verilerin sadece sosyal medya alanında değil, arama motorları, e-posta hizmetleri, çevrimiçi alışveriş siteleri, bankalar, ilaç firmaları, enerji sağlayıcıları, iletişim sektörü, havayolu şirketleri, sağlık merkezleri

[189] GDPR, Beyanlar 71
[190] Right to Data Portability
[191] Diker Vanberg, Aysem ve Ünver, Mehmet Bilal. The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?, 2017, s.3
[192] GDPR, Beyanlar 68

gibi çok çeşitli sektörler kapsamında ilgili kişi tarafından taşınabilirliklerinin sağlanması bakımından önemlidir[193].

İlgili kişi, Tüzük madde 20 kapsamında veri taşınabilirliği hakkını kullansa dahi, bu hakkın kullanılması, mevcut veri sorumlusunun sisteminde bulunan kişisel verilerinin otomatik olarak silinmesi sonucunu doğurmayacaktır. Bu sebeple ilgili kişi bu hakkını kullansa dahi, mevcut veri sorumlusundan hizmet almaya da devam edebilecektir. Ayrıca ilgili kişi tarafından veri taşınabilirliği hakkı ile birlikte, bir sonraki bölümde detaylı olarak anlatılacak olan unutulma (silme) hakkının da kullanılması durumu, mevcut veri sorumlusuna, somut olayda işbu veri taşınabilirliği hakkının kullanılmış olmasını ileri sürerek, kişisel verilerin silinmesini erteleme ya da silme işlemini reddetme hakkı da vermemektedir[194].

Madde 12/6 kapsamında, bilgi talebinde bulunan ilgili kişinin kimliği konusunda makul şüphenin oluşması durumunda, veri sorumlusunun kimlik tespiti yapabilmek adına, ilgili kişinden ek bilgi talep edebileceği hüküm altına alınmıştır. İlgili kişinin bilgilendirilmesine ilişkin olarak 12. madde kapsamında yapılan düzenlemenin uygulanması, özellikle de ilgili kişinin çocuk olduğu durumlarda, temel hak ve özgürlüklerin korunması bağlamında büyük önem arz eder[195].

Madde 29 Veri Koruma Çalışma Grubu, 2017 yılında, henüz GVKT yürürlüğe girmeden önce, bu Tüzük çerçevesinde yapılacak veri ihlal bildirimlerine ilişkin bir rehber yayınlayarak, kişisel veri ihlal çeşitlerini üç kategori altında düzenlemiştir. Buna göre, kişisel verilere ilişkin olarak yetkisiz veya kazara yapılan her türlü ifşa yahut erişim "gizlilik ihlali[196]"; kişisel verilerin yetkisiz kişiler tarafından kazara imhası yahut kayıp edilmesi "ulaşılabilirlik ihlali[197]"; kişisel verilerin yetkisiz kişilerce veya kazara değiştirilmesi faaliyeti ise "bütünlük ihlali[198]" olarak sınıflandırılmıştır[199].

GVKT'nin 32.maddesi kapsamında, kişisel verilerin işlenmesi sürecinde, ihlallerin önlenerek, makul ve kabul edilebilir bir seviyede veri güvenliğinin sağlanabilmesi için

[193] Vanberg ve Ünver, 2017: 2
[194] Article 29 Data Protection Working Party, (2011) "Advice Paper on Special Categories of Data ("Sensitive Data")", Ref.Ares (2011)444105 – 20.04.2011, https://www.pdpjournals.com/docs/88417.pdf adresinden 02 Haziran 2022 tarihinde erişilmiştir. s.7
[195] GDPR, Beyanlar 39,58
[196] Confidentiality Breach
[197] Availability Breach
[198] Integrity Breach
[199] Article 29, 2011: 6-8

gerekli tedbirlerin alınmasına ilişkin, veri sorumlusu ve veri işleyene düşen sorumluluklar düzenlenmiştir[200]. 32. madde hükmü incelendiğinde, uygun teknik ve örgütsel tedbirleri alma yükümlülüğünün eskiye oranla genişletilerek, veri sorumlusunun yanı sıra veri işleyenin de bu tedbirlerin alınmasından sorumlu olduğunun altının çizildiği görülmektedir. Buna göre; Takma ad kullanılması ve şifreleme yapılması[201]; Veri işlemeye ilişkin sistem ve hizmetlerin ihlal girişimlerine karşı, gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve dayanıklılığının sürekliliğinin sağlanması[202]; Teknik veya fiziki bir müdahalenin gerçekleşmesi durumunda kişisel verilerin yeniden kullanılabilirliğinin ve erişilebilirliğinin sağlanması[203]; İşlem güvenliğinin devamlılığını sağlamak adına alınan tedbirlerin etkinliğinin düzenli aralıklarla kontrol edilerek değerlendirilmesi[204], gibi uygulamalar, veri sorumlusu ve veri işleyenin, somut olayın özelliklerini, uygulama maliyetlerini, işleme faaliyetinin kapsam, içerik ve amaçlarını, olası riskleri birlikte göz önüne alarak, veri işleme sürecinin güvenliğinin sağlanması adına alabileceği, teknik ve örgütsel tedbirler kapsamında sayılabilirler.

Kişisel verilere yönelebilecek olası risklerin boyutları, işlenen kişisel verinin niteliği ile işlemenin kapsam ve niteliğine, kullanılan teknolojiye göre değişiklik gösterebilmektedir. Bu doğrultuda Tüzük ile kişisel verilerin işlenmesi kapsamında gerçekleşen ihlalin, ilgili kişinin temel hak ve özgürlüklerine ilişkin büyük risk oluşturduğu hallerde, salt madde 33 kapsamında veri sorumlusu tarafından denetim makamına ihlal bildiriminde bulunulmasının yeterli olmayacağı kabul edilmiştir. Bu sebeple, ihlalin ilgili kişinin temel hak ve özgürlükleri bakımından yüksek risk içermesi durumunda, Tüzük'ün 34.maddesi kapsamında, ilgili kişinin de bu ihlalin kapsam ve niteliğine, ihlalin önlenmesi için alınacak tedbirlere ilişkin olarak veri sorumlusu tarafından kolay anlaşılır şekilde, açık ve sade bir dille gecikmeksizin bilgilendirilmesi şartı getirilmiştir[205].

2017 yılında, Madde 29 Veri Koruma Çalışma Grubu, GVKT'de düzenlenen veri koruma etki değerlendirmesinin tanım ve kapsamına ilişkin bir rehber yayınlamıştır. Bu rehbere göre, "veri koruma etki değerlendirmesi", kişisel verilerin işlenmesinde,

[200] Article 29, 2011: 5
[201] GDPR, Madde 32/1 a
[202] GDPR, Madde 32/1 b
[203] GDPR, Madde 32/1 c
[204] GDPR, Madde 32/1 d
[205] GDPR, Madde 34/1,2.

işlemenin amacının, gerekliliğinin ve oranının belirlenerek, işleme sürecinin tanımlanmasına ve kişisel verilerin işlenmesinden kaynaklanabilecek ihlallerin öngörülüp, olası olumsuz etki ve sonuçlarının en aza indirilmesini sağlayacak tedbirlerin alınmasına, olanak verecek şekilde risk analizi ve yönetiminin hedeflendiği, değerlendirme, öngörü ve GVKT'nin getirdiği hükümlere uygunluk oluşturma süreci olarak tanımlanabilir. Bu bağlamda veri koruma etki değerlendirmesi yapılmasının, hem kişisel verileri işlenen ilgili kişiler, hem de bu işleme faaliyetini gerçekleştiren tüzel kişiler açısından bazı avantajları olduğu söylenebilir. Zira veri koruma etki değerlendirmesi yöntemi vasıtasıyla olası risklerin henüz gerçekleşmeden elenmesi yolu ile hem ilgili kişiler açısından temel hak ve özgürlüklerin daha iyi korunmasının sağlanmasının, hem de Tüzük'ün hükümlerine uyulmaması sebebiyle kesilecek idari para cezalarının engellenmeye çalışılmasının hedeflenmekte olduğu söylenebilir[206].

Teknolojik gelişmelere paralel olarak kapsamı, nitelik ve niceliği günden güne gelişerek artan otomatik veri işleme teknik ve süreçleri, ekonomik gayelerin gerçekleştirilmesine yönelerek, öncelikli olarak temel hak ve özgürlüklerin korunmasını hedeflemedikleri için, bu otomatik işlemelerden kaynaklanan kişisel veri ihlalleri de doğal olarak artmıştır. Bu gelişmeler, kişisel verilerin işlenmesine başlanmadan önce, amaçlanan işlemenin olası etki ve sonuçlarının incelenerek, risk analizi yapılmasının akabinde, ortaya çıkabilecek muhtemel ihlallere karşı alınacak tedbirlerin belirlenmesi bağlamında, Tüzük'ün 35. maddesi ile ortaya konan veri koruma etki değerlendirmesinin önemini bir kere daha ortaya koymaktadır. GVKT'nin 35/1. maddesinden anlaşılacağı üzere, ileri teknoloji kullanılarak yapılan ve doğası, kapsamı, içeriği ve amaçları gereği, ilgili kişinin hak ve özgürlüklerinin yüksek olasılıkla ihlali neticesini doğurabilecek nitelikteki, işleme faaliyetlerine başlanmasından önce, veri sorumlusu tarafından, veri koruma etki değerlendirmesinin yapılması zorunludur. Bu sayede önceden alınacak tedbirler vasıtasıyla, kişisel verilerin işlenmesi neticesinde ortaya çıkabilecek olumsuz sonuçların öngörülerek, engellenmesi yahut en aza indirilmesi hedeflenmektedir. Ancak her ne kadar madde 35/1'in lafzından, veri koruma etki değerlendirmesinin veri sorumlusu tarafından işleme faaliyetine başlanmasından önce yapılması gerektiği anlaşılsa da, aslında veri koruma etki değerlendirmesinin sadece bir kereye mahsus yapılması gereken bir

[206] Article 29, 2011: 4

prosedür değil, riskin ortaya çıkma ihtimalinin olduğu herhangi bir zamanda da tekrarlanabilecek bir süreç olduğu unutulmamalıdır[207].

Tüzük'ün 35/3. maddesi kapsamında ise, veri koruma etki değerlendirmesinin mutlaka yapılması gereken özel durumlar sayılmıştır. Madde 35/3'e göre, "profilleme yapılması da dâhil olmak üzere, kişilik özelliklerine dair kapsamlı inceleme yapılmasına ilişkin olan otomatik işleme faaliyetleri ile, otomatik işleme faaliyetlerinin sonuçlarının ilgili kişi hakkında yasal etkiler doğurabilecek nitelikteki önemli kararların alınmasında kullanılacak olması durumu[208]; Tüzük'ün 9/1.maddesinde ifade edilen özel nitelikli kişisel verilere ilişkin işleme faaliyetleri ile, yine Tüzük'ün 10.maddesinde belirtilen cezai hüküm ve suçlara ilişkin işleme faaliyetleri[209]; ve, halka açık alanların sistematik bir şekilde ve geniş ölçekte izlenmesine ilişkin işleme faaliyetleri[210]", veri koruma etki değerlendirilmesinin mutlaka yapılmasının gerektiği özel durumlar kapsamında sayılmıştır. Yine GVKT madde 35/4'e göre, hangi veri işleme faaliyetleri öncesinde mutlaka bir veri koruma etki değerlendirmesi yapılmasının gerektiği hususu, yetkili denetim makamlarınca özel olarak belirlenmeli ve kamuoyuna açıklanarak, bu konuda Avrupa Veri Koruma Kurulu'nu da bilgilendirilmelidir. Denetim makamının veri koruma etki değerlendirmesi yapılmasına gerek olmayan işleme faaliyetlerinin neler olduğuna ilişkin de bir liste oluşturarak kamuoyunu bilgilendirebileceği hususu da madde 35/5 kapsamında belirtilmiştir. Yapılan veri koruma etki değerlendirmesi neticesinde, işleme faaliyetinin önlem alınmaması halinde, ilgili kişi açısından yüksek risk oluşturacağı sonucuna ulaşılması halinde, işleme faaliyetine başlanmadan önce, veri sorumlusunun, denetim makamını bu hususta bilgilendirerek, izlenecek yola ilişkin olarak denetim makamına danışması gerektiği hususunun altı da Tüzük madde 36 ile çizilmiştir.

Tüzük kapsamında yapılan tanımlar incelendiğinde, GVKT ile veri sorumlusu ve veri işleyenlere ilişkin tanımlamaların değiştirilmediği ancak, bunların sorumluluklarının kapsam ve içeriklerinin genişletildiği görülmektedir. Nitekim Tüzük ile kişisel verilerin işlenmesinde, veri işleyenlere de veri sorumluları ile aynı seviyede sorumluluk yüklenmiş ve kişisel verilerin korunması hususunda, Tüzük kapsamında

[207] Article 29, 2011: 14
[208] GDPR, Madde 35/3 a
[209] GDPR, Madde 35/3 b
[210] GDPR, Madde 35/3 c

ortaya çıkabilecek hukuka aykırılıklardan, veri sorumlusu ve veri işleyenleri birlikte sorumlu tutulmuşlardır[211].

Tüzük'ün 37.maddesine göre; yargılama yetkileri kapsamında hareket eden mahkemeler hariç olmak üzere, kişisel verilerin işlenmesinin bir kamu kurum ya da makamı tarafından gerçekleştirilmesi durumunda[212]; veri sorumlusu veya veri işleyenin esas faaliyet alanının, kişisel verilerin büyük ölçekte toplanarak, düzenli ve sistematik olarak izlenip işlenmelerini gerektiren faaliyetleri kapsadığı hallerde[213]; özel nitelikli veriler ile suç ve mahkumiyetlere ilişkin kişisel verilerin büyük ölçekte işlenmeleri durumlarında[214], veri sorumlusu veya işleyen tarafından yapılan işleme faaliyeti kapsamında bir veri koruma görevlisi atanması zorunluluk arz eder. Bu durum, ilk kez GVKT madde 37/1 ile ortaya konan yasal bir zorunluluktur[215]. Madde 37/1'de sayılanların dışındaki başka işleme faaliyetleri kapsamında da, gerekli görüldüğü takdirde, üye devletler ya da Birlik tarafından zorunlu olarak bir veri koruma görevlisi atama yükümlülüğü getirilebileceğinin altı da madde 37/4 ile çizilmiştir.

Veri koruma görevlileri, aynı zamanda adlarına işlem yaptıkları kurum ve kuruluşlar ile denetim makamları ve ilgili kişiler arasında arabuluculuk yaparak karşılıklı iletişimin sağlanmasına da katkıda bulunurlar. Tüzük madde 37/5 ile veri koruma görevlisinin hangi alanlarda uzman kişiler arasından seçilerek atanması gerektiğine ilişkin bir açıklama getirilmediği görülmektedir. Ancak, veri sorumlusu ve veri işleyen tarafından atanacak veri koruma görevlisinin, kişisel verilerin korunmasına ve özellikle de GVKT'nin yorumlamasına ilişkin mesleki yeterliliğe sahip uzman kişiler arasından seçilmesinin uygun olacağı anlaşılmaktadır. Veri koruma görevlisinin, görevlerini yerine getirirken, kişisel verilerin işlenmesinden etkilenen ilgili kişinin de görüşünü alması önemlidir[216]. Yine Tüzük'ün 37/7.maddesine göre, şeffaflık ve hesap verebilirlik ilkeleri doğrultusunda, veri koruma görevlisinin iletişim bilgilerinin yayınlanması ve bu bilgilerin denetim makamına da bildirilmesi gerekmektedir.

[211] GDPR, Beyanlar 13
[212] GDPR, Madde 37/1 a
[213] GDPR, Madde 37/1 b
[214] GDPR, Madde 37/1 c
[215] Article 29, 2011: 4-5
[216] Article 29 Data Protection Working Party. (2016) "Guidelines on the Right to Data Portability", adopted on 13 December 2016 as last revised and adopted on 5 April 2017, WP 242, rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 , adresinden 18 Haziran 2022 tarihinde erişilmiştir. s.11

İletişim bilgilerinin, gerektiğinde ilgili kişi veya denetim makamının, veri koruma görevlisine rahatlıkla ulaşabilmelerini sağlayacak kapsam ve yeterlilikte bilgi içermesi önemlidir[217].

Avrupa Veri Koruma Kurulu'nun yetki ve görevlerinin temelleri, GVKT'nin Birlik genelinde tutarlı ve doğru bir şekilde yorumlanarak, yeknesak uygulanmasının sağlanması hedefi ile kişisel verilerin korunmasında denetim makamları arasında etkili işbirliğinin gerçekleştirilmesi hedefinde yatmaktadır[218]. Bunu temin için de, Avrupa Veri Koruma Kurulu, Tüzük'ün 70. maddesi kapsamında sayılan, çeşitli konularda Komisyon'a danışmanlık yapma; Tüzük'ün yorumlanıp uygulanmasına yönelik çeşitli rehber ve tavsiyeler yayınlama ile bunların uygulanmasını denetleme; Üye devletlerarasında işbirliği ve bilgi paylaşımını teşvik etme; Denetim makamları ve mahkemeler tarafından tutarlılık mekanizmasına ilişkin olarak alınan kararlarla ilgili kamuya açık dijital sicil tutma, gibi çeşitli görevleri yerine getirmekle yükümlüdür. Madde 70/1 (t)' ye göre ise, Avrupa Veri Koruma Kurulu'nun, Tüzük'ün 65.maddesi kapsamında, bireysel vakalara ilişkin uyuşmazlıkların çözümüyle ilgili olarak aldığı kararlar ile hak kayıplarının önüne geçilebilmesi amacıyla Tüzük madde 66 ile düzenlenen "acil durum prosedürü[219]" kapsamında aldığı kararlar, bağlayıcı olmaktadır.

