

OKTAY KARAALP

İDARENİN KAMU HİZMETİ VE KOLLUK FAALİYETİ KAPSAMINDA VERİ İŞLEMESİ

Bilkent Üniversitesi 2023

İDARENİN KAMU HİZMETİ VE KOLLUK FAALİYETİ KAPSAMINDA VERİ İŞLEMESİ

Yüksek Lisans Tezi

OKTAY KARAALP

Hukuk Bölümü
İhsan Doğramacı Bilkent Üniversitesi
Ankara
Ağustos 2023

İDARENİN KAMU HİZMETİ VE KOLLUK FAALİYETİ KAPSAMINDA
VERİ İŞLEMESİ

İhsan Doğramacı Bilkent Üniversitesi
Ekonomi ve Sosyal Bilimler Enstitüsü

OKTAY KARAALP

Kamu Hukuku Disiplininde Yüksek Lisans Derecesi
Kazanma Yükümlülüklerinin Bir Parçasıdır.

HUKUK BÖLÜMÜ
İHSAN DOĞRAMACI BİLKENT ÜNİVERSİTESİ
ANKARA

Ağustos 2023

İDARENİN KAMU HİZMETİ VE KOLLUK FAALİYETİ KAPSAMINDA
VERİ İŞLEMESİ
Oktay Karaalp

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

.....
Elvin Evrim Dalkılıç
Tez Danışmanı

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

.....
Turgut Tan
Tez Jüri Üyesi

Bu tezi okuduğumu, kapsam ve nitelik bakımından Hukuk Yüksek Lisans derecesi için yeterli bulduğumu beyan ederim.

.....
Eser Us Doğan
Tez Jüri Üyesi

Ekonomi ve Sosyal Bilimler Enstitüsü Müdürü'nün onayı.

.....
Refet S. Gürkaynak
Enstitü Müdürü

ABSTRACT

DATA PROCESSING OF PUBLIC ADMINISTRATION IN THE SCOPE OF PUBLIC SERVICE AND LAW ENFORCEMENT

Karaalp, Oktay

LL.M., Department of Law

Supervisor: Assoc. Prof. Elvin Evrim Dalkılıç

August 2023

Thanks to digitalization and modern technologies, the concept of data processing has developed and the benefit that can be derived from data has reached an incredible level. In this digital world, utilizing data processing technologies has become a necessity for both private and public sector (public administration). However, although data processing has an important role in the scope of public services and law enforcement, there is a risk that data processing may violate individual rights and freedoms. Even though data processing and its's problems have been widely studied in private law, this topic is not sufficiently analyzed from the perspective of administrative law compared to private law in our opinion. In this context, this thesis will examine the data processing carried out by the public administration in the scope of public services and law enforcement as well as the problems that may arise due to these activities.

Keywords: Personal Data, Public Services, Law Enforcement.

ÖZET

İDARENİN KAMU HİZMETİ VE KOLLUK FAALİYETİ KAPSAMINDA

VERİ İŞLEMESİ

Karaalp, Oktay

Yüksek Lisans, Hukuk Bölümü

Tez Danışmanı: Doç. Dr. Elvin Evrim Dalkılıç

Ağustos 2023

Dijitalleşme ve modern teknolojilerle beraber veri işleme uygulamaları da gelişmiş ve veriden sağlanan fayda inanılmaz bir boyuta ulaşmıştır. Bu dijital dünyada faaliyetlerini yerine getirirken veri işleme teknolojilerinden yararlanılması sadece özel sektör için değil, idare için de bir zorunluluk haline gelmiştir. Ancak veri işleme faaliyeti kamu hizmeti ve kamu düzeninin sağlanması açısından önemli bir yere sahip olsa da veri işleme faaliyetlerinin kişi hak ve özgürlüklerini ihlal etme tehlikesi bulunmaktadır. Her ne kadar veri işlenmesi ve bundan dolayı ortaya çıkabilecek problemler özel hukuk boyutuyla geniş çalışma alanı bulsa da kanımızca bu konu idare hukuku perspektifinden, özel hukuka kıyasla, yeterince incelenmemektedir. Bu bağlamda, tezde idarenin kamu hizmeti ve kolluk kapsamında gerçekleştirdiği veri işleme faaliyetleri ile bu faaliyetlerden dolayı ortaya çıkabilecek problemler incelenecektir.

Anahtar Kelimeler: Kişisel Veri, Kamu Hizmeti, Kolluk Faaliyeti.

İÇİNDEKİLER

ABSTRACT	IV
ÖZET.....	IV
İÇİNDEKİLER	V
KISALTMALAR CETVELİ.....	VIII
GİRİŞ	1

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ GENEL BİLGİLER

I. VERİ TÜRLERİ.....	4
A. Veri, Enformasyon ve Bilgi Kavramları.....	4
B. Kişisel Veri	7
1. Genel Olarak Kişisel Veri.....	7
2. Özel Nitelikli Kişisel Veri	12
II. KİŞİSEL VERİ HUKUKUNUN SÜJELERİ.....	14
III. KİŞİSEL VERİLERİN İŞLENMESİ, İŞLEME İLKELERİ VE ŞARTLARI.....	17
A. Kişisel Verilerin İşlenmesi Kavramı	17
B. Kişisel Verilerin İşlenmesinde Temel İlkeler.....	19
C. Kişisel Verilerin İşlenme Şartları.....	24
1. Açık Rıza.....	27
2. Kanunlarda Açıkça Öngörülmesi	32
3. Meşru Menfaat	34
IV. İLGİLİ KİŞİNİN HAKLARI VE İDAREYE BAŞVURU	37
V. KVKK İSTİSNA HÜKÜMLERİ.....	43

İKİNCİ BÖLÜM

KAMU HİZMETİ KAPSAMINDA VERİ İŞLENMESİ

I. KAMU HİZMETİ	45
A. Kamu Hizmeti Kavramı ve Unsurları	45

1. Kamu Hizmeti Kavramı	45
2. Kamu Hizmetinin Unsurları	47
B. Kamu Hizmetinin Genel İlkeleri	50
II. İDARENİN VERİ İŞLEME UYGULAMALARI	52
A. Genel Olarak İdarenin Veri Kullanımı ve Büyük Veri	52
B. E-Devlet.....	57
1. Tanım ve E-Devletin Gelişimi.....	57
2. E-Devletin Faydaları ve Riskleri.....	63
3. Kamu İnternet Sitelerinde Çerez Uygulaması:	74
3.a Çerez Kavramı ve Türleri.....	75
3.b Veri Koruma Hukuku ve E-Devlet Bağlamında Çerezler	77
III. KAMU SEKTÖRÜNDE AÇIK VERİ VE VERİNİN YENİDEN KULLANIMI (<i>DATA REUSE</i>)	85
A. Açık Veri (<i>Open Data</i>) ve Kamusal Veri (<i>Public Data</i>) Kavramları:	86
B. Açık Verinin Faydaları ve Açık Veriden Değer Yaratma	88
1. Şeffaflık.....	92
2. Kamu Hizmetlerinin İyileştirilmesi.....	95
3. Ekonomik Değer ve Verimlilik	98
C. Açık Verinin Kişi Haklarıyla İlişkisi	100

ÜÇÜNCÜ BÖLÜM

İDARİ KOLLUK KAPSAMINDA VERİ İŞLENMESİ

I. İDARİ KOLLUK	108
A. Kolluk ve Kamu Düzeni Kavramı.....	108
B. Kolluk Türleri.....	111
II. KOLLUK FAALİYETLERİ KAPSAMINDA VERİ İŞLEME UYGULAMALARI	113
A. Genel Çerçeve	113
B. AB 2016/680 sayılı Kolluk Direktifi	119
1. Amaç ve Kapsam.....	119
2. LED'in GDPR ile Farkları	121
C. Öngörücü Kolluk Faaliyetleri.....	123

1. Tanım.....	123
2. Öngörücü Kolluğun Faydaları ve Riskleri	127
3. Öngörücü Kolluk Bağlamında Kolluk Direktifi ve Yapay Zeka Yasası...	132
III. İDARENİN ÖZEL SEKTÖRDEKİ KİŞİSEL VERİLERE ERIŞİMİ	134
A. Genel Olarak	134
B. Özel Sektörün Kişisel Verileri İstem Dışı Paylaşması	136
1. Mecburi Paylaşım: Hukuki Düzenlemeler ve Avrupa-Türk İçtihat Hukuku	136
2. Doğrudan Erişim: Hukuki Düzenlemeler ve Zakharov kararı	145
C. Özel Sektörün Kişisel Verileri Gönüllü Paylaşması	148
1. Genel Olarak Gönüllü Paylaşım	148
2. Gönüllü Paylaşım Yolu Olarak Satış: Hukuki Düzenlemeler	150
C. Özel Sektördeki Kişisel Verilere Erişimin Uluslararası Ekonomiye Etkisi ve Genel İlkeler.....	155
SONUÇ.....	161
KAYNAKÇA.....	168

KISALTMALAR CETVELİ

108 sayılı Sözleşme : 28.01.1981 tarih ve 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

ABD : Amerika Birleşik Devletleri

Açık Veri Direktifi : Açık veri ve kamu sektörü bilgilerinin yeniden kullanımına ilişkin 20 Haziran 2019 tarihli ve 2019/1024 sayılı Avrupa Parlamentosu ve Konsey Direktifi

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

BEHK : 4982 sayılı Bilgi Edinme Hakkı Kanunu

BİT : Bilgi İletişim Teknolojileri

Bkz. : Bakınız

C. : Cilt

CNIL : Fransa Veri Koruma Otoritesi

DGA : AB Veri Yönetişim Yasası

ed. : Editör

EDPB : Avrupa Veri Koruma Kurulu

E-Gizlilik Direktifi: : Elektronik iletişim sektöründe kişisel verilerin işlenmesi ve mahremiyetin korunmasına ilişkin 12 Temmuz 2002 tarihli ve 2002/58/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi

FRA : Avrupa Birliği Temel Haklar Ajansı

GDPR : Kişisel verilerin işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımına ilişkin ve 95/46/EC sayılı Direktifi yürürlükten kaldıran 27 Nisan 2016 tarihli ve 2016/679 (AB) sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü)

ICC : Milletlerarası Ticaret Odası

ICE : ABD Göçmenlik ve Gümrük Muhafaza

ICO : Birleşik Krallık Bilgi Komiserliği Ofisi

iç. : İçinde

İYUK : 2577 sayılı İdari Yargılama Usulü Kanunu

Kurul : Kişisel Verileri Koruma Kurulu

Kurum : Kişisel Verileri Koruma Kurumu

KVKK : Kişisel Verileri Koruma Kanunu

LED : Kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımına dair 27

Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve
Konsey Direktifi (Kolluk Direktifi)

MİT : Milli İstihbarat Teşkilatı

OECD : Ekonomik İşbirliği ve Kalkınma Örgütü

Örn. : Örneğin

RG : Resmi Gazete

s. : Sayfa

S. : Sayı

T. : Tarih

GİRİŞ

Teknolojik gelişmelerle beraber dünyamız fiziksel ortamdan dijital ortama doğru bir geçiş yaşamaya başlamış ve dijitalleşmenin ön planda olduğu bu sistemde küresel ölçekte var olan veri miktarı katlanarak artmış, mevcut veri miktarı muazzam bir seviyeye ulaşmıştır. Veri akışının sürekli olduğu bu çağda verileri doğru analiz edebilme ve kullanma kabiliyeti piyasa aktörleri açısından varlığı zorunlu bir yetenek olarak değerlendirilmektedir. Zira veri analizi yardımıyla daha kaliteli hizmet ve ürünler sunulabilmektedir.

Bu kapsamda idari faaliyetleri yerine getirirken veri işlemek idare açısından da kaçınılmaz bir durum haline gelmiştir. İdarenin kamu yararını gözeterek doğru kararlar alması ve eylemlerde bulunması, doğru zamanda doğru bilgilere sahip olmasına bağlıdır. Doğru bilgilere ise veri analizi sayesinde ulaşılmakta ve bu sayede idarenin kamu yararı için en iyi kararları alma kabiliyeti artmaktadır.

Veri işleme uygulamaları özel hukuk bakımından çok çalışılmış bir konu olsa da kanaatimizce idare hukuku perspektifinden özel hukukta olduğu kadar çalışma alanı bulmamıştır. Esasen idare her gün gerçekleştirdiği eylem ve işlemleri ile çok büyük miktarda kişisel ve kişisel olmayan veri işlemektedir. Veri işleme faaliyetinin kişi hak ve menfaatlerini ihlal edebileceği göz önüne alındığında idarenin veri işleme faaliyetlerini nasıl gerçekleştirdiği ve ne gibi sorunların ortaya çıkabileceğinin ele alınması önemlidir. Bu bağlamda, kanımızca idari faaliyetler kapsamında veri işlenmesi ile ilgili önemli ancak idare hukuku doktrininde yeterince yer etmemiş kavramların da ele alınmasında yarar vardır.

Bu amaçla tezin birinci bölümünde, veri işleme faaliyetinin ve hukuki temellerinin anlaşılabilmesi ve ileriki bölümlerde kavram karmaşasına sebep olmamak için, kişisel verilerin korunmasına ilişkin temel bilgiler kısaca verilecektir. Bu kapsamda, öncelikle veri kavramına açıklık getirilecek, sonrasında unsurlarıyla beraber kişisel veri türleri anlatılacaktır. Ardından, kişisel veri hukukunun sınırlarına değinilerek; kişisel verilerin işlenmesi kavramı, kişisel verilerin işlenmesine hakim olan ilkeler ve kişisel verileri işleme şartları ortaya konulacaktır. Son olarak da kişisel verisi işlenen ilgili kişilerin sahip olduğu haklar ve bu hakları veri sorumlusu olan idareye karşı nasıl ileri sürebileceği değerlendirilerek, Kişisel Verileri Koruma Kanunu (KVKK) kapsamı dışında kalan veri işleme hallerine değinilecektir. Bu bölümde kişisel verilerin korunmasıyla ilgili genel kavramlar uygun düştüğü ölçüde idare hukuku ile ilişkilendirilecektir.

Çalışmanın ikinci bölümünde ise, kamu hizmeti kapsamında veri işleme uygulamaları ele alınacaktır. Bu doğrultuda, öncelikle kamu hizmeti kavramı kısaca açıklanacaktır. Devamında, genel olarak idarenin kamu hizmeti kapsamında veri işleme uygulamaları anlatılıp idarenin dijitalleşmesinin en somut örneği olan e-devlet uygulaması incelenecektir. Bu kapsamda, e-devletin genel problemleri açıklanıp, kişisel verilerin korunması noktasında e-devletin taşıdığı riskler ayrıntılı şekilde incelenecek ve bu riskler çerçevesinde doğabilecek idari sorumluluk anlatılacaktır. Daha sonra çerez kavramı ve e-devletin bir uzantısı olan kamu sitelerinde çerez kullanımı kişisel veri hukuku kapsamında değerlendirilecektir. Bölümün son kısmında ise, kamu sektöründe açık veri ve verinin yeniden kullanımı kavramları üzerinde durulacaktır. Açık verinin idareye sağlayabileceği faydalar açıklandıktan sonra açık

verinin kiři haklarıyla iliřkisi irdelenip, idarenin bireylerin haklarını ihlal etmeden açık veriyi nasıl kullanması gerektiğine değinilecektir.