Tüzük'ün kabulünden önceki dönemde, kişisel verilerin sınırlar arası ihlallerine ilişkin, benzer konularla ilgili olarak farklı üye devletlerde verilen, farklı kararlar bulunmakta idi. Bu durum göz önüne alındığında, Tüzük'ün 63 ve 64. maddelerinde bahsedilen "tutarlılık mekanizması[220]"nın önemli parçalarını oluşturan, denetim makamları ile Avrupa Veri Koruma Kurulu'nun, Birlik genelinde Tüzük'ün yeknesak bir şekilde uygulanması çabalarına, önemli katkılarda bulunacağı daha net bir şekilde anlaşılmaktadır. Zira Tüzük vasıtasıyla yapılan düzenleme ile birden fazla üye devleti ilgilendiren sınır aşan sorunların çözümünde üye devletlerde bulunan denetim makamlarına, Avrupa Veri Koruma Kurulu'nun görüşünü bekleme yükümlülüğü getirilmiştir[221]. Bu güçlendirilmiş, işbirliği formülü ile hesap verebilirlik ilkesi

[217] Article 29, 2016: 12
[218] Giurgiu, Andra ve Lommel. Gerard. A New Approach to EU Data Protection, More Control Over Personal Data and Increased Responsibility, 2014, s.26
[219] Urgency procedure
[220] Consistency mechanism
[221] Başalp, Nilgün. Avrupa Birliği Veri Koruma Genel Regülasyonunun Temel Yenilikleri, 2015, s.86-87

doğrultusunda, benzer konularda, birbiriyle tutarlı kararlar alınarak, kişisel verilerin yeknesak uygulamalarla korunması sağlanıp, tek pazarın güvenilirliğine katkıda bulunulması da hedeflenmektedir. Bu durumun uzun vadede, tüketici güvenini yükseltip, Avrupa dijital tek pazarındaki işlem hacmini artırarak, ekonomik büyümeye katkıda bulunacağı unutulmamalıdır[222].

Bir ticari değer olduğu genel kabul gören verilerin serbest dolaşımlarının sağlanmasına ilişkin düzenlemeler, Birlik'in kuruluşundan itibaren ortaya konan temel değerler göz önüne alındığında şaşırtıcı değildir. Buna paralel olarak da, GVKT, kişisel verilerin Birlik düzeyinde uyumlaştırılmış, yasalar dâhilinde en iyi şekilde korunarak, verilerin Avrupa Birliği sınırları içerisinde serbest dolaşımlarının teminini ilke edinmiştir. Küreselleşmenin etkileri ile uluslararası ticaret hacminin artması ve dijital teknolojilerin hızlı gelişimiyle birlikte, kişisel veriler, Birlik dışındaki üçüncü ülkelere ve uluslararası organizasyonlara her geçen gün daha da artan oranlarda aktarılarak, Birlik dışındaki çeşitli sunucular (serverlar) aracılığıyla, depolanıp işlenmeye başlanmışlardır. Engellenemeyen bir şekilde, yüksek miktarlara ulaşan bu veri aktarımları, beraberinde kişisel verilerin Birlik sınırları ötesinde de korunmalarının garanti altına alınması ihtiyacını ortaya çıkarmıştır. Ortaya çıkan bu ihtiyaç sebebiyle de, Tüzük kapsamında, veri aktarımı yapılacak üçüncü ülke veya uluslararası organizasyonlar tarafından, kişisel verilerin, Birlik düzeyinde korunmasının garanti edilmesi kaydıyla, buralara kişisel verilerin aktarımına, belli koşullar altında Komisyon tarafından izin verilebileceği düzenlenmiştir. Kişisel verilerin tıpkı Birlik içinde olduğu gibi, aynı seviyede korunmasının garanti altına alınarak Birlik dışına aktarılmalarına izin verilmesiyle, bu verilerin güvenli bir şekilde serbest dolaşımlarının sağlanması da ulaşılmaya çalışılan hedefler arasındadır[223]. Yapılan yasal düzenlemeler ve alınan tedbirlerle, Birlik dışındaki üçüncü ülkelere ya da uluslararası şirket ve diğer organizasyonlara, her ne şekilde olursa olsun, transfer edilen kişisel verilerin, Birlik içinde tutulanlarla aynı korumadan yararlanması hedeflenmektedir. Bu durum, Tüzük'ün getirdiği hüküm ve koşullar ile bunların ortaya koyduğu korumanın, kişisel verilerle birlikte Birlik dışına taşınarak, -bir diğer ifade ile

[222] Buttarelli, Giovanni, The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", 2016, s.77
[223] GDPR, Beyanlar 3,6,101

kimi koşullar altında Tüzük'ün bölgesel kapsamı genişletilerek- aynı şekilde uygulanması olarak da ifade edilebilecektir.

2016/679 sayılı Tüzük'ün 45.maddesine göre, üçüncü bir ülkenin, belli bir bölgenin, üçüncü ülke kapsamındaki belirli bir sektörün yahut bir uluslararası organizasyonun, kişisel verilere ilişkin Avrupa Birliği düzeyinde yeterli koruma sağladığına, Komisyon tarafından kanaat edildiği takdirde, Komisyon'un özel olarak alacağı ve Avrupa Birliği'nin resmi gazetesinde yayınlanacak bir "yeterlilik kararı" kapsamında, işbu kararda anılan yerlere, bu yerler tıpkı Birlik içindeymiş gibi, başkaca herhangi bir koşul aranmaksızın, kişisel veri transferi yapılabilecektir. Madde 45 kapsamında yeterlilik kararının verilmesinden önce, Komisyon, özellikle ilgili üçüncü ülke veya uluslararası organizasyonda, hukukun üstünlüğüne, temel hak ve özgürlüklere saygı gösterilmesinin gereğinin yasal düzenlemeler ve bunların uygulanmaları bağlamında yerine getirilip getirilmediğini; ilgili kişi haklarını korumaya yönelik etkili ve uygulanabilir yasa hükümleri ile yaptırım mekanizmalarının var olup olmadığını; ilgili kişi haklarını kullanmasına etkin bir şekilde yardım edecek ve onlara yol gösterecek nitelikteki bağımsız denetim makamlarının varlığını, teyit etmelidir. Madde 45/3'e göre ise, bu koşulların korunup korunmadığı, en az dört yılda bir olmak üzere, dönemsel olarak kontrol edilmelidir. Bu kontroller sonunda yeterli koruma seviyesinin yitirildiğinin tespiti halinde de, bu yerlere yapılan kişisel veri aktarımı yasaklanabilecektir[224].

Aktarılacak kişisel verilerin korunması hususunda, uygun önlemlerin alınıp alınmadığının tespitinden önce verilerin hangi üçüncü ülke ya da uluslararası organizasyona aktarılacağı ile aktarılacak verilerin kapsam ve niteliğinin belirlenmesi gerekmektedir. Ancak bu ön tespitlerin yapılmasından sonra, kişisel verilerin korunması hususunda, ilgili üçüncü ülke ya da uluslararası organizasyon tarafından yeterli ve uygun önlemlerin alınıp alınmadığının incelenmesi yerinde olacaktır[225].

Yapılan bu yeni düzenlemeler, mülga 95/46 sayılı Direktif'teki düzenlemelerle karşılaştırıldığında, kişisel verilerin işlenmesinde hukuka aykırı davranılması durumunda, Tüzük ile veri sorumlusu ve veri işleyenlere yüklenen sorumluluğun da, birbirleriyle eşit düzeye getirilerek, genişletildiği görülmektedir. Ayrıca yine Tüzük

[224] GDPR, Beyanlar 103,104,107
[225] Miri, Mina, Foomany, Farbod H. and Mohammed, Nathanael. Complying with GDPR: An Agile Case Study, 2018, s.6

kapsamında kişisel verilerin korunması hususunda karşılaşılan sorunlara, daha elverişli çözüm mekanizmaları getirilmeye çalışıldığı da anlaşılmaktadır. Bu bağlamda, Tüzük'ün kabulüyle, kişisel verilerin hukuka aykırı işlenmeleri sonucu uygulanacak yaptırımların, Birlik düzeyinde uyumlu hale getirilerek, idari para cezası miktarları da dâhil, yaptırımların kapsam ve içerikleri artırılmıştır. Denetim makamları Tüzük kapsamında getirilen yaptırımları uygularken her bir somut olayın özelliğini ayrı ayrı değerlendirerek karar vermekle yükümlüdürler. Bu yaptırımların etkili, orantılı ve caydırıcı nitelik taşımaları ve Birlik çapında aynı ya da benzer nitelikteki ihlallere eşdeğer yaptırımlar getirilerek uygulamada tutarlılığın sağlanması gerekmektedir. Yaptırımların uygulanmasında Birlik çapında uyumun yakalanabilmesi için ise, düzenli yapılacak atölye çalışmaları gibi çeşitli işbirliği mekanizmaları aracılığıyla denetim makamları arasında bilgi paylaşımı ve aktif katılımın sağlanması önemlidir[226]. Tüzük ile yaptırımların, Birlik düzeyinde uyumlu hale getirilmesinin, Avrupa dijital tek pazarının parçalı görünümünden kurtularak uyumlu işleyebilmesi yönünde atılmış bir başka önemli adım olduğu söylenebilir.

GVKT ile siyasi baskı da dâhil her türlü baskıdan uzak tutularak bağımsız niteliklerinin korunacağının altı çizilen denetim makamlarının, işbu Tüzük hükümlerinin etkili uygulanmasının sağlanmasına ilişkin önemli yetkilerle donatıldığı görülmektedir[227]. Zira Tüzük madde 77 kapsamında, kişisel verilerinin, yasal olmayan şekillerde işlendiğini düşünen ilgili kişinin, ilgili denetim makamlarına başvurarak, şikâyette bulunma hakkı düzenlenmiştir. Denetim makamı, ilgili kişinin yapmış olduğu şikâyeti değerlendirirken, bu şikâyetin gidişatına ve sonucuna ilişkin ilgili kişiyi bilgilendirerek haberdar etmekle yükümlüdür. Denetim makamı, yapılan bu şikâyet başvurusunu cevapsız bırakır ya da şikâyetin gidişatına veya sonucuna ilişkin ilgili kişiyi üç ay içerisinde bilgilendirmez ise, ilgili kişinin, Tüzük madde 78'e göre, denetim makamları karşı "etkili hukuk yollarına başvuru hakkı[228]" da bulunmaktadır. Etkili hukuk yollarına başvuru hakkı kapsamında, her gerçek ve tüzel kişinin, denetim makamlarının verdiği bağlayıcı nitelikteki kararlara karşı, ilgili denetim makamının yerleşik bulunduğu üye devlet mahkemelerinde yargı yoluna başvuru haklarının da

[226] Article 29 Data Protection Working Party. (Ekim 2017) "Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation", 2016/679, 17/EN WP 253, 3.10.2017, https://knowww.eu/search-tree?t=5ad7131ed39f5-aa2bcbf0f34# , adresinden 11 Haziran 2022 tarihinde erişilmiştir.
[227] Article 29, Ekim 2017.
[228] The Right to an Effective Judicial Remedy

bulunduğunun altı yine Tüzük'ün 78.maddesinde çizilmiştir. Denetim makamlarının bağlayıcı kararlarına karşı, ilgili kişiler tarafından yetkili mahkemelere başvurulması halinde, uyuşmazlıkların çözümü hususunda bu mahkemeler tam yargı yetkilerini kullanarak her türlü hususu inceleyebileceklerdir.

Kişisel verilerin ihlali halinde uygulanacak idari para cezalarının üst limitleri, söz konusu ihlalin kapsam ve niteliğine göre, Tüzük'ün 83/4 ve 83/5.maddelerinde iki kategori halinde düzenlenmiştir. GVKT ile getirilen idari para cezalarının niteliklerine bakıldığında bu cezaların, Tüzük kapsamında doğrudan uygulanan en güçlü yaptırım mekanizmaları olduğu söylenebilir. Tüzük'ün 83/5.maddesi kapsamında düzenlenen ve ağır ihlaller olarak nitelendirilebilen durumlarda, sorumlulara, 20 milyon Euro'ya kadar veya bir önceki mali yılın küresel cirosunun %4'üne kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası kesilebilmektedir. Tüzük madde 83/4'te ise, daha hafif ihlaller için, 10 milyon Euro'ya veya bir önceki mali yılın küresel cirosunun %2'sine kadar –hangisi daha fazla ise o uygulanacak şekilde- idari para cezası uygulanabileceği hüküm altına alınmıştır[229].

GVKT ve ÇDP Uygulamaları

GVKT'nin belki de çerez politikalarına en doğrudan etkisi, rıza ilkesidir. GVKT, çerezlerin yerleştirilmesi dâhil olmak üzere kişisel verilerin işlenmesi için açık ve olumlu bir onay gerektirir. Bu, kullanıcıların web sitesini ilk ziyaret ettiklerinde genellikle bir çerez bildiriminde belirtilmektedir. İlgili bildirim, web sitesinin çerezleri nasıl ve ne amaçla kullandığını açıklamalı ve kullanıcının çerez kullanımını kabul etme veya reddetme seçeneğine sahip olmalıdır. Bu seçenekler, kullanıcıların verilerinin nasıl kullanılacağı konusunda bilinçli bir karar vermesini sağlamaktadır. Çerez bildirimleri ve gizlilik politikaları gibi onay mekanizmaları, şeffaf, kolay erişilebilir olmalı ve kullanıcılara tercihlerini ayrıntılı bir şekilde kontrol etme imkânı sunmalıdır[230].

GVKT'nin şeffaflık ilkesi, veri işleme süreçlerinin kullanıcılara açık bir şekilde bildirilmesini zorunlu tutmaktadır. Bu ilke kapsamında, özellikle çerez politikalarında, veri sorumluları çerezlerin nasıl ve neden kullanıldığını açıklamak ile yükümlü

[229] Golla, Sebastian. Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, 2017, s.74

[230] Interactive Advertising Bureau (IAB). (2023). Understanding the Transparency & Consent Framework v2.2. https://iabeurope.eu/blog/understanding-the-upcoming-transparency-consent-framework-v2-2/ adresinden 26 Nisan 2023 tarihinde erişilmiştir.

olmaktadır. Şeffaflık ilkesi, web sitesinin hangi çerezleri kullanıyor olduğunu, bu çerezlerin ne tür veri topladığını, bu verilerin ne için kullanılacağını ve bu verilerin ne kadar süreyle saklanacağını belirtilmesini gerektirmektedir[231].

Veri minimizasyonu ilkesi uyarınca kişisel veriler yalnızca belirli bir amacın yerine getirilmesi için gerekli olduğu ölçüde toplanılmalı ve işlenmelidir. Bu, çerez politikalarına, yalnızca kullanıcı deneyimini iyileştirmek veya site işlevselliğini sağlamak için gerekli olan çerezlerin kullanılması şeklinde uygulanmaktadır[232].

GVKT, gizliliği korumak için maskeleme, psödonimizasyon ve anonimleştirme gibi tekniklerin kullanımını teşvik etmektedir. Psödonimizasyon, tanımlanabilir bilgileri bir takma adla değiştirirken, anonimleştirme veriyi geri dönüşü olmayacak şekilde dönüştürerek artık bir bireye atfedilemez hale getirmektedir. Bu yöntemler, kişisel verilerin doğrudan bir bireyle ilişkilendirilmesini sınırlayarak çevrimiçi davranışsal pazarlamada gizlilik risklerini azaltmaya yardımcı olacak seçenekler olarak belirtilmektedir[233].

ÇDP gibi yüksek riskli veri işleme faaliyetlerinde bulunan veri sorumlularının süreç hakkında etki değerlendirmesi yapması gerekmektedir. Bu değerlendirmeler, ilgili kişilerin gizliliği üzerindeki etkileri değerlendirmekte ve potansiyel riskleri belirlemek ve ele almak için yardımcı olmaktadır. Etki değerlendirmeleri, işletmelerin gizlilik odaklı uygulamaları benimsemesine ve GVKT'ye uyumu sağlamasına destek olmaktadır.

GVKT ile ilgili kişilere tanınan belirli haklar bulunmaktadır. Bu kapsamda ilgili kişilerin verilerine erişim hakkı, verilerinin düzeltmesini isteme hakkı, verilerinin silinmesini talep etme ("unutulma hakkı") hakkının yanı sıra, veri taşınabilirliği ve veri işlemeye itiraz etme hakkı da bulunmaktadır. Veri sorumluları tarafından yayımlanacak olan çerez politikaları da sayılan bu hakları desteklemeli ve kullanıcıların bu hakları nasıl kullanabileceklerini ayrıntılı olarak açıklamalıdır.

Son olarak, hesap verebilirlik ilkesi uyarınca veri sorumluları GVKT uyumluluklarını sağlamak ile yükümlüdür. Bu, çerez politikalarının ve uygulamalarının düzenli olarak

[231] IAB, 2023
[232] GDPR EU (2020). Cookies, the GDPR, and the ePrivacy Directive. https://gdpr.eu/cookies/ adresinden 18 Ocak 2023 tarihinde erişilmiştir.
[233] GDPR EU (t.y.). A guide to GDPR data privacy requirements. https://gdpr.eu/data-privacy/ adresinden 10 Aralık 2022 tarihinde erişilmiştir.

gözden geçirilmesi ve güncellenmesi ve hâsıl olduğunda gerekli düzeltmelerin yapılması anlamını taşımaktadır.

GVKT, dijital alanda gizlilik hakları ve veri koruması için yeni bir dönemi başlatmıştır. Çevrimiçi davranışsal pazarlama, hala işletmeler için güçlü bir araç olmasına rağmen, bireylerin gizliliklerini ve kişisel verileri üzerinde kontrolü önceliklendiren bir çerçeve altında faaliyet göstermektedir. GVKT'nin prensip ve gerekliliklerine uyum sağlamak, sorumlu ve etik pazarlama uygulamalarını ve dijital çağda işletmeler ile tüketiciler arasındaki güveni sağlamaktadır.

GVKT düzenlemeleri kapsamında uygulanabilirliği desteklemek, problemleri ve çözüm yollarını belirtmek ve yol haritası çizmek adına hem Avrupa Veri Koruma Otoritesi hem de yerel veri koruma otoriteleri tarafından çok çeşitli rehber ve kararlar yayımlanmaktadır. ÇDP uygulamaları ve bu uygulamalar kapsamında özellikler çerezler bu rehber ve kararlara fazlaca konu olmuştur.

Bunlardan biri olan ve İngiltere Veri Koruma Otoritesi (“ICO”) tarafından yayımlanan Doğrudan Pazarlama Rehberi; GVKT, İngiltere Veri Koruma Kanunu ve Elektronik İletişim Yönetmeliği kapsamında doğrudan pazarlama konusunda önemli bir yol haritası niteliğine sahiptir.