Üçüncü ve son bölüm ise idari kolluk faaliyetleri kapsamında veri işleme uygulamalarına ayrılmıştır. Bu uygulamaların anlaşılabilmesi adına, genel olarak kolluk kavramı ve kolluğun bir türü olan idari kolluğun ne anlama geldiği açıklanacaktır. İdarenin kolluk faaliyetleri kapsamında veri işleminin genel çerçevesi çizildikten sonra Türkiye'ye örnek olabilecek, Avrupa Birliğinde kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi bakımından genel düzenleme olan Kolluk Direktifinin ayrıntıları ele alınacaktır. Devamında, veri analizi yardımıyla idari kolluk faaliyeti yerine getirmek olarak tanımlayabileceğimiz, gelişen teknolojilerle beraber uygulamada yer almaya başlayan öngörücü kolluk faaliyeti fayda ve riskleriyle ortaya konulacak ve Kolluk Direktifi ile Yapay Zeka Yasası¹ kapsamında değerlendirilecektir. Son olarak, idarenin kolluk amacıyla özel sektördeki kişisel verilere erişim yollarının neler olduğu belirtilip, uluslararası kuruluşların bu erişimin sınırlarını belirlemek için geliřtirdiğı ilkeler üzerinde durulacaktır.

¹ Yapay Zeka Yasası esasen şekli anlamda bir kanun değildir. AB hukukunda ikincil mevzuat arasında yer alan bir tüzüktür (regulation).

BİRİNCİ BÖLÜM

KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ GENEL BİLGİLER

I. Veri Türleri

A. Veri, Enformasyon ve Bilgi Kavramları

Veri türlerine ilişkin tanımlama verilmeden evvel, veri (*data*), enformasyon (*information*) ve bilgi (*knowledge*) kavramlarının açıklanması gerekmektedir. Aralarında yakın bağlantı bulunan ve hatta kimi zaman yanlış olarak birbirlerinin yerine kullanılan bu kavramlar arasında anlamsal olarak farklılıklar bulunmaktadır². Aralarındaki bu ilişki dolayısıyla bilimsel çalışmalarda bu üç terim beraber açıklanma ve değerlendirilme eğilimindedir³.

Veri, enformasyon ve bilgi kavramlarının, genel kabul görmüş bir tanımı bulunmamakla beraber⁴, bu kavramlar arasında bir hiyerarşi bulunmaktadır. Enformasyon genellikle verilerin zenginleştirilmesi ve kullanılması yoluyla

² Küzeci, E.: Kişisel Verilerin Korunması, 4. Baskı, Ankara 2021, s. 10; Yılmaz, M.: *Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi*, Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 2009, C. XLIX, S. 1, s. 97-98.

³ Yılmaz, s. 98.

⁴ European Commission: Communication to the Commission-Data, Information and Knowledge Management at the European Commission, 2016, C (2016) 6626 Final, s. 2. ([https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2016\)6626&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2016)6626&lang=en), Erişim Tarihi: 22.06.2023).

üretilirken, bilgi ise enformasyonun özümsemesi yoluyla ortaya çıkmaktadır⁵. Başka bir ifadeyle, veri, enformasyonun; enformasyon ise bilginin hammaddesidir⁶.

Doktrindeki çalışmalar incelendiğinde, verinin genel olarak, kendi başına anlam ifade etmeyen bir dizi sayı veya sembol olarak tanımlandığı görülmektedir⁷. Kavramsal bir bakış açısıyla, veri, enformasyonun ve ardından bilginin türetildiği en düşük soyutlama düzeyi olarak kabul edilmektedir⁸. Avrupa Komisyonu, veriyi, bilgi üretmek için işlenmesi gereken somut nesnel gerçekler, ölçümler veya gözlemler olarak tanımlamıştır⁹. Yılmaz ise, doktrindeki farklı tanımlamaları göz önünde bulundurarak veriyi şu şekilde tanımlamaktadır: “*Veri tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgi(dir). Veriler; belli ve programlı ilişkiler çerçevesinde bir araya getirildiğinde anlam kazanarak enformasyona dönüşürler*”¹⁰. Kamusal bağlamda ise, ham kamusal veri, örneğin, baz istasyonlarından ve uydu gözlemlerinden toplanan temel meteorolojik verileri, uydu gözlemlerinden toplanan kartografik verileri, doğrudan halktan, işletmelerden ve diğer kuruluşlardan toplanan hükümet istatistikleri gibi verileri ifade etmektedir¹¹.

⁵ OECD: *Fostering Innovation in the Public Sector*, Paris 2017, s. 198 (<https://www.oecd.org/gov/fostering-innovation-in-the-public-sector-9789264270879-en.htm>, Erişim Tarihi: 20.06.2023).

⁶ Küzeci, s. 11; Zins, C.: *Conceptual Approaches for Defining Data, Information, and Knowledge*, Journal Of The American Society for Information Science and Technology 2007, C. LVIII, S. 4, s. 479.

⁷ Liew, A.: *DIKW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships*, Business Management Dynamics 2013, C. II, S. 10, s. 49-62; Küzeci, s. 11; Zins, s. 480.

⁸ OECD: *Data-Driven Innovation: Big Data for Growth and Well-Being*, Paris 2015, s. 449. (<https://doi.org/10.1787/9789264229358-en>, Erişim Tarihi: 20.06.2023).

⁹ European Commission, s. 2.

¹⁰ Yılmaz, s. 98.

¹¹ OECD: *Assessing Government Initiatives on Public Sector Information: A Review of the OECD Council Recommendation*, OECD Digital Economy Papers 2015, No. 248, s. 10 (<https://doi.org/10.1787/5js04dr9l47j-en>, Erişim Tarihi: 20.06.2023).

Verilerin bir bağlam çerçevesinde incelenmesi, analiz ve kategorize edilmesi sonucunda ise, ortaya enformasyon çıkmaktadır. Başka bir deyişle, enformasyon anlam kazandırılmış veri olarak tanımlanabilmektedir¹². Verileri işlenmemiş cevherlere benzeten *Ackoff*'a göre, veriler kullanılabilir formlara dönüştürülene kadar ya hiç değer taşımamakta ya da çok az değer taşımaktadır. İşlenerek faydalı bir formata dönüştürülen veri ise enformasyonu oluşturmaktadır. Bu bağlamda, veri ve enformasyon arasındaki fark onların işlevselliklerinden kaynaklanmaktadır. Enformasyon; kim, nerede, ne zaman, kaç gibi sorulara yanıt verebilecek şekilde işlenen verilerdir¹³.

Bilginin ne olduğu konusunda ise doktrinde farklı görüşlere rastlamak mümkündür. Zira, bilginin ne olduğu sorusu tarih boyunca felsefi tartışmalara konu olduğu gibi¹⁴ bilgi teknolojileri bağlamında da tartışılmıştır¹⁵. Ekonomik İş Birliği ve Kalkınma Örgütü (OECD) bilgiyi genellikle “öğrenme” olarak adlandırılan bir süreç aracılığıyla içselleştirilen veya özümseyen enformasyon ve deneyim olarak tanımlamaktadır¹⁶. Bu bağlamda, bilgi uzman görüşü ve deneyimi ile enformasyon ve verinin bir araya getirilmesiyle elde edilen ve karar vermeye yardımcı olan bir kaynaktır¹⁷. *Ackoff*'a göre “nasıl yapılır?” sorusuna verilen cevaplar bilgiyi oluşturmaktadır. Bilgi, örneğin bir sistemin nasıl çalıştığını veya istenen şekilde nasıl çalıştırılacağını bilmek gibi *know-how*'dan oluşur. Bilgi, nesnelerin, sistemlerin ve olayların bakımını ve kontrolünü mümkün kılar¹⁸.

¹² European Commission, s. 2; Yılmaz, s. 98.

¹³ Ackoff, R. L.: *On Learning and the Systems That Facilitate It*, Reflections 1999, C. I, S. 1, s. 15.

¹⁴ Yılmaz, s. 99.

¹⁵ Farklı tanımları bir arada görebilmek için bkz. Zins, s. 480-487.

¹⁶ OECD (Data-Driven Innovation: Big Data for Growth and Well-Being), s. 449.

¹⁷ European Commission, s. 2.

¹⁸ Ackoff, s. 15.

Bu terimler arasındaki önemli farklılıklar bulunduğu açık olmakla beraber, *Küzeci* veri koruma hukuku bakımından, hukuksal tartışmalarda ve yasal düzenlemelerde bu terimler arasında ayrım yapmayı yapay ve gereksiz görmektedir. Uygulamada ise, bu terimler arasında ayrım yapabilmek bir hayli zor olduğu gibi, terimlerin karmaşıklığı ve belirsizliğinin neden olduğu tanım bolluğu nedeniyle yasal düzenlemelerde yapılacak ayrımlar istenmeyen sonuçlar doğurabilecektir¹⁹. *Küzeci*'nin bu görüşünün kişisel veri hukuku bakımından doktrinde kabul gördüğünü söylemek yanlış olmayacaktır. Zira, kişisel verilerin korunması ile ilgili kitaplar ve diğer akademik çalışmalar incelendiğinde birçok çalışmada veri, enformasyon ve bilgi terimlerinin açıklanmadığı ve bu terimlerin birbirinin yerine geçecek şekilde kullanıldığı görülmektedir. Bu kapsamda, örneğin, kişisel verilerle ilgili yapılan çevirilerde enformasyon olarak belirttiğimiz “*information*” sözcüğü bilgi olarak çevrilmektedir.

B. Kişisel Veri

1. Genel Olarak Kişisel Veri

Kişisel veri, birçok ulusal ve uluslararası metinde kimliği belirli veya belirlenebilir bir kişiye ait tüm veriler olarak tanımlanmaktadır. Bu bağlamda, kişisel

¹⁹ Küzeci, s. 13-14.

veri, örneğin; bir kimsenin şahsiyetine, ailesine, mesleki hayatına, etnik kökenine veya öğrenim durumuna ilişkin, o bireyi diğerlerinden ayırmaya elverişli olabilecek her türlü bilgiyi ifade etmektedir²⁰. Bunun yanında, kişisel veri, dijital ortamlarda bulunabileceği gibi fiziki ve basılı ortamlarda da bulunabilmektedir. Bu cümleden olarak, verinin bulunduğu ortamın kişisel veri kavramı yönünden bir önemi bulunmamaktadır²¹.

OECD tarafından 1980 yılında yayınlanan ve kişisel verilerin tanımlandığı ilk uluslararası belge olan “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri”nde kişisel veri “*tanımlanmış veya tanımlanabilir bir bireyle (veri sahibi) ilgili her türlü bilgi (information)*” olarak ifade edilmektedir. Bu belgenin yayınlanmasından yaklaşık bir yıl sonra ise Avrupa Konseyi tarafından, Türkiye’nin de imzalamış olduğu 28.01.1981 tarih ve 108 sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme (108 sayılı Sözleşme)” yayınlanmış ve kişisel veri, OECD Rehber ilkeleriyle paralel olarak “*kimliği belirli veya belirlenebilir bir kişi hakkındaki tüm bilgiler*” olarak tanımlanmıştır²².

Avrupa Birliği’nde (AB) kişisel verinin korunmasına ilişkin mülga düzenleme olan 1995/46/EC sayılı Direktifte kişisel veri şu şekilde tanımlanmıştır: “*Kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye (“veri sahibi”) ilişkin her türlü bilgi anlamına gelir; tanımlanabilir kişi, özellikle bir kimlik numarasına veya fiziksel,*

²⁰ Aşkoğlu, Ş. İ.: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul 2018, s. 5; Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanun’da Yer Alan Temel Kavramlar, s. 13 (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf>, Erişim Tarihi: 17.06.2023).

²¹ Turan, M.: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 4. Baskı, Ankara 2017, s. 58.

²² Sözleşme Türkiye tarafından 08.01.1981 tarihinde imzalanmış ancak 2016 yılına kadar onaylanmamıştır.

fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen kişidir”²³.

2016 yılında kabul edilip, 2018’de yürürlüğe giren ve ilgili Direktifin yerine geçen AB Genel Veri Koruma Tüzüğü’nde (GDPR) ise, kişisel veri, önceki düzenlemelere benzer bir şekilde tanımlanmış olmakla beraber, teknolojik gelişmelere uyum açısından tanımlanabilir kişiye ilişkin örnekler çeşitlendirilerek konum verileri ve çevrimiçi tanımlayıcıları eklenmiştir²⁴.

Ulusal mevzuatımızda ise kişisel veri kavramı, ilk olarak 2004 yılında 5237 sayılı Türk Ceza Kanunu’nda (TCK) kullanılmış olmakla beraber, kişisel verinin bir tanımı yapılmamıştır. Kanunun gerekçesinde kişisel veri “*gerçek kişiyle ilgili her türlü bilgi*” olarak tanımlanmıştır. Ancak, gerekçe bağlayıcı olmadığı için ilgili düzenleme, ceza hukuku doktrininde kanunilik ve belirlilik ilkeleri bakımından eleştirilmiştir²⁵. TCK’dan sonra, 2010 yılında yapılan değişiklikle kişisel veri kavramı Anayasamıza girmiş olmakla beraber Anayasa’da da herhangi bir tanımlama yapılmamış, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Bu kapsamda, 07.04.2016 tarihinde kişisel verilerin korunmasına ilişkin genel düzenleme olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)²⁶ yürürlüğe girmiştir. KVKK, uluslararası düzenlemelere paralel olarak kişisel veriyi “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlamaktadır²⁷.

²³ Bkz. Direktif 95/46/EC, Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması hakkında 95/46/EC sayılı Direktif, m. 2/1-a (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>, Erişim Tarihi: 17.06.2023).

²⁴ Bkz. GDPR, m.4/1 (<https://eur-lex.europa.eu/eli/reg/2016/679/oj>, Erişim Tarihi: 17.06.2023).

²⁵ Oğuz, S.: *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*, Bilgi Ekonomisi ve Yönetimi Dergisi 2018, C. XIII, S. 2, s. 124-125.

²⁶ RG; T. 07.04.2016, S. 29677.

²⁷ KVKK m.3/1-d.

Bu tanımlamalar ışığında kişisel veri kavramı; “bilgi” ve “kimliği belirli veya belirlenebilir kişi” kavramlarından oluşmaktadır. Bilgi unsuru yukarıda açıklanmış olup, ayrıca kişi unsuruna da değinilmesi gerekmektedir. Bu kapsamda, kişi kavramının sadece gerçek kişileri mi ifade ettiği yoksa tüzel kişileri de mi kapsadığı hususunda doktrinde tartışmalar bulunmaktadır²⁸. GDPR’daki tanımda kişisel verinin gerçek kişilere ilişkin olduğu açık bir şekilde belirtilmiş olmakla beraber, kişi unsurunun sınırlarını belirleme üye ülkelerin takdir yetkisine bırakılmıştır²⁹. Zira, Avrupa Birliği Adalet Divanı (ABAD), 2001 tarihli bir kararında, üye devletlerin ulusal mevzuatlarına Direktif (95/46/EC) kapsamına girmeyen alanları da ekleyebileceğini açık bir şekilde belirtmiştir³⁰. Bu bağlamda, İsviçre gibi bazı ülkeler kişisel veri koruma mevzuatları kapsamına tüzel kişileri de alsa da³¹ uluslararası genel eğilim sadece gerçek kişilerin koruma kapsamına alınması yönündedir³².