Doğrudan Pazarlama Rehberi ile organizasyonların, arama yapma, mesaj gönderme, e-posta gönderme veya çevrimiçi reklamlarla hedef kitleye ulaşma gibi herhangi bir yöntemle pazarlama iletileri gönderirken ulusal ve uluslararası düzenlemeleri dikkate almaları gerekliliği vurgulanmaktadır. Bu gereklilik ile sadece GVKT ve İngiltere Veri Koruma Kanunu’na değil, aynı zamanda genel kapsamda elektronik iletişimlere uygulanan Elektronik İletişim Yönetmeliği’ne de atıf yapılmaktadır.

GVKT ve İngiltere Veri Koruma Kanunu, organizasyonların kişisel verileri adil ve şeffaf bir şekilde işlemesi yükümlülüğünü düzenlemektedir. GVKT kapsamında, doğrudan pazarlama için geçerli bir sebebin bulunması ve ilgili kişilerden alınacak rızanın belirli bir amaçla, özgür iradeye dayanarak ve bilgilendirmeye dayanması şartları aranmaktadır.

Doğrudan Pazarlama Rehberi’nde açıklandığı üzere Elektronik İletişim Yönetmeliği’nin uygulandığı durumlarda, sms mesajları ve e-postalar için, mevcut müşterilere yönelik "yumuşak tercih" olarak bilinen bir istisna getirilmiştir. Bu kural, organizasyonlara, iletişim bilgilerinin bir satış veya satış görüşmesi kapsamında elde

edildiği durumlarda, aynı/benzer ürünlerin veya hizmetlerin her ileti içeriğinde ret imkânı sunmak kaydıyla ayrıca rıza almaksızın tanıtımına imkân sağlamaktadır.

Doğrudan Pazarlama Rehberi ile veri sorumlusu organizasyonların, ilgili kişilerin haklarını nasıl kullanabileceklerini, rızalarını nasıl geri çekeceklerini ve doğrudan pazarlamadan çıkma gibi haklarını nasıl kullanabileceklerini açık bir şekilde belirtme yükümlülüğü tekraren vurgulanmıştır.

ICO ayrıca, üçüncü taraflardan müşteri bilgilerinin tedarik edildiği hallerde işlenen verilerin hukuka uygun elde edildiğinden ve ilgili kişilere karşı aydınlatma, gerektiği takdirde de rıza alma yükümlülüğünün yerine getirildiğinden emin olunması gerektiğini de belirtmektedir[234].

Son olarak, GVKT düzenlemeleri ile paralel olarak veri sorumlularının şeffaflık ilkesine uyum sağlamalarının önemi vurgulanmaktadır. Yasal yükümlülüklere uyumun sağlanması konusunda proaktif bir yaklaşım benimsenmesi, kapsamlı ve etkili politika ve prosedürler hazırlanması, veri koruma önlemlerinin alınması, çalışanlara konu kapsamında uygun eğitimlerin sağlanması ve gerekli teknik tedbirlerin alınması konusunda uyarılarda bulunulmaktadır.

4.3.2.2 2002/58/EC Sayılı e-Gizlilik Direktifi

e-Gizlilik Direktifi'nin, 1. maddesi ile yayım amacı kişisel verilerin işlenmesi bağlamında elektronik iletişim alanında mahremiyetin korunmasını olarak belirlenmiştir.

Günümüze dek Direktif'te çeşitli güncellemelere gidilmiş fakat son tahlilde aynı GVKT'nin gelişimi gibi tüm üye ülkelerde yeknesak bir düzen kurulma amacı kapsamında yeni bir regülasyon ihtiyacının hasıl olduğuna karar verilmiştir. Aşağıda henüz yürürlüğe girmemiş olan e-Gizlilik Tüzüğü başlığına ayrıca değinilecektir.

Direktif'in yürürlüğe girdiği süreçten, 2009 yılına gelindiğinde Direktif üzerinde çeşitli değişiklikler yapılmış ve bu ilgili değişiklikler arasında çerez kullanımının ilgili kişilerin rızası kapsamına alınması da dâhil edilmiştir. Bu bağlamda ilgili değişiklikler

[234] Information Commissioner's Office (ICO Consent). (t.y.). What is valid consent? İngiltere https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/#:~:text=All%20consent%20must%20involve%20a,(whether%20oral%20or%20written) adresinden 22 Ocak 2023 tarihinde erişilmiştir.

Direktif'in "Çerez Kanunu" olarak anılmasına da sebebiyet vermiştir[235]. Üye ülkelerin Direktif'i kendi yerel mevzuatlarına aktarmaları sırasında çeşitli değişiklikler meydana gelmiş ve aynı 95/46/EC Direktif'inde olduğu gibi yeknesak bir düzenleme olma özelliği kazanamamıştır.

Direktif'e değişiklikler kapsamında eklenen çerez düzenlemelerine değinmek de uygun olacaktır. İlgili değişiklikler kapsamında getirilen en çarpıcı düzenleme çerez kullanımının ilgili kişi rızasına tabi kılınmasıdır. Çerezler, hukuka uygun amaçlar doğrultusunda verilerin işlenmesini gerektirmekte ve işlenecek kişisel verilere erişim, yalnızca hukuka uygun amaçlar varsa mümkün olabilecektir. İlgili kişilerden alınacak rıza öncesinde mutlaka işleme amaçları hakkında açık ve kapsamlı bir şekilde bilgilendirme yapılmalıdır. Direktif'in 5. maddesinin 3. fıkrasına göre, verilerin depolanması veya düzenleme öncesinde hâlihazırda depolanmış olan verilere erişim elde edilmesi, ilgili kişinin açık ve kapsamlı bilgilendirme neticesinde rızasını vermiş olması şartına bağlıdır. Direktif bu zorunlu rıza kuralına bazı istisnalar da getirmiştir[236].

Kullanılan çerezlerin türünden bağımsız olarak, veri sorumluları ilgili kişileri bilgilendirmekle yükümlüdür. Bu bilgilendirme, kullanıcının bir web sayfasına girdiği anda ve karşısına çıkan ilk sayfada açık, kapsamlı ve görünür bir bildirim şeklinde yapılmalıdır. Bu bildirimde, kullanıcıların tüm çerez türlerine ilişkin bilgilere erişebilmesi sağlanmalıdır. Ayrıca, varsa kullanılan üçüncü taraf çerezler ve çerezler yoluyla veri aktarımı ile çerezlerin saklama sürelerine ilişkin konular da bilgilendirme kapsamında yer almalıdır. Bilgilendirme metni mutlaka açık ve anlaşılır olmalıdır, karmaşık ve gereğinden fazla teknik bilgi içeren metinler bilgilendirme amacını gerçekleştiremeyeceğinden Direktif uyarınca kabul edilmemektedir. İlgili kişilere mutlaka çerezler konusunda kabul etme ve reddetme seçenekleri sunulmalı, ayrıca bu tercihleri daha sonra nasıl değiştirebilecekleri de açıklanmalıdır.

Öte yandan üçüncü taraf çerezleri kullanıldığı durumlarda ilgili kişilerin tüm veri sorumluları hakkında bilgi sahibi olabilmesi için üçüncü tarafların kapsamlı ve güncellenen bir listesinin paylaşılması da yine Direktif kapsamında önerilmektedir.

[235] Aksoy ve Halıcıoğlu, 2021
[236] Information Commissioner's Office (ICO Cookies). (t.y.). Guidance on the use of cookies and similar technologies. İngiltere. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf adresinden 15 Aralık 2022 tarihinde erişilmiştir.

Bilgilendirme sonrası, ilgili kişilerden alınacak rızanın GVKT ile paralel olarak, mutlaka özgür iradeyle belirli bir konuya ilişkin ve bilgilendirmeye dayalı olarak alınmış olması gerekmektedir. Rızanın geçerli olabilmesi için kullanıcın aktif bir hareketi aranmakta olup, önceden işaretlenmiş kutucuklarla alınan rızalar geçerlilik unsurunu sağlamayacaktır. İlgili kişilerden çerezlere dair alınacak rıza, mümkün olduğu takdirde seçim yapma imkânı verilerek ve katmanlı bir şekilde sunulmalıdır[237]. Bu durum yine GVKT'nin 43. maddesinde ilgili kişinin farklı kişisel veri işleme amaçlarına karşı ayrı ayrı rıza verme imkânının olmaması durumunda, rızanın özgür iradeyle verilmiş sayılmayacağı düzenlemesi ile aynı kapsamda değerlendirilebilecektir.

Direktif kapsamında çerez kullanımına yönelik rıza alma zorunluluğuna getirilen bazı istisnalar da düzenlenmiştir. WP 29 tarafından "Kriter A" ve "Kriter B" olarak adlandırılan istisnalar kapsamında ilgili kişilerin rızası olmadan da işleme faaliyetinin gerçekleştirilebileceği durumlar belirlenmiştir.

"Kriter A" çerezleri, kullanılması iletişimin sağlanması için mutlak surette zorunlu olan çerezleri nitelendirmektedir. (i) *İletişimin rotasını ve* doğru noktaya ulaşmasını sağlayan çerez uygulamaları, (ii) verilerin ve veri paketlerinin taşınması ile karşılıklı akışını sağlayan çerez uygulamaları ile (iii) iletim hataları ve veri kaybını tespit eden çerez uygulamaları bu istisna kapsamında değerlendirilir[238].

"Kriter B" çerezleri ise bir hizmetinin sunulmasına ilişkin olup, ilgili kişilerin açıkça talep ettiği bir hizmetin sunulması için mutlak surette zorunlu olan çerezlerdir. Bu çerezler kullanılmadığı halde, kullanıcının talep ettiği hizmetin sunulması mümkün olmamalıdır. Kriter B istisnasının geçerli olabilmesi için ilgili kişinin hizmet için açıkça talepte bulunması ve çerezin kullanımının mutlak surette zorunlu olması gerekmektedir[239].

Çerezlerin kullanım amaçlarına yönelik kesin bir ayrım yapmak günümüzde zorlaşmıştır. Çok amaçlı çerezler, hem Kriter A hem de Kriter B amaçlarını karşılayabilir. Ancak Kriter A veya Kriter B istisnalarını karşılayan bir çerezin diğer

[237] Article 29 Data Protection Working Party. (2013). "Working Document 02/2013 providing guidance on obtaining consent for cookies" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf adresinden 24 Kasım 2022 tarihinde erişilmiştir.
[238] Article 29 Data Protection Working Party. (2012). "Opinion 04/2012 on Cookie Consent Exemption". Brüksel. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf adresinden 28 Kasım 2022 tarihinde erişilmiştir.
[239] Article 29, 2012.

amaçlar için kullanılması durumunda da ilgili kişilerden yine rıza alınması gerekecektir[240].

Özetle, çerez kullanımında genel kural rıza alınmasıdır, ancak "Kriter A" ve "Kriter B" istisnaları doğrultusunda çerezlerin ilgili kişi rızası bulunmadan zorunlu kullanımı mümkün olacak, ancak istisnalar dışındaki çerezler için kullanıcının rızası gerekecektir.

Sonuç olarak, 2002/58/EC Sayılı Direktif kapsamındaki çerez düzenlemeleri, kullanıcıların mahremiyetini koruma amacı güderken, çerezlerin kullanımı ve veri işleme süreçlerine ilişkin önemli kurallar ve bazı istisnalar getirmektedir. Bu kurallar, kullanıcılara bilgilendirme yapma yükümlülüğü, geçerli rıza alınması ve rızanın özellikleri gibi konuları içermektedir. AB üye devletleri arasında çerezlere ilişkin bazı farklılıklar bulunmakla birlikte, temel amaç kullanıcıların haklarını korumaktır.

4.3.2.3 e-Gizlilik Tüzük Taslağı (EGT)

Elektronik haberleşme hizmeti sunan şirketlerin veri gözetimi uygulamalarının artması, yapay zekâ ve otomatik veri işleme sistemlerinin yaygınlaşması gibi faktörler, yeni düzenlemelerin yapılmasını zorunlu hale getirmiştir.

Avrupa Parlamentosu ve Avrupa Veri Koruma Kurulu, 2009'daki değişikliklerin beklenen etkiyi yaratmadığını ve çerez duvarları ile rıza yorgunluğunu beraberinde getirdiğini belirtmiştir. Bu nedenle, çerez düzenlemelerinde köklü ve teknolojik gelişmelere uygun bir değişiklik yapılması gerektiği görüşünü dile getirmişler ve bu doğrultuda, 10 Ocak 2017'de e-Gizlilik Tüzüğü'nün ilk taslağı yayınlanmıştır[241].

EGT, esas olarak mevcut e-Gizlilik Direktifi'ni[242] yerine koymayı ve GVKT ile uyumlu hale getirmeyi amaçlamaktadır. EGT, Düzenleme, içerik ve meta veriler de dâhil olmak üzere elektronik iletişim verilerinin işlenmesine uygulanmak ve bu iletişimlerin gizliliği ve mahremiyeti için gerekli kuralları belirlemek adına düzenlenmiştir.

[240] Aksoy ve Halıcıoğlu, 2021
[241] Aksoy ve Halıcıoğlu, 2021
[242] Direktif 2002/58/EC

İlgili kişilerin elektronik iletişim süreçleri kapsamında alınacak rızaların özgür iradeyle verilmiş, belirli bir amaç uğruna ve bilgilendirmeye dayanan olumlu bir eylem ile alınmış rızalar olması gerekliliği düzenlenmiştir[243].

EGT ile çerezler ve benzer teknolojilerin kullanımı konusunda belirli gereksinimler getirilmektedir ve yerine geleceği e-Gizlilik Direktifi ile tanımlanan istisnaların kapsamı daha ayrıntılı düzenlenmiş ve yalnızca kesinlikle gerekli çerezler dışında bu tür teknolojilerin kullanılmadan önce kullanıcı rızası alınması zorunluluğunu yinelemiştir. Çerezlerden farklı olarak ilgili kişilere yapılması planlanan doğrudan pazarlama uygulamaları kapsamındaki rıza mekanizmaları da istisnaları belirlenerek açıklanmıştır. EGT, özellikle çerez kullanım istisnalarının daha net bir çerçeveye oturtulmasını ve Direktif uygulamalarındaki belirsizliklerin azaltılmasını hedeflemektedir. Tüzük taslağı, çerez uygulamalarına ilişkin olarak Direktif'ten farklı bir çerçeve ve daha uzun bir istisnalar listesi öngörmektedir.

EGT altındaki çerez düzenlemeleri incelendiğinde, rızanın genel kural olarak korunduğu görülmekle birlikte Avrupa Veri Koruma Kurulu önerilerinin de dikkate alındığı ve bu kapsamda rıza istisnalarının daha ayrıntılı ve günümüz ihtiyaçlarına uygun şekilde düzenlendiği anlaşılmaktadır. EGT ayrıca, tartışmalı konular olan "çerez duvarları", "rıza yorgunluğu" ve "veri sorumlusu" konularında da düzenlemeler içermektedir.

Yukarıda açıklanan Kriter A ve Kriter B istisnalarına yönelik düzenlemeler EGT kapsamında bazı değişikliklere uğramış ve özellikle Kriter A ile belirlenen istisnalar kapsamında önemli yenilikler getirilmiştir. İstatistiksel amaçlarla kullanılan analitik çerezlerin üçüncü taraf çerezler kapsamında da belirli kriterlerin sağlandığı takdirde rızaya tabi olmadan kullanılabileceği, cihaz güvenliğinin sağlanması, dolandırıcılığın önlenmesi gibi konular için kullanılan çerezlerin sınırlı süre kuralı ile yine ilgili kişi rızası olmadan kullanılabileceği, yazılım güncellemesi amacıyla kullanılan çerezlerin belirli koşullar altında istisna kapsamına alınması ve acil durumlarda konum tespiti için kullanılan çerezler de istisna kapsamına alınmıştır.

Çerez duvarı, kullanıcının çerez uygulamalarına rıza vermesini zorlayan ve verilen rıza miktarını ve tüm çerezleri sınırlayan, rıza verilmediği takdirde internet sitesine girişi engelleyen bir çerez yasaklama aracıdır. Çerez duvarı kullanan web siteleri, çerez

[243] Article 29, 2017

yerleştirilmesine izin vermeyen kullanıcıların girişine izin vermezler. Çerez duvarlarının yasaklanması gerekip gerekmediği konusu çerezlerle ilgili Direktif uygulaması bağlamında da sıkça tartışılan bir konudur.

GVKT'ye göre, kişisel verilerin işlenmesine ilişkin rızanın "özgür bir şekilde" verilmesi gerektiğinden, bir web sayfasının kullanıcıya sunulan hizmet karşılığında ücret ödeme veya çerez kullanımına izin verme seçeneklerini sunmasının GVKT'nin aradığı şartı sağlayıp sağlamadığı tartışmalıdır.

Bu tartışmalar devam ederken, Avrupa Veri Koruma Kurulu 4 Mayıs 2020 tarihinde yayınladığı tavsiye kararlarıyla çerez kullanımına ilişkin rızanın bir web sayfasına giriş için koşullandırılamayacağını ifade etmiştir. Ancak Kurul, 2021 yılında yayınladığı açıklamada, aynı hizmet sağlayıcılar tarafından kullanıcılara adil alternatifler sunulmadıkça çerez duvarlarının kullanımının rızanın özgür iradeyle verilmesi koşulunu bozabileceğini ifade etmiştir.

Tüzük düzenlemesi ise çerez duvarlarının belli koşullar altında kullanılmasına izin vermektedir. Tüzüğün gerekçesinde, kullanıcılara kullanılan çerezlerin ve benzer tekniklerin amaçları hakkında açık, kesin ve kullanıcı dostu bilgilerin verilmesi ve web sitesine erişim bakımından çerezlerin kabul edilmesi koşuluna eşdeğer ve denk bir alternatif sunulması şartıyla çerez duvarlarının kullanılabileceği belirtilmektedir. Ancak kullanıcı ile hizmet sağlayıcılarının denk olmadığı durumlarda (örneğin, kamu kurumları tarafından sunulan hizmetleri içeren web sitelerine erişimde) çerez duvarlarının kullanıcıları özgür seçim haklarından mahrum bırakabileceği ifade edilmektedir.