Ülkemizde de KVKK kapsamında sadece gerçek kişilerin korunduğu açık bir şekilde belirtilmiştir. Zira, KVKK m.1’de belirtildiği üzere KVKK’nın amacı özel hayatın gizliliği başta olmak üzere kişilerin temel hak ve özgürlüklerini korumaktır. Bununla beraber, Anayasa Mahkemesi (AYM) Posta Hizmetleri Kanunu’ndaki ticari amaçla oluşturulan veri tabanında gerçek kişilerden rıza alınması ve fakat tüzel kişiler bakımından ise böyle bir rıza alınmaması yönündeki düzenlemeyi eşitlik ve ilkesine

²⁸ Aşıkoglu, s. 14.

²⁹ Ayözger Öngün, Ç.: Kişisel Verilerin Korunması Hukuku, 2. Baskı, Ankara 2019, s.10.

³⁰ ABAD, C-101/2001, 06.11.2003, Bodil Lindqvist, (<https://curia.europa.eu/juris/liste.jsf?num=C-101/01>, Erişim Tarihi: 07.07.2023)

³¹ İsviçre’nin ilgili çalışmanın yapıldığı sırada yürürlükte olan veri koruma mevzuatı tüzel kişileri de kapsamına rağmen 01.09.2023 tarihinde yürürlüğe girecek olan yeni veri koruma yasası kapsamında sadece gerçek kişiler düzenleme kapsamına alınmıştır.

³² Çekin, M. S.: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul 2020, s. 25.

aykırı bulmuştur³³. Bu bağlamda, sektörel bakımdan bazı durumlarda tüzel kişilerin verileri de kişisel veri gibi korunabilmelidir³⁴. Belirtmek gerekir ki, tüzel kişilerin verilerinin kişisel veri olarak kabul edilmemesi, bu verilerin hiçbir şekilde korunmadığı anlamına gelmemektedir. Tüzel kişilere ait veriler de devlet sırrı veya ticari sır kapsamında korumaya tabi olabilmektedir.³⁵

Kişisel veri tanımında, verinin belirli veya belirlenebilir bir kişiye ait olması şartı aranmıştır. Genel anlamda, bir gerçek kişi, bir grup kişi içinde, grubun diğer tüm üyelerinden ayırt edildiği zaman belirli olarak kabul edilebilir³⁶. Bu bağlamda, kişinin kimliğini başka hiçbir işlem gerekmeksizin ortaya çıkaran bilgiler belirli bir kişiye ait kabul edilmektedir. Örneğin, bir kişinin kimlik numarası o kişiyi doğrudan tespit edebilmeyi sağladığından belirli kişiye ait veridir³⁷. Buna karşın, belirlenebilirlikten söz edebilmek için bir verinin kişiyi tespit etmeye tek başına elverişli olmaması, ancak, mevcut verinin başka verilerle birleştirilerek kişinin tespitinin mümkün olması gerekmektedir. Başka verilerden kast edilen ise, GDPR’ın giriş bölümünün 26.

³³ AYM’ye göre “(...) Posta ve kargo taşımacılığı sektöründe faaliyet gösteren özel hukuk tüzel kişisi ticari işletme PTT A.Ş. ile aynı sektörde faaliyet gösteren diğer özel hukuk tüzel kişisi ticari işletmeler arasında sermayeye sahiplik dışında hukuken hiçbir fark bulunmadığı halde, PTT A.Ş.’ye ayrıcalık tanınmasının Anayasal eşitlik ilkesine aykırılığı bir yana; gerçek kişilerin fiziki ve elektronik adreslerinin reklam ve tanıtım amacıyla kullanılmasında rızaları aranırken, tüzel kişilerin rızalarının aranmaması, gerçek kişi ticari işletmelerde rıza aranırken, tüzel kişi ticari işletmelerde rıza aranmaması ve böylece fiziki ve elektronik adreslerin reklam ve tanıtım amacıyla kullanılmasında kişisel nitelikleri ve durumları özdeş olanlar için yasayla değişik kurallar konulması, Anayasanın 10 uncu maddesindeki eşitlik ilkesine aykırılık oluşturur. Anayasal eşitlik ilkesinin çiğnenmemesi için gerçek kişiler yanında tüzel kişilerin de rızalarının aranması, tüzel kişilerin yetkili organından izin alınması, Anayasal bir zorunluluktur. Maddede geçen “gerçek” ifadesinin iptali halinde bu zorunluluk yasal hale gelecektir.” Bkz. AYM Genel Kurul, E. 2013/84-K- 2014/183, R.G.: 13.03.2015, sayı: 29294.

³⁴ Ayözger Öngün, s. 10.

³⁵ Küzeci, s. 6.

³⁶ Bkz. Article 29 Data Protection Working Party, Opinion 4/2007 on The Concept Of Personal Data, 01248/07/ENWP 136, s. 12. (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, Erişim Tarihi: 15.06.2023).

³⁷ Ayözger Öngün, s. 11.

paragrafında belirtildiği üzere; veri sorumlusunun menfaatleri ışığında elde edilmesi makul ve ölçülü olan verilerdir³⁸.

AYM'nin yerleşik içtihatlarında belirttiği üzere³⁹ “(kişinin) adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler” kişisel veri niteliği taşımaktadır.

2. Özel Nitelikli Kişisel Veri

Ulusal ve uluslararası düzenlemelerde bazı kişisel verilerin “hassas veri”, “özel koruma gerektiren veri”, “özel tür veri”, “özel nitelikli veri” gibi isimlerle tanımlandığı görülmektedir. Bu verilerin ayrı şekilde düzenlenmesinin nedeni, özel nitelikli kişisel verilerin daha hassas olması nedeniyle özel korumaya sahip olması gerektiği düşüncesidir. Zira, bu verilerin kullanılması bireylerin temel hak ve özgürlükleri açısından önemli riskler taşımakta, özellikle de bireyleri ayrımcılığa maruz bırakma olasılığı bulunmaktadır⁴⁰. Hem GDPR’da hem de KVKK’da özel nitelikli kişisel

³⁸ Çekin, s. 46.

³⁹ AYM, T. 09.04.2014, E. 2013/122, K. 2014/74, R.G.: 26.7.2014, S. 29072; AYM, T. 12.11.2015, E. 2015/32, K. 2015/102, R.G.: 02.12.2015, S. 29550; AYM, T. 1.6.2022, E. 2022/33, K. 2022/67, R.G.: 22/7/2022, S. 31900

⁴⁰ Information Commissioner's Office (ICO), *What is Special Category Data?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/>), Erişim Tarihi: 15.06.2023).

verilerin bir tanımı yapılmamış olmakla beraber, hangi verilerin kişisel veri olduğu belirtilmiştir.

GDPR’a göre; ırk, etnik köken, siyasi görüş, dini veya felsefi inançlar, sendika üyeliği, genetik ve biyometrik bilgiler, sağlık ile ilgili veriler veya cinsel yönelime ilişkin veriler özel nitelikli kişisel veri niteliği taşımaktadır⁴¹. Buna karşın, yukarıda belirtildiği üzere, üye devletlerin GDPR’da düzenlenen asgari şartları daha kapsamlı bir şekilde hukuk sistemlerine entegre etmeleri önünde bir engel bulunmamaktadır⁴².

KVKK’da ise özel nitelikli kişisel veri; *Kişilerin 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 olarak sayılmıştır*⁴³. Görüleceği üzere, KVKK, GDPR’da bulunmayan dernek ve vakıf üyeliği, kılık kıyafet, ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili verileri özel nitelikli kişisel veri kategorisinde kabul etmiştir.

*Dülger’in belirttiği üzere “özellikle kişinin ırkına veya etnik kökenine ilişkin verilerin diğer kişisel verilerden ayrı bir düzenlemeye tabi tutulmasının nedeni, söz konusu kişilerin verilerinin devlet kurumları tarafından kötüye kullanılması endişesidir. Bu kaygının sebebi özellikle nüfus kayıtlarının ayrıntılı tutulması sonrası gerçekleşen Yahudi soykırımı gibi tarihsel olayların yaşanmış olmasıdır”*⁴⁴.

⁴¹ Bkz. GDPR m. 9.

⁴² Aksoy, H. C.: Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Ankara 2010, s. 30-31.

⁴³ Bkz. KVKK m. 6.

⁴⁴ Dülger, M. V.: *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 2016, C. III, S. 2, s. 109.

II. Kişisel Veri Hukukunun Søjeleri

Kişisel verilerin korunması ile ilgili ulusal ve uluslararası düzenlemeler incelendiğinde, veri koruma hukukunun søjelerinin; veri sorumlusu, veri işleyen ve ilgili kişi olduğu görölmektedir. Bu kavramların tanımlanmasına, “*veri koruması mevzuatına uymakla yükümlü olanı belirlemek, kişisel veri hukukuna uyum için organizasyon yükümlölüğünü tespit etmek, ilgili kişilerin haklarını kime karşı ileri sürebileceğini ve taleplerinin muhatabını tespit etmek gibi nedenlerle*”⁴⁵ ihtiyaç duyulmaktadır.

Kişisel veri koruma mevzuatının temel konusunu oluşturan ve verinin nitelediğı kişi, GDPR’da veri sűjesi/sahibi, KVKK’da ise ilgili kişi olarak adlandırılmaktadır. Başka bir deyişle, “ilgili kişi”, verisi işlenen kişiyi ifade etmektedir. KVKK’da ilgili kişi, kişisel verisi işlenen gerçek kişi olarak tanımlanmaktadır⁴⁶. Yukarıda gerçek kişinin özellikleriyle ilgili yapılan açıklamalar ilgili kişinin özelliklerini belirttiğinden burada tekrarlanmayacaktır.

Veri işleme sürecine dahil olan ve kişisel verileri koruma hukukunda merkezi bir konuma sahip olan bir diğerk aktör ise, veri sorumlusudur. GDPR’da veri sorumlusu (*controller*); “*yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu*

⁴⁵ Ersoy Kekevi, Ç.: *Genel Kavramlar*, iç. Kişisel Verilerin Korunmasına Akademik Bakış - KVKK Akademi Derleme Çalışması (ed. Aksoy, Pınar Çağlayan/ Aksoy, Hüseyin Can), Ankara 2023, s. 114.

⁴⁶ Bkz. KVKK m. 3/1-ç.

veya diğer herhangi bir organ”⁴⁷ olarak tanımlanmıştır. KVKK’daki tanıma göre ise veri sorumlusu, “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*” ifade etmektedir⁴⁸. Tanımlarda bahsedilen amaç, verilerin neden işlendiğinin, araç ise nasıl işlendiğinin cevabını oluşturmaktadır⁴⁹.

Veri sorumlusu, bir bütün olarak, baştan sonra veri işleme faaliyetinin hukuka uygunluğunu sağlamakla yükümlüdür. Başka bir anlatımla, veri sorumlusunun mevzuattaki yükümlülükleri yerine getirebilmesi adına münferit işleme faaliyetlerine dair yasal dayanak sunması yeterli olmamakta, verilerin hukuka uygun işlenebilmesi için gerekli organizasyonu sağlayarak teknik ve idari tedbirleri de alması gerekmektedir⁵⁰.

GDPR’den farklı olarak ulusal mevzuatımızda, veri sorumlusu kavramına kamu kurumları açık bir şekilde dahil edilmemiştir. Ancak, mevzuattaki tüzel kişi ifadesi kamu tüzel kişiliğine de işaret etmektedir. Nitekim, KVKK bir bütün olarak incelendiğinde kamu tüzel kişilerinin de veri sorumlusu olabildiği anlaşılmaktadır⁵¹. Ne var ki, Çekin’in belirttiği üzere, Kanun’da veri sorumlusu tanımlanırken sadece gerçek veya tüzel kişiden bahsedilmesi, kamu tüzel kişilikleri açısından birtakım sorunlar doğurmaktadır. Kamu kurum ve kuruluşlarının tamamı ayrı tüzel kişiliğe sahip olmadıklarından, KVKK’daki tanım uyarınca bunlar veri sorumlusu olamayacaktır. Bu bağlamda, merkezden yönetim içindeki tüm kurum ve kuruluşlar

⁴⁷ GDPR, m.4/7.

⁴⁸ Bkz. KVKK m. 3/1-ı.

⁴⁹ Çekin, s. 54.

⁵⁰ Çekin, M. S./ Berktaş, A. S./ Akıncı, M. F.: Veri Hukuku, İstanbul 2023, s. 121.

⁵¹ Küzeci E./ Kılıç, Ş.: 698 Sayılı Kişisel Verilerin Korunması Kanunu’nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 2019, C. XVI, S. 63, s. 963.

devlet tüzel kişiliğine bağlı olduklarından tüm bu kurumların işlediği kişisel verilerden sorumlu tek müessese devlet tüzel kişiliği olacaktır. Böylelikle, bütün veri işleme süreçleri tek bir envanterde toplanacak ve güncelleştirilecektir. Ancak, böyle bir durum işlevsel ve uygulanabilir olmadığı gibi, şeffaflıkla da bağdaşmamaktadır. KVKK'daki tanımın, ayrı tüzel kişiliği olmamakla beraber bağımsız bir şekilde harcama yapabilen ve karar alabilen organizasyonları da kapsayacak şekilde yeniden düzenlenmesi daha isabetli olacaktır. Zira, GDPR'daki tanımda “*diğer herhangi bir organ*” denilmek suretiyle bu sorunun önüne geçilmeye çalışılmıştır⁵². Kişisel Verileri Koruma Kurumu da doğrudan devlet tüzel kişiliğiyle ilgili olmasa da “*(kanundaki) tanımın hayatın olağan akışına uygunluğun sağlanması ve pratikte ortaya çıkan sorunların çözülebilmesi adına geniş yorumlanması gerektiği*”ne karar vermiştir⁵³.

Bahsedilmesi gereken son aktör ise veri işleyendir. GDPR'daki tanıma göre, veri işleyen, “*veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır*”⁵⁴. Veri sorumlusu ve veri işleyen arasındaki ayrımın tespit edilmesi büyük önem taşımaktadır. Zira, sorumluluk esas olarak veri sorumlusuna yüklenmişken, veri işleyenin kısıtlı bir sorumluluğu

⁵² Çekin, s. 62.

⁵³ Site Yönetimlerine ilişkin 6698 sayılı Kişisel Verilerin Korunması Kanunu ile 634 sayılı Kat Mülkiyeti Kanunu çerçevesinde Kişisel Verileri Koruma Kurulu'nun 22.07.2020 tarihli ve 2020/560 sayılı Kararı'nda yer alan değerlendirmeler için bkz. “*Kanun'un “veri sorumlusuna ilişkin getirdiği tanımın, hayatın olağan akışına uygunluğunun sağlanması ve pratikte ortaya çıkan sorunların çözülebilmesi adına geniş yorumlanması gerektiği; bu kapsamda her ne kadar tüzel kişiliği haiz olmasa da kural olarak apartman, site ve benzeri yapılar bakımından veri sorumlusu olarak kat malikleri kurulunun kabul edilebileceği, kat malikleri kurulunun ise Kanun'un veri sorumlusuna yüklediği yükümlülüklerin yerine getirilmesi bakımından bir kişiyi görevlendirebileceği, görevlendirilen bu kişinin yönetici olmasının mümkün olduğu gibi başka bir kat malikinin yahut iradi temsilcinin de olabileceği değerlendirilmekle beraber, uygulamada istisnai durumların da ortaya çıkabileceği gözetilerek nihai olarak kişisel veri işleme faaliyetinde veri sorumlusu sıfatını haiz olanların belirlenmesi için; her somut hadise açısından kişisel veri işlenmesine ilişkin kararları alan, veri kayıt sistemlerini kuran, uhdesinde bulunduran ve yöneten birimlerin tespit edilmesinin gerektiği değerlendirilmelerine yer verilmiştir*”. (<https://www.kvkk.gov.tr/Icerik/6798/2020-560>, Erişim Tarihi: 15.06.2023).