Direktif uygulamaları bağlamında, kullanıcıların maruz kaldığı çok sayıda rıza talebi sonucunda ortaya çıkan "rıza yorgunluğu" ve buna bağlı olarak ortaya çıkan hukuki sorunlar da tartışma konusu olmaktadır. EGT, bu tartışmaların büyük ölçüde azalmasını amaçlayarak, yazılımcılara daha basit ve kullanıcı dostu çerez rızası uygulamaları geliştirmelerini tavsiye etmektedir. Ayrıca, teknik olarak uygulanabilir olduğu durumlarda, kullanıcılara belirli sağlayıcıların çerezlerini güvenli listeye alma veya bu listeden çıkarma hakkı tanınmaktadır[244].

Üçüncü taraf çerezlerin yerleştirildiği web sitelerinde, veri koruma mevzuatına uygun şekilde hareket edilmemesi durumunda sorumluluğun kimde olduğu tartışma konusu

[244] E-Gizlilik Tüzüğü Gerekçe Madde 20/a

olmaktadır. GVKT madde 26 uyarınca, iki veya daha fazla veri sorumlusunun işleme amaçlarını ve yöntemlerini birlikte belirledikleri durumlarda "ortak veri sorumlusu" olacaklarını kabul edilmektedir. Bu durumda, ilgili kişi, GVKT'den doğan haklarını ortak veri sorumlularından her birine karşı kullanabilir. Ulusal veri koruma otoriteleri de benzer görüşleri paylaşmaktadır. EGT kapsamında maalesef bu konuya ilişkin açık bir düzenleme bulunmamaktadır. Fakat özellikle Google'ın üçüncü taraf çerezler ile ilgili gelişmeleri ve diğer önemli şirketlerin aksiyon planları değerlendirildiğinde yakın gelecekte üçüncü taraf çerezlerinin aşamalı olarak kullanılmaya son verileceği tahmininde bulunmak da mümkündür[245].

Avrupa Birliği Veri Koruma Otoritesi, e-Gizlilik Direktifi'nin EGT olarak revizyon sürecini, acilen tamamlanması gereken önemli ve gerekli bir adım olarak değerlendirmektedir. Bu görüşünü de Avrupa Komisyonu, Parlamento ve Konseyi'ni konu hakkında birlikte çalışmaya davet ederek belirtmiştir[246]. Bu çağrı metni uyarınca elektronik iletişimlerin gizliliğinin, GVKT ötesinde özel koruma gerektirdiğini ve ileten mesajlaşma hizmetlerinin gizliliğini ve tarafsızlığını güçlendirmenin bir zorunluluk olduğu vurgulanmıştır.

Elektronik iletişimlerin dijital yaşamlarımızdaki yeri, önemli ve yaygın kullanımı göz önüne alındığında, özellikle elektronik iletişim içerikleri veya meta verilerin toplanması nedeniyle, özel nitelikli kişisel veri ihlalleri ile karşılaşmanın riskinin arttığı ve bunun da insan hakları ve özgürlükleri için tehlike oluşturduğu Avrupa Birliği Veri Koruma Otoritesi tarafından bildirilmiştir. Bu bağlamda veri işleme yasaklamalarının geniş kapsamlı tutulması, istisnaların mümkün olduğu sürece sınırlı belirlenmesi ve mutlaka ilgili kişilerin rıza mekanizması üzerine kurulu bir düzen geliştirilmesi desteklenmektedir[247].

4.3.3. Türkiye'deki Hukuki Düzenlemeler ve Yasal Durum

Avrupa Birliği'nde uzun yıllardır ÇDP uygulamaları ve çerezlere ilişkin hukuki düzenlemeler bulunmakta ve bu düzenlemeler sürekli olarak değişmekte,

[245] Bump Pamela. The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2023 Phase-Out, 2022.
[246] European Data Protection Board (EDPB) (2018). Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications. https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf adresinden 17 Nisan 2022 tarihinde erişilmiştir.
[247] EDPB, 2018

güncellenmektedir. Türk hukukunda ise ÇDP uygulamaları ve özellikle çerezler ilişkin belirgin ve kapsamlı hükümler bulunmamaktadır. Bu durum, çeşitli hukuki soru ve sorunları beraberinde getirmektedir.

Çalışmanın ilk iki bölümünde ayrıntılı olarak açıklandığı üzere Türkiye'deki mevcut kişisel verilerin korunması düzenlemeleri, KVKK ve ilgili yönetmelikler tarafından belirlenmektedir. Öte yandan ÇDP uygulamalarına yönelik tanımlamalar bazı rehber ve kararlarda yer almaktan öteye geçememiş, KVKK ve ilgili yönetmeliklerde açıkça belirtilmemiştir. Bu durum da, ÇDP uygulamaları ve özellikle bu kapsamda çerezlerin kişisel veri olup olmadığı ve hangi tür çerezlerin belirli düzenlemelere tabi olduğu konusunda belirsizliklere yol açmaktadır.

Dünya genelinde kişisel verilerin korunması konusunda ülkeler nezdinde yapılmış olan normlara bakıldığında, bu düzenlemelerin çok büyük bir kısmının AB mevzuatında yer alan ve kişisel verilerin korunması ile ilişkili olan düzenlemeler öncülüğünde yapılmış olduğu görülmektedir. Bu durumun sebeplerinden biri gerek AB üyesi ülkelerin gerek Birlik üyesi olmayan diğer devletlerin tarih içerisinde sahip oldukları otoriter rejimlerin halklarına yaşattıkları birtakım olumsuz deneyimlerin yaşanmasının tekrarının önüne geçmek ve bu amaçla bireylerin temel hak ve özgürlüklerinin korunmasına verilen önemi vurgulayarak korumayı arttırmaktır. Bir diğer sebebi ise AB üyesi ülkeler ile ticari ilişki içerisinde bulunan diğer devletlerin, AB mevzuatındaki hükümlere kıyasla kendi mevzuatlarında kişisel verilerin korunması konusunda yeterli koruma sağlamıyor olmalarının tespiti hâlinde kendilerine AB üyesi ülkeler tarafından veri transferinin yasaklanarak gerçekleşmeyecek olması karşısında ticari ilişkilerinin zedelenmesi sonucu ile karşılaşmak istemeyişleridir. Yıllardır AB üyesi olmak gayretiyle kendi iç hukukunda birçok alanda birtakım mevcut normları, AB mevzuatı ile uyumlu hale getiren ve gerektiğinde yeni kanunî düzenlemeler gerçekleştiren Türkiye de kişisel verilerin korunması konusunda, mevzuatında birçok düzenlemeye yer vermiştir. Şüphesiz ki devletlerce bu verilere duyulan ihtiyacın karşılanması sırasında hukuk devleti olmanın bir sonucu olarak kişilerin temel hak ve hürriyetlerine riayet edilmeli ve bireylerin kişisel verilerinin hukukî koruma altına alınması gerekmektedir. Zira kişisel verilerin korunması hakkı özü itibariyle yüksek kişilik değerlerini korumaya yönelik bireysel bir hak olup, temelinde bireyin insan onurunun korunması ve kişiliğini serbestçe

geliştirmesi hakkı yer almaktadır. Bu nedenledir ki kişisel verilerin korunması hakkı da bireyin sahip olduğu en temel haklardan birisi olarak karşımıza çıkmaktadır[248].

4.3.3.1. 6698 Sayılı Kişisel Verileri Koruma Kanunu

26 Aralık 2014 tarihinde kişisel verilerin korunması ile ilgili kanun tasarısı Türkiye Büyük Millet Meclisi'ne sunulmuştur. Bu tasarı 24 Mart 2016 tarihinde kabul edilmiş ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016'da yürürlüğe girmiştir. Kanun'un hazırlanması esnasında dayanak aldığı uluslararası düzenleme AB üye devletleri arasında kişisel veri akışını düzenleyen ve korumayı amaçlayan 95/46/EC Sayılı Direktif'tir.

Kanun ana amacını birinci maddesinde açıklamıştır. Bu maddeye göre Kanun'un ana amacı başta özel hayatın gizliliği olarak veri işleme faaliyeti kapsamında temel hak ve özgürlükleri korumak ve veri işleyen gerçek kişiler ile tüzel kişilerin uyacakları yükümlülükleri belirlemektir. Madde gerekçesinde de kişisel verilerin işlenmesinin bir disiplin çerçevesinde yürütülmesinin sağlanması, ilerleyen yıllarda önemi fark edilen mahremiyet hakkı ve bilgi güvenliği hakkını korumayı amaçladığı ifade edilmiştir.

Kanun'un ikinci maddesinde ise kapsam unsuru açıklanmıştır. Bu maddeye göre Kanun kişisel verileri işlenen gerçek kişiler ve bu kişisel verileri otomatik ya da otomatik olmayan yollarla işleyen gerçek kişiler ile tüzel kişiler bakımından uygulama alanı bulur. Gerekçede de açıklandığı üzere Kanun kişisel verileri işleyen tüzel kişiler bakımından özel veya kamu tüzel kişiliği ayrımında bulunmamıştır. Bundan dolayı Kanun hem özel hem de kamu tüzel kişilerine uygulanır.

Otomatik olmayan yollarla işlenen kişisel verilerin otomatik veya herhangi bir veri kayıt sistemi parçası olması şartından bahsedilmiştir. Veri kayıt sistemi, Kanun'un üçüncü maddesinin h fıkrasında kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi olarak tanımlanır. Bu noktada Kanun fiziki ya da dijital kayıt sistemleri açısından bir fark gözetmemiştir.

ÇDP uygulamaları kapsamında, çerezler gibi izleme yöntemleri vasıtasıyla elde edilen veriler analiz edilerek profilleme işlemleri gerçekleştirilmektedir. Türk hukuku çerçevesinde profilleme tanımı yapılmamış olsa da GVKT uyarınca *"bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları,*

[248] Ensari, Ali Burak. Çevrimiçi Davranışsal Pazarlamanın Tüketici Davranışları Üzerindeki Etkileri ve Kişisel Verilerle ilişkisi, 2014, s.110

güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi" olarak ifade edilmektedir.

Profilleme süreçleri, toplanan çok sayıda kişisel verinin işlenmesi ile birlikte ilgili kişi hakkında bir profil oluşturulmasına izin veren uygulamalardır. İlgili kişiler, kişisel verilerinin işlenmesine açık rıza vermiş olsalar bile, bu kişisel verilerle yapılan profilleme sonucu, kişinin ve veri sorumlularının kontrolü dışında yeni veriler elde edilebilecektir. Örneğin, bir kişi cinsel tercihi, eğitim düzeyi veya dini görüşleri hakkında herhangi bir kişisel veri paylaşmamış olsa bile, çevrimiçi davranışsal reklamcılıkta kullanılan çerezler aracılığıyla gerçekleştirilen aramalar ve arama frekansları, ilgi alanları üzerinden bu tür veriler elde edilebilecek niteliktedir. Bu verilerin gerçeği ne derece yansıttığı her zaman belirlenemese de, kişisel verilerin korunması ve gizlilik konusunda riskler taşıdığı açıktır. Çünkü çerezler aracılığıyla elde edilen verilerin hedefleme ve izleme yöntemleriyle işlenmesi sonucu ortaya çıkabilecek kişisel verilerin neler olabileceğini tam olarak tahmin etmek mümkün olmamaktadır. Bu nedenle, ilgili kişiye sunulmuş aydınlatma metni ve bu kapsamda alınan açık rıza, kimi zaman yeterli olmayabilecektir. Bu durum, Kişisel Verilerin Korunması Kanunu'nun (KVKK) 4. maddesinin (a) bendinde düzenlenen hukuka ve dürüstlük kurallarına uygunluk, (c) bendinde belirli, açık ve meşru amaçlar için işleme ve (ç) bendinde işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkelerine aykırılık anlamına gelmektedir.

Kişisel Verilerin Korunması Kanunu ile getirilen düzenlemelere ayrıntılı olarak çalışmanın ikinci bölümünde değinildiği için burada tekrarlanmayacaktır. Öte yandan KVKK kapsamında ÇDP uygulamalarından çerezlere yönelik yayımlanan rehber ve Kurul tarafından verilen önemli kararlara kısaca değinmek uygun olacaktır.

Kişisel Verileri Koruma Kurulu / 27/02/2020 tarihli ve 2020/173 sayılı karar özeti

Kurul artık Amazon Kararı olarak bilinen *"27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti*[249]*"* yayımladığında hem o tarihe kadar verilmiş para cezaları arasında dikkat çeken bir miktar olduğu hem de tartışmalı olan birçok konuya değindiği için

[249] *"Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti, https://www.kvkk.gov.tr/Icerik/6739/2020-173 adresinden 24 Mayıs 2022 tarihinde erişilmiştir.*

özellikle de kişisel verilerin korunması mevzuatı çerçevesinde ilk kez çerezler konusunda bir bilgilendirme yapılmış olması kapsamında büyük dikkat çekmiştir.

Amazon Turkey Perakende Hizmetleri Limited Şirketi ("Amazon")'un web sitesi üzerinde bulunan "Belirli bilgileri vermemeyi tercih edebilirsiniz, ancak bu durumda Amazon Hizmetlerinin çoğundan yararlanamazsınız." ve "Çerezlerimizi engellerseniz veya reddederseniz alışveriş sepetinize ürün ekleyemez, satın alma aşamasına geçemez veya oturum açmanızı gerektiren herhangi bir Amazon hizmetini kullanamazsınız." ifadeleri genel olarak ilgili kişi şikayetinin ana konusunu oluşturmaktadır[250].

Amazon web sitesinde çerezler kullanılarak kişisel verilerin işlendiği fakat çerez kullanımına ilişkin aydınlatma yapılmadığı gibi, açık rıza alınması gereken çerez süreçleri için de ilgili kişilerden açık rıza alınmadığı Kurul tarafından tespit edilmiştir.

Kurul kararı ile açık rıza kapsamındaki tespit edilen hukuka aykırılıklar; üyelik yapıldığı anda ilgili kişinin rıza vermiş olduğunun değerlendirilmesi ve daha sonra ilgili kişilere açık rızalarını geri alma imkânı tanınması, kişisel verilerinin işlenmesine otomatik onay verilen ve kişilere bu onayı kaldırmaları yönünde imkân veren bir sistem (opt-out) kullanılması, açık rızanın hizmet şartına bağlanması ile kişisel veri işleme şartlarından birisinin mevcut olduğu durumlar için de açık rıza alınması olarak değerlendirilmiştir[251].

Öte yandan yine ilgili karar kapsamında Kurul tarafından aydınlatma yükümlülüğü konusunda tespit edilen hukuka aykırılıklar; yükümlülüğü yerine getirebilmek amacı ile hazırlanan "Gizlilik Bildirimi"nin, genel bilgilendirme içeriğine sahip olması ile web sitesine giriş anında kişisel verilerin işlenmeye başlanmasına rağmen bu aşamalarda aydınlatma yükümlülüğünün yerine getirilmemesi olarak değerlendirilmiştir[252].

Amazon kararı ile öne çıkan konulardan bir diğeri ise ETK ve KVKK ilişkisidir. Kurul Amazon Kararı ile ticari nitelikli bir elektronik iletinin ETK mevzuatına uygun olarak gönderilmesine ek olarak ilgili kişiler açısından kişisel verileri işleme faaliyetinin de

[250] Kişisel Verileri Koruma Kurulu (2020). "Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6739/2020-173 adresinden 24 Mayıs 2022 tarihinde erişilmiştir.
[251] Kişisel Verileri Koruma Kurulu, 2020
[252] Kişisel Verileri Koruma Kurulu, 2020

yürütülmesi sebebi ile aynı zamanda kişisel verilerin korunması mevzuatına da uygun olması gerektiğini vurgulamaktadır.

Amazon Kararı'nı takiben Türkiye'de veri koruma mevzuatı kapsamında çerezler konusundaki eksiklikler tartışılmaya devam edilmiştir. Daha sonra Kurum mevzuatta bulunan bu eksikliği dikkate alarak çerez kullanımı konusunda bir rehber taslağı yayınlamış ve görüşe açmıştır.

Kişisel Verileri Koruma Kurulu / Çerez Uygulamaları Hakkında Rehber

Kurul tarafından hazırlanan ve son halini 20.06.2022 tarihinde alan "Çerez Uygulamaları Hakkında Rehber" ("Rehber"), çerez ve çerez türleri, Elektronik Haberleşme Kanunu ile Kişisel Verilerin Korunması Kanunu arasındaki bağlantıyı, çerez kullanımının yasalara uygun şekillerini, çerez kullanımı için gereken rıza ve bunun hukuki unsurlarını, çerezlerin yurt dışına aktarımını, uygun bilgilendirme ve Kurul'un bir kararının çerezlere yönelik değerlendirmesini içermektedir.

Rehber uyarınca çerez türleri aşağıdaki şekilde üç başlık ile sınıflandırılmıştır:

<table>
<tr><th colspan="2">Sürelerine Göre Çerezler</th><th colspan="2">Kullanım Amaçlarına Göre Çerezler</th><th colspan="2">Taraflarına Göre Çerezler</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Oturum Çerezleri</td><td>1</td><td>Zorunlu Çerezler</td><td rowspan="2">1</td><td rowspan="2">Birinci Taraf Çerezler</td></tr>
<tr><td>2</td><td>İşlevsel Çerezler</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Kalıcı Çerezler</td><td>3</td><td>Performans/Analitik Çerezler</td><td rowspan="2">2</td><td rowspan="2">Üçüncü Taraf Çerezler</td></tr>
<tr><td>4</td><td>Reklam/Pazarlama Çerezleri</td></tr>
</table>

Çerezlerin KVKK kapsamında yer almadığı Rehber içerisinde belirtilmiş, Elektronik Haberleşme Kanunu'nun 51. maddesi, Avrupa Birliği'nin 2002/58/EC sayılı Direktifi ile benzerlik gösterdiği için, bu maddenin çerezler üzerinde sınırlı bir etkisi olduğu açıklanmıştır. Öte yandan Elektronik Haberleşme Kanunu, sadece elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme altyapısını sağlayan şirketlere uygulanır.