⁵⁴ Bkz. GDPR m. 4/8.

bulunmaktadır⁵⁵. Belirtmek gerekir ki, aşağıda açıklanmış olan veri işleme faaliyeti, veri işleyenin etkinliği anlamına gelmemektedir. Bu kapsamda, örneğin, KVKK'nın amaç maddesinde “*kişisel verileri işleyen*” ifadesi kullanılmaktadır. Bununla kast edilen, kişisel verilerin korunması alanındaki temel etkinlik olan işlemedir⁵⁶. Nitekim, veri sorumlusu kişisel verileri kendi işleyebileceği gibi, bu verileri bir üçüncü kişiye de işletebilmektedir. Veri sorumlusu kişisel verilerin işlenmesine ilişkin kararların alınması yetkisine sahipken, veri işleyenin faaliyetleri veri işlemenin daha çok teknik kısımları ile sınırlıdır⁵⁷.

III. Kişisel Verilerin İşlenmesi, İşleme İlkeleri ve Şartları

A. Kişisel Verilerin İşlenmesi Kavramı

Kişisel verilerin işlenmesi kavramı; bu verilerin elde edilmesi, silinmesi, yok edilmesi, kaydedilmesi, aktarılması gibi, kişisel veriler üzerinde gerçekleştirilen herhangi bir işlemi ya da işlemler bütünü ifade etmektedir⁵⁸.

Kişisel verilerin işlenmesi kavramı hem GDPR'da hem de KVKK'da birbirine benzer şekilde düzenlenmiştir. GDPR'a göre işleme faaliyeti işlenmesi “*otomatik*

⁵⁵ Çekin, s. 53.

⁵⁶ Küzeci/Kılıç, s. 960.

⁵⁷ Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, s. 2 (<https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>, Erişim Tarihi: 07.07.2023).

⁵⁸ Küzeci, s. 16; Ayözger Öngün, s. 131.

yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir”⁵⁹.

Görüleceği üzere veri işleme kavramı verinin elde edilmesinden imha edilmesine kadar olan tüm süreci kapsayacak şekilde geniş tutulmuştur⁶⁰. Ayrıca işleme faaliyeti kapsamına hem kişisel verilerin bilgisayar gibi otomatik sistemlerle işlenmesi hem de otomatik olmayan yöntemlerle işlenmesi dahil edilmiştir⁶¹. Ancak otomatik olmayan yollarla işlenen kişisel verilerin veri koruma mevzuatı kapsamına girebilmesi için bir veri kayıt sisteminde işlenmesi ya da bir veri kayıt sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesi gerekmektedir⁶². KVKK’daki tanıma göre ise veri kayıt sistemi “*kışisel verilerin belirli kriterlere göre yapılandırılarak işlendiğı kayıt sistemi*”ni ifade etmektedir.

İdare hukuku bakımından ise veri işleme faaliyetinin bir idari işlem mi yoksa eylem mi olduğunun tespit edilmesi gerekmektedir. Nasıl idari işlemler idarenin hukuksal işlemlerinin büyük bir çoğunluğunu oluşturuyorsa⁶³ idarenin kişisel veri işleme faaliyetleri de genel olarak bir idari işlem den kaynaklanmaktadır. *Saygı’nın* belirttiğı üzere; “*idare tarafından gerçekleştirilen kişisel veri işleme faaliyeti büyük çoğunlukla verilerin bir veri tabanına/sisteme kaydedilmesi ve daha sonra bu*

⁵⁹ Bkz. GDPR m. 4/2.

⁶⁰ Çekin/ Berktaş/Akıncı, s. 118.

⁶¹ Ayözger Öngün, s. 132.

⁶² GDPR m. 2.; KVKK m. 2

⁶³ Gözübüyük, A. Ş./ Tan T.: İdare Hukuku Cilt I Genel Esaslar, Güncellenmiş 14. Baskı, Ankara 2019, s. 334.

*kayıtların kullanılması/aktarılması/paylaşılması vb. işlemler şeklinde gerçekleşmektedir. Bu nedenle, kişisel verilerin idare tarafından işlenmesi büyük bir çoğunlukla idari işlem ile gerçekleşmektedir*⁶⁴. Gerçekten de kişisel verilerin işlenmesi, idarenin tek taraflı irade beyanı ile hukuk dünyasında bir yenilik veya değişiklik yarattığından idari işlem tanımıyla örtüşmektedir⁶⁵. Danıştay da kişisel verilerin işlenmesinin kesin ve yürütülebilir bir işlem olduğunu kabul etmektedir⁶⁶. Ancak, idari faaliyetlerin çeşitliliği göz önüne alındığında, veri işleme faaliyetinin sadece idari işlem ile gerçekleşeceğini belirtmek hatalı olacaktır. Zira, idarenin idari eylemler ile de kişisel veri işleyebilmesi mümkündür. Örneğin, kamu kurumlarındaki güvenlik kameralarının görüntü kaydetmesi bir işlem değil, eylem olarak kabul edilmedir⁶⁷. Ancak, görüntünün kaydedilmesi bir eylem olarak tasnif edilse de güvenlik amacıyla kameraların binaya yerleştirilmesine dair kararın bir idari işlem ile yapıldığının unutulmaması gerekmektedir. Bu sebeple, kamu binasında kamera kaydı ile kişisel verilerin işlenmesinin hukuka aykırı olması halinde idari işleme karşı iptal davası açılması gerekmektedir.

B. Kişisel Verilerin İşlenmesinde Temel İlkeler

Kişisel verilerin işlenmesi, uluslararası belgelerde kabul görmüş ve pek çok ülkenin ulusal mevzuatına entegre ettiği birtakım temel ilkelere dayanmaktadır. Gerek

⁶⁴ Saygı, S.: 6698 Sayılı Kanun'un Sistematığında Yargısal Başvuru Yolları, Kişisel Verileri Koruma Dergisi 2002, C. II, S. 2, s. 38.

⁶⁵ Başar, C.: Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması, İstanbul 2020, s. 48.

⁶⁶ Dan., 12.D, T. 15.05.2006, E. 2005/6811, K. 2006/1959, (Legalbank).

⁶⁷ Saygı, s. 39.

108 sayılı Sözleşme’de gerekse mülga 95/46/EC sayılı Direktifte yer alan bu ilkeler hem GDPR’da hem de ulusal mevzuatımızda paralel şekilde yer almaktadır. Bu genel ilkelerin önemi, hukukun gelişen teknolojilerin gerisinde kalması noktasında kendisini göstermektedir. Modern teknolojik inovasyon eşi benzeri görülmemiş bir hızda gerçekleşmekte olup teknolojiyi hukuki mekanizmalarla düzenlemek giderek zorlaşmaktadır. Zira, teknolojik gelişmeler katlanan bir hızda ilerlerken, yasal düzenlemeler kademeli şekilde ilerlemektedir⁶⁸. Bu durum, hukuki düzenlemelerin teknolojinin gerisinde kalmasına ve yeni bir teknolojinin piyasaya sürülmesi ile bu teknolojinin güvenli gelişimini şekillendirecek yasa, yönetmelik ve gözetim mekanizmalarının oluşturulması arasındaki boşluğu ifade eden hız problemine (*pacing problem*) sebebiyet vermektedir⁶⁹. Özellikle, gelişen teknolojilerle yakın ilişki içerisinde bulunan kişisel verilerin korunması hukukunun, teknolojik gelişmelere yetişemeyerek yetersiz kalması muhtemeldir. Bu bağlamda, her yeni teknoloji için mevcut düzenlemeleri değiştirmek mümkün olmadığından, kişisel verilerin işlenmesindeki temel ilkeler, gelecekte oluşabilecek her koşulda ilgili kişinin haklarının korunmasını garanti altına almaktadır. Ayrıca, bu ilkeler sayesinde bireylerin veri güvenliği ve mahremiyetinin ihlal edilmeyeceğine ilişkin güvenleri artmakta ve bu sayede veri paylaşımı artarak çeşitli ve nitelikli veriye ulaşabilmek kolaylaşmaktadır⁷⁰. İlkeler detaylıca açıklanmadan önce bu ilkelere uymanın tek başına hukuka uygunluk sebebi oluşturmayacağını belirtmek gerekir. Veri

⁶⁸ Downes, L.: *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age*, New York 2009’dan naklen, Frennert, S.: *Hitting A Moving Target: Digital Transformation And Welfare Technology in Swedish Municipal Eldercare. Disability and Rehabilitation, Assistive Technology* 2019, C. XVI, S. 1, s. 107.