Çerez kullanımına dair belirli kurallar ve kriterlerin Rehber'de belirtilmesi amaçlanmış, çerezlerin iletişimin sağlanması için kullanılmasını, belirli senaryolar altında çerez kullanımını, açık rıza gerektiren durumları ve çerez kullanımı için gereken kişisel veri işleme şartlarını açıklamıştır.

Rehber, KVKK düzenlemeleri ile paralel olarak ilgili kişilerden çerez kullanımına ilişkin olarak alınacak açık rızanın belirli bir konuya ilişkin, özgür irade ile verilmiş ve bilgilendirmeye dayalı olması gerektiğini vurgulamaktadır. Yukarıda gösterilen sınıflandırmalar kapsamında reklam/pazarlama çerezleri kullanımının ancak ilgili kişilerden toplanacak açık rıza vasıtasıyla mümkün olacağını, bu çerçevede ilgili kişilerin açık, net ve anlaşılır bir dille bilgilendirmesinin gerekliliği de Rehber ile belirtilmiştir[253].

Örneğin, çevrimiçi davranışsal reklamcılık için kullanılan çerezlerin, çerez politikalarında diğer çerezlerden farklı olarak belirtilmesi ve önceden işaretli bir kutucuk ile ilgili kişilerden açık rıza alınamayacağı vurgulanmıştır.

Bir web sitesinde, yukarıda sınıflandırması gösterilen çerez türlerinin çoğu aynı anda kullanılabilmektedir. Yine de veri işleme şartları noktasında değerlendirildiğinde birtakım farklılıkların gözetilmesi gerekecek ama özellikle kullanım amacı ayrımına göre uygun katmanlı bir aydınlatma yapılması ve ihtiyaç olduğu takdirde ilgili kişinin açık rızasına başvurulması gerekecektir. Yukarıda bahsedilen Amazon Kararı ile paralel olarak çerezlerin kullanımı için alınacak açık rıza da hiçbir şekilde hizmet şartına bağlanmamalı veya bir battaniye rıza olacak şekilde toplu olarak alınmamalıdır.

Önemine binaen Rehber ile Avrupa Birliği sınırlarında da çok tartışma yaratan çerez duvarı uygulamalarının kişinin özgür iradesini engelleyebileceği ve bu durumda alınan açık rızanın geçerli olmayacağı belirtilmektedir. Üçüncü taraf çerezlerin kullanıldığı durumlarda ise iki tarafın da kullanıcıları çerezler hakkında açıkça bilgilendirmek ve gerektiğinde açık rızalarını almakla yükümlü olduğu düzenlenmiştir.

Öte yandan Türk veri koruma mevzuatı kapsamında uzun süredir tartışmalara konu olan ve henüz uygun bir çözüm yolu da bulunamamış yurtdışına aktarım konusunda ise Rehber, KVKK ile paralel olarak ilgili kişinin açık rızası alındığı takdirde aktarımın gerçekleştirilebileceği, aksi halde ancak yeterli koruma sağlanan ülkelere veya Kurul

[253] Kişisel Verileri Koruma Kurumu (Haziran 2022). Çerez Uygulamaları Hakkında Rehber.

tarafından onaylanmış taahhütname kapsamında aktarımın gerçekleştirilebileceği belirtilmiştir.

Rehber'in son bölümünde ise, çerezlerin açık rıza şartına dayalı olarak işlenmesi durumunda, aydınlatma ve açık rıza alınması işlemlerinin ayrı ayrı yerine getirilmesi, her bir farklı amaç için ayrı açık rıza alınması gerektiği ve açık rızanın aktif bir eylem ile gerçekleştirilmesi gerektiği belirtilmiştir.

Rehber ayrıca, iyi uygulama örnekleri, çerez uygulamalarına ilişkin örnek aydınlatma metni ve çerez kullanımında kişisel verilerin işlenmesine dair kötü örnekler içermektedir.

Yine de daha önce hiçbir kanun veya yönetmelik metni ile düzenlenmeyen bir konunun Kurul tarafından yayınlanan bir rehber vasıtasıyla çok da ayrıntılı olmayacak şekilde düzenlenmesi uygulamada oldukça fazla eleştiri almıştır.

Kişisel Verileri Koruma Kurulu / 10/03/2022 tarihli ve 2022/229 sayılı karar özeti

Kişisel Verileri Koruma Kurulunun 10/03/2022 tarih ve 2022/229 sayılı kararında[254] çerezler hakkında bazı önemli değerlendirmeler yer almaktadır.

Kurul ilgili karar kapsamında yapılan değerlendirmeleri ile web sitesinin düzgün çalışması için zorunlu olan çerezler için ilgili kişilerden açık rıza alınmasına gerek olmadığı öte yandan reklam, pazarlama ve performans amacıyla kullanılan çerezlerin mutlaka ilgili kişinin açık rızasına tabi olduğunu belirtmiştir.

Web sitelerinin çalışmalarını sağlayan çerezleri "kesinlikle gerekli çerezler" olarak tanımlayan Kurul, KVKK'nin 5. Maddesinin ikinci fıkrası ile 6. Maddesinin üçüncü fıkrasında yer alan işleme şartlarından birine dayanılarak işleme faaliyetinin yürütülebileceği, yine bu kategoride olmayan ama sayılan işleme şartlarından birine dayanılabilen çerezler için de açık rıza alınmasının gerekli olmadığı kararda açıklanmıştır.

İlgili karar ile göze çarpan değerlendirmelerden biri KVKK ile açıkça sayılan işleme şartlarından *"İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"* haline ancak kesinlikle gerekli çerezler bakımından başvurulabileceği, aksi halde başka bir işleme

[254] *"E-ticaret sektöründe faaliyet gösteren veri sorumlusu şirket tarafından internet sitesinde/mobil uygulamalarında kullanılan çerezler aracılığıyla hukuka aykırı olarak kişisel veri işlenmesi"* hakkında Kişisel Verileri Koruma Kurulunun 10/03/2022 tarih ve 2022/229 sayılı kararı

şartına dayanılamadığı durumlarda ilgili kişilerden açık rıza alınması gerektiği değerlendirmesidir.

Kullanıcı tercihlerinin kesinlikle gerekli çerezler kapsamında değerlendirilemeyeceği ancak işlevsellik çerezleri olarak değerlendirilebileceği bu durumda ise ilgili kişi bu hizmeti açıkça talep etmediği takdirde ancak açık rızaya dayanarak işleme faaliyetinin gerçekleştirilebileceği yine Kurul tarafından belirtilmiştir.

Yine yapılan incelemelerde veri sorumlusunca reklam/pazarlama amaçlı çerezler kullanıldığı fakat bir pop-up vasıtasıyla bilgilendirme yapılsa da açık rıza alınmasına dair herhangi bir işlem gerçekleştirilmediği anlaşılmıştır. Bu kapsamda yapılan değerlendirmede kesinlikle gerekli olmayan; işlevsel çerezler, performans-analitik çerezler ve reklam/pazarlama çerezlerinin kullanılarak veri işlenebilmesi için herhangi bir veri işleme şartına dayanılamadığı takdirde ancak "opt-in" mekanizmasıyla açık rıza alınması yoluna başvurulabileceği aksi halde kanuna aykırı bir veri işleme gerçekleşeceği belirtilmiştir.

Çerez politikaları hakkında yine ilgili karar içerisinde Kurul tarafından yapılan değerlendirmeler ile; çerez politikalarının ayrı bir bağlantıyla kolayca erişilebilir olması gerekliliği, çerez politikası hazırlanırken aydınlatma yükümlülüğü kapsamında uyulması gereken yönlendirmelere de uyulması ve bu kapsamda *veri sorumlusunun kimliği, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin kimlere ve hangi amaçla aktarılabileceği, kişisel veri toplamanın yöntemi ve hukuki sebebi* ile ilgili kişinin haklarının da belirtilmesi gerektiği, genel olarak bu bilgilendirmenin teknik detaylar içinde kaybolmadan açık ve anlaşılır şekilde yapılması konularına değinilmiştir.

4.3.3.2. 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

ETK elektronik ticaret hakkındaki hükümleri düzenlemektedir. ETK'nin 6. Maddesi ile müşterilere izinsiz ileti gönderimi yasaklanmıştır. Kişisel verilerin güvenliğine yönelik 10. maddesi ile de elektronik ticaret esnasında elde edilen kişisel verileri saklanma yükümlüğü getirilmişti ve veri güvenliğine yönelik hizmet sağlayıcılarının sorumlu tutulması gerektiği ifade edilmiştir. Ayrıca ETK'nin 12. maddesi ile de veri ihlalleri sonucunda veri sorumlularına verilecek para cezaları düzenlenmiştir[255].

[255] Altındere, 2020: 28

Öte yandan elektronik hizmet sunucuları, ticari elektronik ileti yoluyla kişilere reklam, kampanya ve pazarlama gibi hizmetleri sunarken, bu kişilere ait genellikle ad/soyadı, e-posta ve cep telefonu gibi kişisel verileri de işlemektedir. Dolayısıyla, kişisel verilerin işlenmesi mevzuatı ile elektronik ticaret mevzuatı çoğu alanda iç içe geçmekte fakat ayrı şekilde değerlendirme gerektirmektedir.

Öncelikle ticari elektronik ileti gönderiminde ETK kapsamında zorunlu tutulan onay kavramının[256], KVKK kapsamında düzenlenen açık rıza kavramından farklı olduğunu ve ilgili kişilerden alınan açık rızanın ETK anlamında onay sayılamayacağı gibi ETK kapsamında kişilerden alınan ileti gönderme onayının da KVKK kapsamında açık rıza sayılmasının mümkün olmayacağını belirtmek gerekir.

ETK, henüz kişisel verilerin korunmasına ilişkin bir düzenleme yayımlanmadan önce yürürlüğe girmiş ve elektronik ticaret işlemlerinde kişisel verilerin korunmasını sağlayan kurallar koymuştur. Daha sonra KVKK'nin yürürlüğe girmesi ile çatışan düzenlemeler hakkında doktrinde özel-genel kanun tartışması yürütülmüş ve özellikle ihlal halinde çift ceza sorunu olup olmayacağı soruları ortaya çıkmıştır[257].

ETK-KVKK ilişkisi Kurul'un bazı kararlarına da konu olsa da özellikle 17 Aralık 2021 tarihinde yayımlanan Kurul'un "Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu" ile; ilgili kişilere gönderilecek iletilerin amacı ve sonucu hakkında katmanlı bir aydınlatma yapılması ve bu aydınlatmaların söz konusu SMS içeriklerinde de yer alması gerekliliği, KVKK kapsamında açık rıza, ETK kapsamında ileti onayı ve üyelik sözleşmesi onayları gibi işlemlerin tek bir eylemle gerçekleştirilmemesi ve ayrı ayrı açık rıza alınması zorunluluğu, açık rıza alınması ve aydınlatma yükümlülüğü işlemlerinin birlikte gerçekleşmemesi gerekliliği gibi konulara dikkat çekilmiştir[258].

[256] Keser, Yıldırım. Tüketicinin kişisel verisinin işlenmesinde açık rıza, 2020.

[257] İbrahimoğlu Güreş, Selen ve Aytaç, Batuhan. (2019). Kişisel Verileri Koruma Kurulu'nun Elektronik Ticari İletilerle İlgili İlke Kararına Dair Güncel Tartışmalar. https://www.ozbek.av.tr/kvk-blog/kisisel-verileri-koruma-kurulu-nun-elektronik-ticari-iletilerle-ilgili-ilke-kararina-dair-guncel-tartismalar/ adresinden 12 Ocak 2023 tarihinde erişildi.

[258] Kişisel Verileri Koruma Kurumu (2021). Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu. KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu adresinden 18 Eylül 2022 tarihinde erişilmiştir.

Bu tartışmalara son nokta ise 2022 yılının Temmuz ayında konulmuştur. ETK mevzuatında meydana gelen değişiklikler çerçevesinde; KVKK düzenlemelerinin hâlihazırda veri sorumlusu sıfatıyla hizmet sağlayıcı ve aracı hizmet sağlayıcıları da kapsaması ile daha detaylı hükümler içermesi neden gösterilerek kişisel verilerin korunması konularını düzenleyen 10. madde yürürlükten kaldırılmıştır.

4.3.3.3. 5809 Sayılı Elektronik Haberleşme Kanunu

2008 yılında yürürlüğe giren 5809 Sayılı Kanun Elektronik Haberleşme Kanunu'nun ("EHK") çeşitli hükümleri de kişisel verilerin korunması konusunda düzenlemeler içermektedir. Çerezler kapsamında yasal mevzuatta yer alan tek hüküm yine Elektronik Haberleşme Kanunu içerisinde yer almaktadır.

Ayrıca 5809 Sayılı Kanun'un 51. maddesi kişisel verilerin işlenmesini ve gizliliğin korunması düzenlenmiştir. Bu madde ile kişisel verilerin işlenmesine ilişkin ilkeler, verilerin yurt dışına aktarımı, veri işleme faaliyetinin hukuka uygunluğu gibi hususlar ele alınmıştır. Bu maddedeki birçok hüküm Kanun ile paraleldir.

Danıştay İdari Dava Daireleri Kurulu 5809 Sayılı Kanun'un 51.maddesinin 1.fıkrasına ilişkin Anayasa Mahkemesi'ne itiraz yoluna başvurmuş ve söz konusu fıkra iptal edilmiştir. İptal edilen fıkrada elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğin korunması hususlarında Bilgi Teknolojileri ve İletişim Kurumu'nun usul ve esasları belirlemeye yetkili olduğu düzenlenmiştir. Anayasa Mahkemesi'nin iptal gerekçesinde yasama yetkisinin devredilemezliği ilkesi uyarınca Anayasa'da açıkça kanunla düzenlenmesini öngörülen konularda yürütme organının ilk elden düzenleme yapamayacağını, Anayasa'nın 20. maddesinde düzenlenen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceği ifade edilmiştir[259].

Öte yandan Elektronik Haberleşme Kanunu nitelik bakımından e-Gizlilik düzenlemeleri ile paralel uygulama alanı olması gereken bir kanun olup, içerik bakımından hem e-Gizlilik Direktifi hem de EGT'den oldukça eksik bir düzenlemedir.

Yukarıda incelenen ETK-KVKK ilişkisi ve mevzuat düzenlemelerinin eksikliğinden kaynaklanan karışıklık aynı şekilde EHK-KVKK ilişkisinde de söz konusu olmaktadır. Özellikle ÇDP uygulamaları ve çerezlerin kullanımı konuları hem KVKK hem de

[259] Taştan ve Kaya, 2018: 196

EHK'nin kapsamına girmektedir ve bu çerçevede hangi kanun uygulamasının öncelikli sayılacağı ya da hangi düzenlemelerin birbirini nasıl destekleyeceği konusu mutlaka açıklığa kavuşturulmalıdır. Özellikle veri işleme şartları KVKK düzenlemelerine göre EHK kapsamında oldukça sınırlı sayıldığından çerezler vasıtasıyla kişisel verilerin işlendiği durumlarda hangi kanunun uygulama alanı bulacağı önem arz etmektedir.

Haberleşmenin sağlanması için gerekli olan çerez uygulamaları aynı e-Gizlilik Direktifi'nin 5. maddesi ile rıza istisnası kapsamında sayıldığı gibi EHK'nin 51. maddesi kapsamında da açık rızanın istisnası olarak belirtilmiştir. Yine de e-Gizlilik Direktifi rıza alınmasını gerektirmeyen halleri oldukça ayrıntılı düzenlerken EHK ilgili maddenin üçüncü fıkrasında yalnızca "haberleşmenin sağlanması" hallerinden bahsetmekte ve istisna kapsamını hem e-Gizlilik Direktifi hem de Çerez Rehberi ile belirlenen *"Kriter A"* grubu olarak sınırlı tutmaktadır.

EHK düzenlemeleri kapsamında "işletmeci" tarafından bahsedilmiş ve *"Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirket"* olarak tanımlanmıştır. Bu durumda EHK'nin uygulama alanı daraltılmış ve tüm veri sorumlularını kanun kapsamında yükümlü kılmak neredeyse imkânsız hale gelmiştir.

Yukarıda daha önce değindiğimiz Avrupa mevzuatı kapsamındaki düzenlemelere bakıldığında konu ile ilgili herhangi bir tartışma bulunmadığı çünkü çerez uygulamalarının GVKT'ye göre özel bir düzenleme olan e-Gizlilik Direktifi'nin bir konusu olduğu ve bu bağlamda incelenmesi gerektiği kabul edilmiş aynı zamanda herhangi bir düzenleme arasında çatışan haklar bulunmamasına özen gösterilmiştir.

Bu bağlamda gerek KVKK gerekse de EHK özelinde yapılacak düzenlemeler ile istisna hükümlerinin genişletilebileceği ve özellikle EHK kapsamında sorumlu taraf niteliğinin de değiştirilebileceği; bunun da çağın gerekliliklerine ayak uydurabilmek adına elzem olduğu kanaatindeyiz.

4.4. Değerlendirme

Yaşadığımız bu dijital çağda veri koruma ve gizlilik ihtiyaçlarına doğru şekilde yanıt verebilmek oldukça önemli bir konudur. Ticari hayatın ayrılmaz bir parçası halinde gelen kişisel verilerin bireylerin haklarını korumak ve işletmelerin güvenilirliğini artırmak açısından doğru düzenlenmiş sistemlerle korunması gerekmektedir. Bu

çalışma ile; yukarıda detaylı olarak açıklanan ulusal ve uluslararası kanun düzenlemeleri, yönetmelikler, tüzükler, rehber ve kararlar uyarınca kişisel verileri koruma mevzuatı ve ilgili mevzuat kapsamında çevrimiçi davranışsal pazarlama uygulamalarının değerlendirilmesi amaçlanmıştır.

Öncelikle KVKK ve GVKT karşılaştırmasının, Türkiye'deki mevcut durumu ve uluslararası iyi uygulamaları anlamak açısından doğru olacağı kanaatindeyiz. Zaten hâlihazırda kanunun hazırlık aşamasında o dönem Avrupa'da geçerli olan Direktif'ten faydalanıldığı dikkate alındığında gelişen teknoloji de göz önünde bulundurulursa KVKK kapsamında bir güncelleme ihtiyacı olduğu yadsınamaz. GVKT'nin yürürlüğe girmesi ile birlikte Direktif'in yürürlükten kaldırılması sonucunda, kişisel verilerin işlenmesine ilişkin daha sıkı koşullar getiren hükümlerle, yerel hükümler ve AB hukuku arasında önemli bir boşluk oluşmuştur. Bu noktada, KVKK'nin GVKT ile uyumlu hale getirilmesi, Türkiye'nin veri koruma politikalarını uluslararası standartlara uygun hale getirirken aynı zamanda yabancı yatırımları ve uluslararası işbirliğini de teşvik edecektir.

Uygulamada sorunlara yol açabilecek ve potansiyel olarak bu boşluğu oluşturan en dikkate değer farklılıklar; idari para cezası sınırları, veri işleyenin sorumlulukları, veri koruma görevlisi, verilere erişim ve veri taşınabilirliği, ortak veri sorumlusu, veri koruma etki değerlendirmesi gibi belirli konuları içermektedir.

KVKK'nin GVKT ile daha uyumlu hale gelmesi, Türkiye'nin uluslararası iş ve ticaret ortamında daha güvenilir bir partner olması anlamına gelecektir. Bu nedenle, bu konuda yapılacak çalışmaların ve düzenlemelerin Türkiye'nin dijital geleceği açısından büyük bir öneme sahip olduğu izahtan varestedir.

GVKT'nin yanı sıra, EHK'nin de e-Gizlilik Tüzük Taslağı ile uyumlu hale getirilmesinin, ÇDP uygulamaları öncelikli olarak birçok konuda avantaj sağlayacağı söylenebilecektir. Özellikle çerezler, izleme teknolojileri ve elektronik iletişim hizmetlerindeki veri koruma konularında daha ayrıntılı düzenlemeler, sıkı kurallar ve doğru istisnalar hem bireylerin korunması hem de organizasyonların işleyişi için kolaylık yaratan bir ortam oluşturacaktır. EHK'nin taslak tüzük ile uyumlu hale getirilmesi, Türkiye'nin dijital çağda veri koruma ve gizlilik konularında liderlik etme çabalarını da destekleyecektir.

Kişisel verilerin korunması ve Türkiye'nin uluslararası alanda güvenilir bir partner olarak konumunu güçlendirmesi için bu iki önemli konuda atılacak adımların hayati öneme sahip olduğu kanaatindeyiz.

SONUÇ

Bilgi ve iletişim teknolojileri ile internet kullanımında ortaya çıkan devrim niteliğindeki gelişmeler neticesinde, kamusal işlemlerden, ticarete, siyasi ve sosyal hayata kadar pek çok yaşam alanı etkilenerek, kalıcı şekilde değişime uğramıştır. Manuelden dijitale olarak da nitelendirilebilen bu değişiklikler, birçok tehdit ve fırsatı da beraberinde getirmiştir.

Artan veri akışı ve bu verilere erişimin kolaylaşması sayesinde, bilim ve teknolojide daha fazla ilerleme imkanının ortaya çıkması; kamu sektörü ve özel sektörde işlemlerin dijitalleşmesiyle birlikte işlem süre ve maliyetlerinin azalması, katma değerli, kişiselleştirilmiş, ve yenilikçi mal ve hizmetler ortaya konulmasının kolaylaşması; bilgi ve iletişim teknolojileri ile internet kullanımında yaşanan gelişmelerin ortaya koyduğu önemli fırsatlar arasında sayılabilecektir. Bu konuda ortaya çıkan en önemli fırsatlardan bir diğeri de, küresel e-ticaret hacminin tahminlerin çok ötesinde artmasıdır. Zira bu gelişmeler, dünya üzerindeki tüm pazarların dijital bir alternatifini ortaya koyarak, bu dijital pazarları da adeta görünmez zincirler yardımıyla birbirlerine bağlamıştır. Ortaya çıkan bu dijital bağlar sebebiyle, nerede kurulu olursa olsun bir ticari işletme, dünyanın herhangi bir yerindeki bir diğer işletme ya da tüketiciyle karşılıklı etkileşime girerek, dijital pazarlarda kolaylıkla mal ve hizmet alıp satarak, ticaret yapabilmektedir.

Yaygınlaşarak dünyayı çepeçevre saran çok çeşitli dijital sistem ve çevrimiçi ağlardan oluşan ve geleceğin iş modelleri olarak da tasvir edilerek, büyük bir hızla genel ekonomi içerisindeki payını artıran dijital ekonominin dışında kalmak ise dünya üzerindeki hiç bir aktör için kabul edilebilir bir durum olmamaktadır. Nitekim Avrupa Birliği de, dijital pazarların yarattığı büyük ekonomik potansiyeli görerek, Birlik'in dijital ekonomiye entegrasyonunun sağlanması bağlamında pek çok çalışma yaparak, bu konuda çeşitli stratejiler geliştirmeye çalışmaktadır. Avrupa Birliği'nin bu hususta ortaya koyduğu en önemli strateji belgelerinden biri de "Avrupa için Dijital Tek Pazar Stratejisi"dir. Avrupa Birliği, işbu Strateji kapsamında, her türlü ticaret engelinden arındırılarak, uyumlu Birlik yasaları dahilinde regüle edilip, parçalı pazar görünümünden kurtarılacak yekpare bir Avrupa dijital tek pazarının, Birlik'in dijital

ekonomiye entegrasyonunun sağlanması bakımından atılacak en önemli adımlardan biri olduğunun bilincindedir.

Avrupa Birliği, sadece iç pazarda dahi 500 milyondan fazla tüketiciye ulaşma potansiyeline sahip bulunan Avrupa dijital tek pazarının tamamlanması yoluyla, Birlik ekonomisine yılda yaklaşık 415 milyon Euro katkı sağlanabileceğinin de altını önemle çizmektedir. Bu sebeplerle, Birlik, dijital dönüşümü gerçekleştirerek, Avrupa dijital tek pazarının tamamlanması çalışmalarına büyük kaynak ve efor sarf etmektedir. Avrupa Birliği, bu yolla her geçen gün gelişerek, küresel anlamda genel ekonomi içerisindeki payını artıran dijital ekonomiden alacağı payı yükselterek, sürdürülebilir büyümeyi yakalayıp, rekabet edebilirlik ve istihdam oranlarını da artırarak, Avrupa Birliği'nde refah artışını desteklemeyi de hedeflemektedir.

Avrupa Birliği, bilgi ve iletişim teknolojileri ile internet kullanımındaki gelişmelerin yol açtığı dijitalleşmenin getirdiği tüm bu fırsatların farkında olarak, bir yandan dijital ekonomiye entegrasyon çalışmalarını sürdürürken, bir yandan da, bu fırsatların yanı sıra, pek çok tehdidin de var olduğunun bilincindedir. Özellikle sınır ötesi veri akışındaki artış ve çevrimiçi ağda toplanan verilerin büyük hacmi ve işlenme çeşitliliği ile bu verilere üçüncü kişilerin erişim oranlarındaki yükseliş sebebiyle ortaya çıkan, veri güvenliği ihlalleri ve buna bağlı olarak artan siber suçlar ile mahremiyete ve temel haklara ilişkin ihlaller, bu bağlamda sayılabilecek en önemli tehdit gruplarını oluşturmaktadır. Zira yaşanan dijital devrim ile birlikte hayatın her alanında ortaya çıkan çevrimiçi dijital ağ sistemleri içerisinde bulunan büyük miktar ve çeşitlilikteki kişisel ve kişisel olmayan veriler, tabiri caiz ise ışık hızıyla ve kütleler halinde, sınırlar arasında oradan oraya aktarılarak, farklı amaçlarla ve çok çeşitli şekillerde işlenebilmektedir. Hızla gelişen dijital teknikler karşısında engellenemeyen bu veri akışının ve işleme faaliyetlerinin, Birlik yasaları ile denetim altına alınarak, kişisel ve kişisel olmayan veri ayrımının doğru yapılması bu noktada büyük önem arz etmektedir. Nitekim bu ayrımın yapılarak Birlik hukukunda temel hak ve özgürlükler kapsamında tanınıp, koruma altına alınan kişisel verilerin, ortaya konacak Birlik düzeyinde uyumlu yasalar ve yaptırım mekanizmaları ile korunmaları, hem Birlik'in olmazsa olmaz etik değerlerinden sayılan temel hak ve özgürlüklerin güvence altına alınmasına, hem de Avrupa dijital tek pazarının güvenilirliğinin sağlanıp, parçalı yapısından kurtarılarak dijital ekonomiden alınacak payın yükseltilmesine, göz ardı edilemeyecek seviyede önemli katkılarda bulunabilecektir. Avrupa Birliği, tüm bu

hususları bir arada göz önünde bulundurarak hazırladığı "Avrupa için Dijital Tek Pazar Stratejisi" ile Avrupa dijital tek pazarının oluşumunun tamamlanması hedefi doğrultusunda kapsamlı bir Veri Koruma Reformu yapılmasının gereğinin altını önemle çizmiştir. Zira Birlik, gerçekleştirmeye çalıştığı ekonomik hedefleri doğrultusunda Avrupa dijital tek pazarının oluşumunu tamamlamaya çalışırken, aynı zamanda köklerinin dayandığı temel değerler ile insan haklarına saygı ilkesinden de ödün vermeye niyetli değildir.

Veri Koruma Reformu ile ortaya konan 2016/679 sayılı Genel Veri Koruma Tüzüğü, gerek temel hak ve özgürlüklerin Birlik düzeyinde korunması, gerekse de uyumlu Birlik yasaları dâhilinde Avrupa dijital tek pazarının oluşumunun tamamlanarak, parçalı pazar görünümünden kurtarılması hususlarında atılmış önemli bir adım niteliğindedir.

Genel Veri Koruma Tüzüğü'nün kabulüne kadar geçen sürede, kişisel veriler, bu verilerin korunması ve serbest dolaşımlarının sağlanmasında çerçeve niteliğinde hükümler getirip, bu hususta yasal düzenleme yapma yetkisini ise üye devletlere bırakması sebebiyle, Birlik içinde farklı uygulamaların ortaya çıkmasına sebep olarak eleştirilerin hedefi haline gelen mülga 95/46 sayılı Direktif kapsamında korunmaya çalışılmıştır. Oysa bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ve dijital çağın gerekleri göz önüne alındığında, temel haklardan biri olan kişisel verilerin, Birlik hukukunda bir direktif kapsamında korunmasının yeterli olmadığı, dijital çağın gereksinimlerine uygun, Birlik düzeyinde uyumlu olan ve güçlü yaptırım mekanizmaları ile desteklenen, doğrudan uygulanabilir yasa hükümlerine ihtiyaç olduğu zaman içinde Birlik tarafından daha net olarak anlaşılmıştır. Öte yandan Türkiye sınırları içerisinde hala ilgili Direktif kapsamında hazırlanmış bir veri koruma kanununun geçerli olduğunu da burada tekraren belirtmek uygun olacaktır. Genel Veri Koruma Tüzüğü'nün kabulü ile birlikte kişisel verilerin, Birlik düzeyinde doğrudan uygulanabilir ve uyumlu yasa hükümleri kapsamında koruma kazanmaları, dijitalleşme ile ortaya çıkan yeni tehditlerle baş edilerek, temel hak ve özgürlüklerin daha etkili bir şekilde korunmaları, hem Avrupa dijital tek pazarında hukuki öngörülebilirlik ve güvenin tesisi ile pazarda işlem hacminin artırılması yoluyla, Birlik'in küresel dijital ekonomi kapsamında ortaya çıkan fırsatlardan en iyi şekilde yararlanması, hem de Avrupa dijital tek pazarının parçalı görünümünden kurtulması yönünde atılmış, bir adım niteliğindedir. Zira kişisel verilerin Birlik düzeyinde

doğrudan uygulanabilir, uyumlu ve güçlü yasalarla korunması, tamamlanmaya çalışılan Avrupa dijital tek pazarında veri güvenliğinin yükseltilmesine katkıda bulunacağı gibi, kişisel verilerin korunmasında ve serbest dolaşımlarının sağlanmasında Birlik içindeki yasa ve uygulama farklılıklarından kaynaklanan eşitsizlikleri gidererek, hukuki öngörülebilirliği de artırmaktadır. Ayrıca, kişisel verilerin korunması hususundaki uyumlu yasalar dâhilinde veri güvenliğinin ve hukuki öngörülebilirliğin sağlanması, neticede Birlik içindeki ve dışındaki tüketicilerin güveninin kazanılmasını da beraberinde getirmektedir.

Tüm bunların yanı sıra, Genel Veri Koruma Tüzüğü, kişisel verilerin korunması ve Birlik dışı üçüncü ülkelere veri aktarımı hususlarında, temel hakların korunması perspektifinden hareketle bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte ortaya çıkan tehditlerle gerektiği gibi başa çıkılarak, kişisel verilere hak ettikleri yüksek korumanın sağlanması hedefleri doğrultusunda, üçüncü ülkelerle kıyaslandığında sert hükümler içermektedir. Genel Veri Koruma Tüzüğü, bu sebeple, Avrupa Birliği'ni aşılması zor bir dijital kaleye dönüştürdüğü gerekçesi ile eleştirilmiştir. Ancak Genel Veri Koruma Tüzüğü'nün kişisel verilere Birlik genelinde sağladığı yüksek standartlardaki korumanın, hukuki öngörülebilirliği tesis ederek, Avrupa dijital tek pazarında güvenilirliği artırması sebepleriyle, orta ve uzun vadede bu eleştirileri boşa çıkararak, tüketici ve şirketlerin işlemlerinde Avrupa dijital tek pazarını tercih etmelerine ve neticede de rakipleri karşısında küresel ticarette Birlik'e rekabet avantajı sağlayarak, Avrupa Birliği'nin rekabet edebilirliğinin yükselmesine yol açmıştır.

Özellikle Türkiye gibi aday ülkelerde kişisel verilerin korunması hususunda Birlik'teki gelişmelere paralel olarak yapılan ya da yapılmaya çalışılan yasal düzenlemeler incelendiğinde, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü kapsamında yapmış olduğu yasal düzenlemelerin, bu hususlarda farkındalık yaratarak, Birlik'in küresel arenada öncü kural koyucu olma hedefine katkı sağladığı da anlaşılmaktadır.

Economist Dergisi'nde yayınlanan 21 Aralık 2019 tarihli makale de, Birlik'in kişisel verilerin korunması hususunda üçüncü ülkelere kural ihraç ederek, bu konularda öncü olma iddiasını destekler niteliktedir. Nitekim bu makale ile, Amerika Birleşik Devletleri'nin Kaliforniya Eyaleti'nin, yürürlüğe girdiği tarihten itibaren, küresel arenada faaliyet göstererek, pek çok konuda lider durumda bulunan dev dijital teknoloji firmalarını derinden sarsan, GVKT ile uyumlu olan, "Kaliforniya Tüketici

Mahremiyeti Kanununu (California Consumer Privacy Act-CCPA)", Ocak 2019 tarihi itibarı ile, ülkenin tamamının önüne geçerek, kabul ettiğinin altı çizilmektedir. Avrupa Birliği'nin 500 milyonu aşkın kullanıcıya sahip olan yekpare dijital tek pazarında faaliyetlerine devam etmekte istekli olan, Microsoft ve Apple gibi Amerikan teknoloji devleri de bu gelişmelere paralel olarak yaptıkları açıklamalarla, CCPA'nın sadece Kaliforniya'da değil, Birleşik Devletlerin tamamında uygulanmasını sağlayacak düzenlemeleri yapmayı planladıklarını beyan etmişlerdir. Bu beyanlardan hareketle, Genel Veri Koruma Tüzüğü'nün, lider teknoloji firmalarının dikkatlerini yoğun olarak çekerek, Amerika Birleşik Devletleri de dâhil olmak üzere küresel dünyanın tamamını kişisel verilerin korunması hususlarında etkilediği ve Birlik tarafından ortaya konan bu hüküm ve ilkelerin, yayılarak evrensel hale gelmede her geçen gün bir adım daha ileri gittiğini söylemek yanlış olmayacaktır.

Mart 2020 tarihinden itibaren küresel arenada olduğu gibi Avrupa Birliği'nde de Covid 19 salgınına ilişkin etkiler, dramatik bir şekilde hissedilmiştir. Bu pandemi süreci beraberinde Birlik'in e-ticaret hacminde artış gibi kimi fırsatlar getirse de, aynı zamanda mahremiyetin ve kişisel verilerin korunması gibi temel hak ve özgürlükler kapsamında bazı önemli tehditler de ortaya koymuştur. Nitekim Genel Veri Koruma Tüzüğü ile hassas kişisel veriler kapsamında kabul edilerek korunmalarına ilişkin daha sıkı kurallar getirilen bireylerin sağlık ve konum verilerinin korunmalarına ilişkin hükümlerin, kamu sağlığı ve kamu yararının korunması istisnaları çerçevesinde, pandemi döneminde Avrupa Birliği'nde de gevşetildiği anlaşılmaktadır. Bu durum özellikle mobil uygulamalar aracılığıyla, hasta kişilerin yerlerinin belirlenerek, bu kişilerin hareketlerinin kontrol edilmeye çalışılması hususunda atılan adımlarla iyiden iyiye su yüzüne çıkmıştır. Toplum sağlığını etkileyen bu ölçekteki bir salgının, kimi kısıtlamaları kaçınılmaz kıldığı yadsınamasa da kişisel verilerin korunmasına ilişkin istisnaların uygulanırken, Genel Veri Koruma Tüzüğü madde 23/1'de belirtildiği gibi hakkın özüne dokunmadan, meşru bir amaca hizmet etmek için gerekli olandan fazla olmamak kaydı ile ve toplumsal demokrasi anlayışına zarar gelmeden orantılılık ilkesi çerçevesinde yapılmasının gerekli ve önemli olduğu unutulmamalıdır.

Sonuç olarak söylemek gerekirse; Genel Veri Koruma Tüzüğü ile getirilen Birlik düzeyinde uyumlu yasal düzenlemelerin, temel hak ve özgürlüklerin korunarak, kişisel verilerin Avrupa dijital tek pazarında güvenli bir şekilde serbest dolaşımlarının sağlanması temel hedeflerinin gerçekleşmesine katkıda bulunduğu yadsınamaz. Ancak

Genel Veri Koruma Tüzüğü ile Avrupa Birliği'nin kişisel verilerin korunması hususunda kat etmiş olduğu önemli mesafeye rağmen, gerek şirketlerin, gerek çalışanların, gerekse de hane halkının dijital kültürü benimseyerek bu bağlamda gerekli teknik becerileri elde edebilmeleri noktasında, Avrupa Birliği'nin, ABD, Çin, Güney Kore gibi rakipleri ile karşılaştırıldığında hala biraz daha geride olduğu söylenebilecektir.

Bilgi ve iletişim teknolojileri ve internet alanında yaşanan gelişmeler büyük bir süratle devam ettiğinden, Avrupa Birliği'nin kişisel verilerin korunması bağlamında ortaya çıkabilecek yeni fırsat ve tehditlere ilişkin çalışmalarını sürdürmesinin ne kadar önemli olduğu bir kere daha ortaya çıkmaktadır.

Kişisel verilerin korunması konusunda özellikle de çevrimiçi davranışsal pazarlama uygulamalarına kapsamında, Avrupa Birliği düzenlemelerinin sürekli gelişim ve değişim sürecinde olduğunu aşikârdır.

Öte yandan, Türkiye'nin günümüzde bu konuda hala önemli eksiklikleri olduğunu kabul etmek gerekmektedir. KVKK ve GVKT arasındaki belirgin bir farklardan ilki, yaptırımların limitleri ve uygulanma aralıklarıdır. GVKT, ihlaller durumunda, genellikle şirketlerin yıllık küresel cirosunun %4'üne kadar para cezası uygulayabilmekte, bu da caydırıcılığı artıran ve veri sorumlularını veri koruma ihlallerine karşı daha dikkatli olmaya teşvik eden bir düzenleme olarak görülmektedir. Öte yandan KVKK'nin yaptırımları ise, maddi anlamda caydırıcılıktan uzak olup, özellikle son dönemde verilen kararlarda uygulanan para cezası miktarları incelendiğinde genellikle alt sınıra yakın olduğu görülmektedir.

Veri işleyen tanımı her iki mevzuat kapsamında neredeyse aynı şekilde belirlenmiş olsa da veri işleyenin sorumlulukları GVKT ile oldukça ayrıntılı şekilde açıklanmıştır. Her ne kadar veri sorumlusu GVKT kapsamında ana sorumlu olmaya devam etse de veri işleyen de veri sorumlusu kadar katı olmasa da ihlal halinde sorumlu tutulabilmektedir.

Bununla birlikte, GVKT, veri sorumlularının bir veri koruma görevlisi ("DPO") atamasını da zorunlu kılmaktadır. Bu kişi kişisel veri korunması alanında bilgili ve yönlendirme sağlayabilecek yetkinlikte olmalıdır. KVKK'da ise, böyle bir zorunluluk olmayıp, bu durum özellikle büyük ölçekli şirketlerde veri koruma stratejilerini etkilemekte ve etkin bir denetim mekanizmasının eksikliği riskini doğurmaktadır.

Diğer bir konu ise GVKT madde 20 ile düzenlenen verinin taşınabilirliği ve erişim hakkıdır. Bu kapsamda ilgili kişiler diledikleri takdirde kişisel verilerine erişebilir veya tüm verilerinin başka bir veri sorumlusuna aktarılmasını talep edebilirler. Veri taşınabilirliği düzenlemeleri ancak açık rıza ve sözleşmenin kurulması/ifası şartlarından birine dayanılarak kişisel verilerin işlendiği hallerde mümkün olacaktır. Öte yandan her ne kadar KVKK'da ilgili kişi haklarını düzenleyen 11. madde ile kişilere tanınan "kişisel veri işlenip işlenmediğini öğrenme ve kişisel verileri işlenmişse buna ilişkin bilgi talep etme" hakkı çoğu zaman erişim hakkı ile karıştırılsa da GVKT ile düzenlenen erişim hakkı, ilgili kişilere işlenen tüm verilerinin bir kopyasını talep etme imkânı vermektedir.

Özellikle ÇDP uygulamaları kapsamında oldukça önem arz eden başka bir konu ise veri koruma etki değerlendirmesidir. GVKT madde 35 ile ayrıntılı olarak düzenlenen etki değerlendirmeleri veri sorumluları tarafından gerçekleştirilen ve veri işleme faaliyetinin kişisel verilerin korunması konusundaki etkilerini değerlendiren bir işlemdir. Çerezler gibi yeni teknolojilerin uygulamaya konulmadan önce veya uygulama sırasında; çalışma şekli, riskleri, işleme kapsamı ve amacı da dikkate alınarak, veri işlemenin gerekliliği ve orantılılığını ölçen bu süreçlerin veri koruma mevzuatına uyumluluğun sağlanması açısından rolünün önemli olduğu kanaatindeyiz.

Son olarak GVKT'nin 26. maddesi ile açıkça düzenlenmiş ortak veri sorumlusu kavramı KVKK'de yer almamaktadır. Öte yandan Kurul tarafından yayımlanan "Araç kiralama sektöründeki kara liste uygulamaları hakkında Kişisel Verileri Koruma Kurulunun 23/12/2021 tarihli ve 2021/1304 sayılı İlke Kararı" ile ortak veri sorumlusu tanımı yapılmıştır. Böyle bir tanımın kanun veya yönetmelik vasıtasıyla değil bir karar ile yapılmış olması, bizim de katıldığımız üzere, öğretide oldukça fazla eleştiri almıştır.

Çevrimiçi davranışsal pazarlama uygulamalarının kişisel verilerin korunması mevzuatı kapsamında değerlendirilmesi neticesinde ise yalnızca KVKK ve GVKT uyumlandırılması değil aynı zamanda EHK'de de belirli güncelleme ihtiyacının varlığı yadsınamaz. Özellikle çerezler söz konusu olduğunda kanuni bakımından erişilebilen tek düzenleme yine EHK kapsamında bulunmaktadır.

Her ne kadar çerezlere yönelik bazı düzenlemeler EHK ile getirilmiş olsa da özellikle Avrupa düzenlemeleri dikkate alındığında güncel teknolojik gelişmelerin geriden

takip edildiğini söylemek yanlış olmayacaktır. Yukarıda da ayrıntılı olarak değinildiği üzere EHK madde 51/3 hükmü uyarınca ilgili kanun yalnızca işletmelere uygulanabilmekte ve taraf yönünden oldukça daraltıcı bir kısıta gidilmiş bulunulmaktadır. Gerekli korumayı doğru şekilde sağlayabilmek adına EHK kapsamının ve en azından belirli hükümler doğrultusunda uygulama alanının genişletilerek "veri sorumlusu" tanımına uygun hale getirilmesi kayda değer bir adım olacaktır.

Öte yandan EHK kapsamındaki çerezler düzenlemesi yalnızca elektronik haberleşmenin sağlanması için gerekli olan halleri kapsamaktadır, bu halde EHK, Çerez Rehberi ve sair Kurul Kararları dikkate alındığında açık rızaya dayanarak çerezlerin kullanımının da mümkün olduğu anlaşılsa da diğer zorunlu haller ve dahi istisnalar konusunda yasal bir boşluk yaratmaktadır. Her ne kadar daha önce de bahsedildiği üzere Çerez Rehberi ve bazı kararlar ile ilgili konu düzenlenmeye çalışılmışsa da bizim de katıldığımız şekilde öğretide bu durum yeterli bulunmamakta ve kanuni bir düzenleme ihtiyacı vurgulanmaktadır.

Bu çerçevede yapılması beklenen güncellemeler ile EHK kapsamının ve özellikle kanun metninde yer alan tanımların genişletilerek değiştirilmesi, gelişen teknolojik araçlar ve AB güncel mevzuatı dikkate alınarak EHK ve dahi KVKK içeriğinde değişikliğe gidilmesi gerekmektedir.

İlgili sebepler ve AB yasal düzenlemeleri dikkate alındığında mevcut KVKK ve EHK düzenlemelerinin gelecek teknolojik gelişmeler şöyle dursun güncel durum dikkate alındığında bile yenilenmeye yönelik ihtiyacı izahtan varestedir.

Avrupa Birliği'nin getirdiği düzenlemelerin, dijital yaşamın güvenliği ve kişisel verilerin korunmasını sağlama konusunda elde ettiği başarı yadsınamazken, gelişen teknoloji karşısında güncelleme ve yenilik arayışı da hız kesmeden devam etmektedir.

Henüz beş yıl önce yürürlüğe giren GVKT'nin güncellenme ihtiyacının Avrupa kulislerinde görüşüldüğü, e-Gizlilik Direktifi'nin yerine hazırlanan e-Gizlilik Tüzüğü taslağının değerlendirildiği dikkate alındığında *95/46/EC sayılı Avrupa Birliği Veri Koruma Direktifi* temel alınarak hazırlanmış olan KVKK'nin çağı yakalamakta güçlük çekeceği de açıktır. İşbu çalışma ile dikkat çekilmesi amaçlanan Türkiye mevzuatındaki eksiklikleri gidermek için Avrupa Birliği düzenlemelerinin dikkate alınması ve ülkemiz sınırları içerisinde de hayata geçirilmesi büyük önem

taşımaktadır. Türkiye'de, mevcut mevzuat ile evirilen dijital manzara arasındaki uçurumu kapatma ihtiyacı bulunmaktadır. Türkiye'nin hukuki çerçevesini Avrupa Birliği'nin belirlediği prensip ve standartlarla uyumlu hale getirmek için önemli adımlar atılmalıdır. Bu durum, salt KVKK değişikliği değil, gerekli e-ticaret düzenlemeleri, EHK değişiklikleri, yeni yönetmelikler gibi önemli revizyonları gerektirirken, uygulama mekanizmalarının da güçlendirilmesi teorinin pratiğe döndüğü noktada kaçınılmazdır.

Türkiye'nin, Avrupa standartlarına uygun etkili düzenlemeler geliştirmeyi öncelik haline getirmesi ve benzer uygulamaları kendi yasal çerçevesine dahil etmesi, dijital çağın getirdiği zorluklara yanıt verebilmesi için hayati önem taşımaktadır. Bu, Türkiye'nin dijital ekonomide daha güçlü bir pozisyon elde etmesine ve dijital ortamda daha fazla güven oluşturmasına yardımcı olacaktır.

Bu sebeple, bu tez çalışması kapsamında yapılan incelemeler neticesinde, hem genel kapsamda temel hak ve özgürlüklerden olan kişisel verilerin korunması alanında hem de ilgili çerçevede yürütülen çevrimiçi davranışsal pazarlama uygulamaları özelinde Avrupa Birliği gelişmelerinin takibi ve yerel mevzuata uygulanmasının önemi vurgulanmış, teknolojik gelişmelerin hız kesmeden devam ettiği ve edeceği de dikkate alınarak Birlik'in bu konudaki araştırma ve çalışmalarının da devam edeceği öngörüldüğünden bu uyumluluk sürecinin de hız kesmeden devam ettirilmesi gerekliliğine vurgu yapılmak istenmiştir.

KAYNAKÇA

Acharjya, Debi Prasanna, ve Ahmed, Kauser (2016). "A Survey on Big Data Analytics: Challenges, Open Research Issues and Tools." International Journal of Advanced Computer Science and Applications, 7(2), 511-518.

Akçalı Gür, Berna. (2019). Uluslararası hukuk ve AB hukuku boyutuyla kişisel verilerin yurt dışına aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi- Prof. Dr. Ferit Hakan Baykal Armağanı, 25 (2), 850-872.

Akgül, Aydın. (2014). Danıştay ve Avrupa İnsan Hakları Mahkemesi kararları ışığında kişisel verilerin korunması. İstanbul: Beta Yayıncılık.

Akıncı, Ayşe Nur. (2019). Büyük veri uygulamalarında kişisel veri mahremiyeti. T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı Sektörler ve Kamu Yatırımları Genel Müdürlüğü Uzmanlık Tezi, Yayın No: 0001.

Akipek, Jale; Akıntürk, Turgut; ve Ateş, Derya. (2015). Türk medeni hukuku- Başlangıç hükümleri Kişiler hukuku I. cilt. (Yenilenmiş 12. Baskı), İstanbul: Beta Yayıncılık.

Aksar, Yusuf (2013). Teoride ve uygulamada uluslararası hukuk- II. (2. Baskı), Ankara: Seçkin Yayıncılık.

Aksoy, Hüseyin Can ve Halıcıoğlu, Mesut. (2021). AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme. Kişisel Verileri Koruma Dergisi 3(1), 61-88.

Alarslan, Fatma. (2016). Medeni Hukuk'da dürüstlük kuralı ve hakkın kötüye kullanılması yasağı. Çankaya Üniversitesi Hukuk Fakültesi Dergisi, 1 (2), 413-434.

Altındere, Murat. (2020). Kişisel verilerin korunması hukuku ve uygulaması. Ankara: Adalet Yayınevi.

Anderson, Chris (2009). Free: The Future of Radical Price. London: Random House Business Books.

Anı, Nevzat Ali. (2018). Kişisel verilerin işlenmesi ve açık rıza. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Aras, Ümit Yaşar. (2010). İnsan hakları temelinde özel hayat hakkının ulusal ve uluslararası alanda uygulamaları. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.

Arslan Öncü, Gülay. (2019). Özel yaşama ve aile yaşamına saygı hakkı- Anayasa Mahkemesine bireysel başvuru el kitapları serisi-. Avrupa Konseyi Ankara Program Ofisi.

Article 29 Data Protection Working Party, (2011) "Advice Paper on Special Categories of Data ("Sensitive Data")", Ref.Ares (2011)444105 – 20.04.2011, https://www.pdpjournals.com/docs/88417.pdf adresinden 02 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party (2017). "Guidelines on Consent under Regulation 2016/679, Adopted on 28.11.2017", WP259rev.01, as last revised and adopted on 10.04.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 adresinden 02 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to result in a High Risk' for the Purposes of Regulation", 2016/679, 13.10.2017, 17/EN WP 248 rev.01, https://ec.europa.eu/newsroom/artic-le29/item-detail.cfm?item_id=611236 adresinden 02 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (Aralık 2016) "Guidelines on Data Protection Officers ("DPOs")" Adopted on 13 December 2016, 16/EN WP 243, https://ec.europa.eu/information_society/newsroom/image/document/201651/wp243_en_40855.pdf?wb48617274=CD63BD9A adresinden 07 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (3 Ekim 2017) "Guidelines on Personal Data Breach Notification under Regulation 2016/679", 03.10.2017, WP250 17/EN, https://webcache.googleusercontent.com/search?q=cache:X49fS0vPpRgJ:https://ec.europa.eu/newsroom/document.cfm%3Fdoc_id%3D47741+&cd=1&hl=tr&ct=clnk&gl=tr&client=safari , adresinden 12 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (Ekim 2017) "Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation", 2016/679, 17/EN WP 253, 3.10.2017, https://knowww.eu/search-

tree?t=5ad7131ed39f5-aa2bcbf0f34# , adresinden 11 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (2016) "Guidelines on the Right to Data Portability", adopted on 13 December 2016 as last revised and adopted on 5 April 2017, WP 242, rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 , adresinden 18 Haziran 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (Transperancy, 2017) "Guidelines on Transparency under Regulation 2016/679", WP260, adopted on 29.11.2017, as last revised and adopted on 11.04.2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item-622227,_id= adresinden 10 Temmuz 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (2013). "Working Document 02/2013 providing guidance on obtaining consent for cookies" https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf adresinden 24 Kasım 2022 tarihinde erişilmiştir.

Article 29 Data Protection Working Party. (2012). "Opinion 04/2012 on Cookie Consent Exemption". Brüksel. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf adresinden 28 Kasım 2022 tarihinde erişilmiştir.

Aşıkoğlu, Şehriban İpek. (2018). Avrupa Birliği ve Türk Hukukunda kişisel verilerin korunması ve büyük veri, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi, İstanbul: On İki Levha Yayıncılık.

Atak, Songül. (2010). Avrupa Konseyi'nin kişisel veriler açısından sağladığı temel güvenceler. TBB Dergisi, 2010 (87), 90-120.

Avcı Braun, Cihan. (2018). "Kişisel Verilerin İşlenmesinde Rıza", YÜHFD, C.XV, 2018/1, s.13-33.

Ayözger Öngün, Çiğdem. (2019). Kişisel verilerin korunması hukuku- elektronik haberleşme sektörüne ilişkin özel düzenlemeler dahil. (Genişletilmiş 2. Baskı). İstanbul: Beta Yayıncılık.

Aytın, Sinem. (2017). Televizyon yoluyla kişilik hakkı ihlalinden doğan manevi tazminat davası. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Başkent Üniversitesi Sosyal Bilimler Enstitüsü.

Badur, Emel. (2017). Tıbbi müdahaleye rızanın özellik gösterdiği haller. Ankara: Seçkin Yayıncılık.

Basan, Nuri Mehmet ve Bilir, Nazmi. (2016). Koruyucu sağlık hizmetlerinde önleme çelişkisi ve nedenleri. TAF Preventive Medicine Bulletin, 15 (1), 44-50.

Başalp, Nilgün. (2015). Avrupa Birliği Veri Koruma Genel Regülasyonunun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MÜHF HAD), 2015, 21(1), 77-105.

Başar, Cemal. (2019). Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması. Yayımlanmamış Doktora Tezi. İzmir: Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü.

Boerman, Sophie C., Sanne Kruikemeier, and Frederik J. Zuiderveen Borgesius. "Online behavioral advertising: A literature review and research agenda." Journal of advertising (2017), 46(3), 363-376.

Bradlow, Eric; Gangwar, Manish; Kopalle, Praveen ve Voleti, Sudhir (2017). "The Role of Big Data and Predictive Analytics in Retailing." Journal of Retailing, 93, 76-96.

Bump Pamela. (2022). The Death of the Third-Party Cookie: What Marketers Need to Know About Google's 2023 Phase-Out. https://blog.hubspot.com/marketing/third-party-cookie-phase-out adresinden 25 Ağustos 2022 tarihinde erişilmiştir.

Bulut Çimen, İpek, (2020). Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Getirilen Yeni Teknik ve Yaptırım Mekanizmaları. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 20(2), 127-142

Bulut, Nihat. (2008). Eski Yunan'dan aydınlanma çağına insan onuru kavramının gelişimine genel bir bakış. Erzincan Üniversitesi Hukuk Fakültesi Dergisi, 12 (34), 1-12.

Buttarelli, Giovanni. (2016). The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", Guest Editorial. International Data Privacy Law, Cilt.6, Sayı.2, 77-78.

Chen, Jianqing ve Stallaert, Jan. (2014). “An Economic Analysis of Online Advertising Using Behavioral Targeting.” MIS Quarterly, 38(2), 429-449.

Çekin, Mesut Serdar. (2016). 6698 sayılı kişisel verilerin korunması hakkında kanun’un big data (büyük veri) ve irade serbestisi açısından değerlendirilmesi. İstanbul Üniversitesi Hukuk Fakültesi Dergisi, 74(2), 629-644.

Çekin, Mesut Serdar. (2020). Avrupa birliği hukukuyla mukayeseli olarak 6698 sayılı kanun çerçevesinde kişisel verilerin korunması hukuku. (3. Baskı). İstanbul: On İki Levha Yayıncılık.

Çelik, Yeşim. (2017). Özel hayatın gizliliğinin yansıması olarak kişisel verilerin korunması ve bu bağlamda unutulma hakkı. Türkiye Adalet Akademisi Dergisi, Yıl: 8, Sayı: 32, 391-410.

Çelikel, Serdar. (2021). Kişisel verilerin işlenmesinde, açık rıza hukuka uygunluk nedeninin, 95/46 sayılı Direktif ve GDPR’la karşılaştırılmalı olarak incelenmesi. Uyuşmazlık Mahkemesi Dergisi, Yıl:9 Sayı: 17, 161-190.

Dal, Ufuk. (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü’nün ülke dışı uygulama yetkisi ve bu yetkinin uluslararası hukukta meşruiyeti. Kişisel Verileri Koruma Dergisi, 1 (1), 21-33.

Davenport, Thomas. (2014). Big Data @ Work: Efsaneye Son Vermek, Fırsatları Keşfetmek. (Çev. Müge Çavdar) İstanbul: Türk Hava Yolları Yayınları

Davis, Joel J. (1994). “Ethics in Advertising Decisionmaking: Implications for Reducing the Incidence of Deceptive Advertising.” The Journal of Consumer Affairs, 28(2), 380-402.

Develioğlu, Hüseyin Murat (2017). Avrupa birliği genel veri koruma tüzüğü. (1.Baskı). İstanbul: On İki Levha Yayıncılık.

Diker Vanberg, Aysem ve Ünver, Mehmet Bilal (2017). The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?, European Journal of Law and Technology, Cilt.8, Sayı.1, 2017, 1-22.

Doğan, Başak ve Bozkurt, Tuğçe. (2020). Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle. Lexpera Blog.

Drumwright, Minette E. ve Murphy, Patrick E. (2009) The Current State of Advertising Ethics: Industry and Academic Perspectives, Journal of Advertising, 38:1, 83-108.

Duman, Berat. (2020). Anayasa hukukunda kişisel verilerin korunması. Yayımlanmamış Doktora Tezi. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Dülger, Murat Volkan. (2018). İnsan hakları ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5 (1), 71-143.

Dülger, Murat Volkan. (2020). Kişisel verilerin korunması hukuku. (3.Baskı). İstanbul: Hukuk Akademisi Yayıncılık.

Ensari, Ali Burak (2014). Çevrimiçi Davranışsal Pazarlamanın Tüketici Davranışları Üzerindeki Etkileri ve Kişisel Verilerle ilişkisi. İstanbul Bilgi Üniversitesi. Yayınlanmamış Yüksek Lisans Tezi. İstanbul.

European Data Protection Board (EDPB) (2018). Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications. https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_en.pdf adresinden 17 Nisan 2022 tarihinde erişilmiştir.

Fayyad, Usama; Piatetsky-Shapiro, Gregory ve Smyth, Padhraic (1996). "From Data Mining to Knowledge Discovery in Databases." AI Magazine, 17(3), 37-54.

Fendoğlu, Hasan Tahsin. (2018). Hukuka Giriş.(4. Baskı), Ankara: Yetkin Yayınları.

Gare, Elisson, (2016). Profiling and Online Behavioural Advertisement Under the GDPR Has the New Regulation Succeed in Ensuring the Protection of Fundamental Rights without Hindering innovation and Economic interests in the Digital Economy? Yüksek Lisans Tezi. Oslo Üniversitesi.

GDPR EU (2020). Cookies, the GDPR, and the ePrivacy Directive. https://gdpr.eu/cookies/ adresinden 18 Ocak 2023 tarihinde erişilmiştir.

GDPR EU (t.y.). A guide to GDPR data privacy requirements. https://gdpr.eu/data-privacy/ adresinden 10 Aralık 2022 tarihinde erişilmiştir.

Girgin, Atilla, (2003). Yazılı Basında Haber ve Habercilik Etiği. İstanbul: inkılap Yayıncılık.

Giurgiu, Andra ve Lommel. Gerard (2014). A New Approach to EU Data Protection, More Control Over Personal Data and Increased Responsibility, Critical Quarterly for Legislation and Law, Cilt. 97, Sayı. 1, 10-27.

Goddard, Michelle. (t.y.) The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact, International Journal of Market Research, Cilt.59, Sayı.6, 703-705.

Golla, Sebastian. (2017). Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, Journal of Intellectıal Property, Information Technology and E-Commerce Law, Cilt.70, Sayı. 8 (1), 70-78.

Göçmen Uyarer, Sinem (2020). Kişisel verilerin korunması. (2. Baskı), Ankara: Seçkin Yayıncılık.

Gümüş, Ali Tarık (2004). Türk anayasasında kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı. Yayımlanmamış Yüksek Lisans Tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Gürpınar, Damla. (2017). Kişisel verilerin korunamamasından doğan hukuki sorumluluk. Dokuz Eylül Hukuk Fakültesi Dergisi, Prof. Dr. Şeref Ertaş'a Armağan 19 (Özel Sayı-2017), 679-694.

Ham, Chang-Dae. (2017). "Exploring How Consumers Cope With Online Behavioral Advertising." International Journal of Advertising, 36(4), 632-658.

Hunt, Matthew K. (2016). "Cookie Consumer: Tracking Online Behavioural Advertising in Australia." Computer Law & Security Review, 32, 55-90.

Interactive Advertising Bureau (IAB). (2023). Understanding the Transparency & Consent Framework v2.2. https://iabeurope.eu/blog/understanding-the-upcoming-transparency-consent-framework-v2-2/ adresinden 26 Nisan 2023 tarihinde erişilmiştir.

Information Commissioner's Office (ICO Consent). (t.y.). What is valid consent? İngiltere https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-

consent/#:~:text=All%20consent%20must%20involve%20a,(whether%20oral%20or%20written) adresinden 22 Ocak 2023 tarihinde erişilmiştir.

Information Commissioner's Office (ICO Cookies). (t.y.). Guidance on the use of cookies and similar technologies. İngiltere. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf adresinden 15 Aralık 2022 tarihinde erişilmiştir

İbrahimoğlu Güreş Selen, Aytaç Batuhan, (2019). Kişisel Verileri Koruma Kurulu'nun Elektronik Ticari İletilerle İlgili İlke Kararına Dair Güncel Tartışmalar. https://www.ozbek.av.tr/kvk-blog/kisisel-verileri-koruma-kurulu-nun-elektronik-ticari-iletilerle-ilgili-ilke-kararina-dair-guncel-tartismalar/ adresinden 12 Ocak 2023 tarihinde erişildi.

İmançlı, Canan (2020). Kişisel sağlık verilerinin korun(a)mamasından doğan özel hukuk sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Özel Hukuk Yüksek Lisans Tezleri Dizisi, İstanbul: On İki Levha Yayıncılık.

Keser, Yıldırım (2020). Tüketicinin kişisel verisinin işlenmesinde açık rıza. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 28 (3), 1181-1215.

Keser Berber, Leyla. (2014). Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması. istanbul: On iki Levha Yayıncılık.

Kılıçoğlu, Ahmet M. (2013). Borçlar hukuku genel hükümler. (Genişletilmiş 17.Bası). Ankara: Turhan Kitabevi.

Kim, Yoojung. (2014). "Consumer Privacy Concerns and Responses to Online Behavioral Advertising: A Cross-Cultural Comparison of Americans and Koreans." Proceedings of the Conference - American Academy of Advertising, (s. 163-164). Atlanta.

Kişisel Verileri Koruma Kurulu (2020). "Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6739/2020-173 adresinden 24 Mayıs 2022 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurumu (2019). Kişisel verilerin korunması kanununa ilişkin uygulama rehberi. Ankara. Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu.

Kişisel Verileri Koruma Kurumu (2021). Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu. KİŞİSEL VERİLERİ KORUMA KURUMU | KVKK | Mağazalarda Alışveriş Sırasında İlgili Kişilere SMS ile Doğrulama Kodu Gönderilmesi Suretiyle Kişisel Verilerin İşlenmesine İlişkin Kamuoyu Duyurusu adresinden 18 Eylül 2022 tarihinde erişilmiştir.

Kişisel Verileri Koruma Kurumu (2022). 6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2. Ankara.

Kişisel Verileri Koruma Kurumu (Haziran 2022). Çerez Uygulamaları Hakkında Rehber. Ankara.

Knapp, Maureen. (2013). "Big Data." Journal of Electronic Resources in Medical Libraries, 10(4), 215-222.

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

Kostic, Bojana ve Penagos, Emmanuel Vargas. (2017). The Freely Given Consent and the "Bundling" Provision under the GDPR, Computerrecht, Cilt.4, Sayı.153, 217-222.

Kumar, V. ve Gupta, Shaphali: (2016). "Conceptualizing the Evolution and Future of Advertising." Journal of Advertising, 45(3), 302-317.

Küzeci, Elif. (2020). Kişisel verilerin korunması. (4. Baskı). Îstanbul: On Îki Levha Yayıncılık.

Legge, Adam. (2015). "Online Behavioural Advertising: A Comparative Study of Regulation Between the EU and Hong Kong." Computer Law & Security Review, 31(3), 422-429.

Leibowitz, Jon, (2009). Self-Regulatory Principles for Online Behavioral Advertising. Washington, DC: Federal Trade Commission.

Leon, Pedro Giovanni; Cranshaw, Justin; Cranor, Lorrie Faith; Graves, Jim; Hastak, Manoj; Ur, Blase ve Xu, Guzi (2012). What Do Online Behavioral Advertising Disclosures. Pittsburgh: Carnegie Mellon University.

Lokke, Eirik. (2018). Mahremiyet: Dijital Toplumda Özel Hayat. (Çev. Dilek Başak) istanbul: Koç Üniversitesi Yayınları.

McDonald, Aleecia M. and Cranor, Lorrie. "An Empirical Study of How People Perceive Online Behavioral Advertising (CMU-CyLab-09-015)." (2009). Pittsburgh: Carnegie Mellon University.

McDonald, Aleecia M. ve Cranor, Lorrie. (2010). "Beliefs and Behaviors Internet Users" Understanding of Behavioral Advertising." TPRC 43rd Research Conference on Communication, http://aleecia.com/ authors-drafts/tprc-behav-AV.pdf adresinden alındı.

McStay, Andrew (2011). "Profiling Phorm: An Autopoietic Approach to The Audience-as- Commodity." Surveillance & Society, 8(3), 310-322.

Mendos Kuşkonmaz, Elif. (2013). Kişisel verilerin Türk Ceza Kanunu kapsamında korunması. Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Miri, Mina, Foomany, Farbod H. and Mohammed, Nathanael (2018). Complying with GDPR: An Agile Case Study, ISACA Journal, Cilt.2, 1-7.

Nill, Alexander ve Aalberts, Robert J. (2014). "Legal and Ethical Challenges of Online Behavioral Targeting in Advertising." Journal of Current Issues & Research in Advertising, 35, 126-146.

Oğuz, Sefer. (2018). Kişisel verilerin korunması hukukunun genel ilkeleri. Bilgi Ekonomisi ve Yönetimi Dergisi, 13 (2), 121-138.

Özdem, Berk Hasan (2019). Alman Anayasacılığında insan onuru kavramı. Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2019/1, 241-289.

Özdemir, Hayrunnisa. (2009). Elektronik haberleşme alanında kişisel verilerin özel hukuk hükümlerine göre korunması. Ankara: Seçkin Yayıncılık.

Özel, Kadir Can. (2020). Ana hatlarıyla kişisel verilerin korunmasının tarihsel süreci ile amacı ve kişisel verilerin korunması hakkı. İstanbul Barosu Dergisi, 94 (2), 241255.

Özkan, Oğulcan (2020). Kişisel verilerin korunması. Ankara: Yetkin Yayınları.

Özkök Gökmen, Başak. (2020). Patent hakkının sınırları ve istisnaları (kamu sağlığı gerekçesi özelinde incelenmesi). Yayımlanmamış Doktora Tezi. Ankara: Hacı Bayram Veli Üniversitesi Sosyal Bilimler Enstitüsü.

Patgiri, Ripon ve Ahmed, Arif. (2016). "Big Data: The V"s of the Game Changer Paradigm." 18th International Conference on High Performance Computing and Communications (s. 17-24). Researchgate

Peltekoğlu Balta, Filiz (2010). Kavram ve Kuramlarıyla Reklam. istanbul: Beta Yayıncılık.

Polat, Yeliz. (2011). 4857 sayılı İş Kanunu'na göre işçi özlük dosyası. Yayımlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Politou, Eugenia, Alepis, Efthimios ve Patsakis, Constantinos, (2018). Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions, Journal of Cyber Security, Cilt.4, Sayı.1, 1-20.

Roberts, Marilyn S. ve Ko, Hanjun (2001). "Global Interactive Advertising." Journal of Interactive Advertising, 1(2), 18-27.

Rosch, J. Thomas, (2012). Protecting Consumer Privacy in an Era of Rapid Change. Washington, DC: Federal Trade Commission.

Sanchez, Noain. (2016). Privacy by default' and active 'informed consent' by layers: Essential measures to protect ICT users' privacy, Journal of Information, Communication and Ethics in Society, Cilt. 14, Sayı. 2, 124-138.

Schultz, Don. (2016). "The Future of Advertising or Whatever We're Going to Call It." Journal of Advertising, 45(3), 276-285.

Serozan, Rona. (2018), Medeni hukuk- Genel bölüm/ Kişiler hukuku (8. Bası), İstanbul: Vedat Kitapçılık.

Skouma Georgia ve Leonard Laura. (2015), On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Reforming European Data Protection Law (C. 1-20, C. Privacy and Data Protection, 35-63. Brüksel

Smith, Edith G.; Noort, Guda Van ve Voorveld, Hilde A. (2014). "Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe." Computers in Human Behavior, 32, 15-22.

Sümer, Haluk Hadi (2020). Hukuka giriş- kavramlar & kurumlar. (Güncellenmiş 4. Baskı), Ankara: Seçkin Yayıncılık.

Şeker, Şadi Evren (2015). "Sosyal Ağlarda Veri Madenciliği." YBS Ansiklopedi, 2(2), 30-39.

Şimşek, Oğuz. (2008). Anayasa hukukunda kişisel verilerin korunması. İstanbul: Beta Yayıncılık.

Taştan, Furkan Güven (2017). Türk sözleşme hukukunda kişisel verilerin korunması. (2. Baskı), İstanbul: On İki Levha Yayıncılık.

Taştan, Furkan Güven ve Kaya, Mehmet Bedii (2018). Kişisel Veri Koruma Hukuku Mevzuat & İçtihat, On İki Levha Yayınları, İstanbul.

Tene, Omer, & Polonetsky, Jules (2012). "To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising." Minnesota Journal of Law, Science & Technology, 13(1), 281-357.

Terzi, Ramazan.; Sağıroğlu, Şeref. ve Demirezen, Umut. (2017). Büyük Veri ve Açık Veri: Temel Kavramlar. Şeref Sağıroğlu, Orhan Koç (Ed.), Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar içinde (s. 13-29). Ankara: Grafiker Yayınları.

Tunç, Hasan. (2019). Anayasa hukuku genel esaslar. (2. Baskı), Ankara: Gazi Kitabevi.

Turow, Joseph. (2015). İzleniyoruz: Yeni Reklam Sektöründeki Kimliğimiz ve Değerlerimiz. İstanbul: Hil Yayın.

Uncular Selen. (2014). İş ilişkisinde işçinin kişisel verilerinin korunması. Ankara: Seçkin Yayıncılık.

Uygun, Murat. (2010). Avrupa Birliğinin 95/46 sayılı veri koruma yönergesi ışığında kişisel verilerin korunması. Yayımlanmamış Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Wachter, Sandra. (2018). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR, Computer Law and Security Review, Cilt.34, Sayı.3, 436-449.

Yaman, Fikret (2009). Reklamcılık Sektöründe Reklam Etiği Algılamasının Değerlendirilmesi. Afyon Kocatepe Ünivesitesi Sosyal Bilimler Enstitüsü işletme Anabilim Dalı. Yayınlanmamış Doktora Tezi. Afyonkarahisar

Yılmaz, Recep ve Erdem, Nur. (2016). 150 Soruda Geleneksel ve Dijital Reklamcılık. Kocaeli: Umuttepe Yayınları.

Yılmaz, Sabire Sanem. (2014). Tıp alanında kişisel verilerin hukuka aykırı olarak verilmesinin ceza hukuku açısından değerlendirilmesi (sır saklama yükümlülüğü kapsamında). Yayımlanmamış Yüksek Lisans Tezi. İstanbul: Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü.

Yüksel Civelek, Dilek. (2011). Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi. T.C. Başbakanlık Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi.

Yüzbaşı Topaz, Firdevs. (2021). Uluslararası insan hakları hukukunda ve Türk hukukunda kişisel verilerin korunması. Yayımlanmamış Doktora Tezi. Trabzon: Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü.

Zarsky, Tal, (2017). Incompatible: The GDPR in the Age of Big Data, Seton Hall Law Review, Cilt.47, Sayı 4(2), 995-1020.