⁶⁹ Hagemann, R./ Huddleston, J./ Thierer, A. D.: *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, Colorado Technology Law Journal 2018, C.XVII, S. 1, s. 59.

⁷⁰ Aşıkoğlu, s. 115.

sorumlularının aynı zamanda veri işleme şartlarından birine de dayanma mecburiyeti bulunmaktadır. Ancak, temel ilkelere uyulmamış olması, veri işleme faaliyetini hukuka aykırı hale getirmek için yeterlidir⁷¹.

Mülga mehzaz 95/46/EC sayılı Direktif ile paralel olarak KVKK'da bu ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme şeklinde sayılmıştır⁷². GDPR'da ayrıca hesap verilebilirlik (*accountability*) olarak ayrı bir ilke de bulunmaktadır⁷³. Belirtmek gerekir ki, birbirine kaynaklık eden ve birbirini tamamlayan bu ilkeler birbirleriyle ilişkili olduğundan, temel ilkelerin kesin hatlarla ayrılması bir hayli güçtür⁷⁴.

Hukuka uygun olmak, isminden de anlaşılacağı üzere verilerin işlenmesi sırasında hukuki düzenlemelerden doğan hak ve yükümlülüklerle riayet edilmesi anlamına gelmektedir. Bu ilke, esasen, hukuk devleti ilkesinin bir uzantısıdır⁷⁵. Zira, hukuk devleti ilkesi hem bireylerin hem de devletin işlem ve eylemlerini hukuk kurallarına bağlı olarak yürüttüğü bir sistemi ifade etmektedir⁷⁶. Dürüstlük kuralına uygun işlemekten kast edilen ise Türk Medeni Kanunu (TMK) m. 2 kapsamındaki dürüstlük kuralıdır. Kişisel verilerin korunması bağlamında, veri sorumlusu, ilgili kişinin beklemediği ve beklemesinin de gerekmediği sonuçların doğmasını engelleyecek şekilde hareket etmelidir. Bu kapsamda, işleme faaliyetinin şeffaf olması

⁷¹ Çekin/Berktaş/ Akıncı, s. 140.

⁷² Bkz. KVKK m. 4.

⁷³ Bkz. GDPR m. 5.

⁷⁴ Küzeci, s. 227; Oğuz, s. 129.

⁷⁵ Çekin/Berktaş/ Akıncı, s. 143.

⁷⁶ Gözübüyük/Tan, s. 33-34.

ve veri sorumlusunun bilgilendirme ile uyarı yükümlülüklerini yerine getirmesi gerekmektedir. Genel bir ilke olan hukuka ve dürüstlük kurallarına uygun olma, diğer ilkeler aracılığıyla somutlaşmaktadır⁷⁷.

Doğru ve gerektiğinde güncel olma ilkesi uyarınca, doğru olmayan kişisel verilerin gecikmeksizin silinmesi veya düzeltilmesi için gerekli eylem ve işlemlerin gerçekleştirilmesi anlamına gelmektedir⁷⁸. Veri işleme faaliyeti, kamusal işlemlerin yerine getirilmesinden davranışsal reklamcılığa kadar çok farklı amaçlarla kullanılabilir. Ancak, hangi amaçla olursa olsun yanlış kişisel verilerin işlenmesinden doğan sonuçlar hatalı olacak ve veri işlenmesinden sağlanmak istenen faydayı ortadan kaldıracaktır⁷⁹. Bu bağlamda, veri sorumlusu, işlediği kişisel verilerin güncel, eksiksiz ve hatasız olması için makul her türlü önlemi almakla yükümlüdür. İlgili kişinin yanlış veya eksik bilgilerin düzeltilmesini talep hakkı da⁸⁰ bu ilkenin bir uzantısıdır⁸¹. Danıştay'ın da belirttiği üzere, idarenin silinmesi gereken kişisel verileri silmemesi ve verileri güncel tutmaması hizmet kusuru oluşturmaktadır⁸². Örneğin Danıştay'ın önüne gelen bir davada, başvuru askerliğini tamamlamış olmasına rağmen bilgisayar kayıtlarından bakaya kaydının düşülmemesi nedeniyle havalimanı pasaport kontrolü sırasında yurtdışına çıkışına izin verilmemiştir. Olayı değerlendiren Danıştay, bilgisayar kayıtlarını düzenli bir şekilde tutmanın ve güncellenmenin idarenin

⁷⁷ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2-3. (<https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf>, Erişim Tarihi: 20.06.2023).

⁷⁸ Ersoy Kekevi, s. 139.

⁷⁹ Küzeci, s. 243.

⁸⁰ Bkz. GDPR m. 16; KVKK m. 11.

⁸¹ Çekin/Berktaş/ Akıncı, s. 155.

⁸² Dan 10. D, T. 17.10.2007 , E. 2007/1376, K. 2007/4756, (Lexpera).

yükümlülüğü olduğunu belirterek, hizmet kusuru nedeniyle başvurucunun uğradığı maddi ve manevi zararların ödenmesi gerektiğine hükmetmiştir⁸³.

Belirli, açık ve meşru amaçlar için işleme ise; veri sorumlularının kişisel verilerin hangi amaçlarla toplandığını, veri işleme faaliyetinin en başından belirleme ve veri işleme sürecinin sonuna dek bu amaca uygun hareket etmesi yükümlülüğü anlamına gelmektedir. Ayrıca, meşruluk şartının yerine getirilmesi için veri işleme faaliyetinin hukuki düzenlemelerle uyum içinde gerçekleşmesi gerekmektedir⁸⁴.

İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi uyarınca, veri işleme faaliyeti olabilecek en düşük seviyede tutulmalıdır. Kişisel verilerin işlenmesi için, işleme ile, gerçekleşecek amaca başka bir şekilde ulaşılamaması gerekmektedir. Başka bir ifade ile, eğer arzu edilen amaca temel hak ve özgürlüklere daha az müdahale edilerek veya hiç müdahale edilmeden ulaşılabilirse kişisel verilerin işlenmemesi gerekmektedir⁸⁵. Kişisel verilerin işlenmesi durumunda ise, işleme faaliyeti yalnızca amaca ulaşmaya yetecek oran ile sınırlı tutulmalı ve “*amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden*”⁸⁶ kaçınılması gerekmektedir⁸⁷. Örneğin, Kişisel Verileri Koruma Kurumu bir belediyenin memurların işe giriş çıkış saatlerinin takibinin parmak izi sistemiyle, yani özel nitelikli

⁸³ Dan 10. D, T. 24.02.1998, E. 1998/5023, K. 1998/807, (Danıştay Dergisi, S. 97. s. 685 vd.).

⁸⁴ ICO, *A Guide to the Data Protection Principles*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>, Erişim Tarihi: 20.06.2023).

⁸⁵ Çekin/Berktaş/ Akıncı, s.156.

⁸⁶ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 10 (<https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf>, Erişim Tarihi: 20.06.2023).

⁸⁷ Finck, M./ Biega, A.: *Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems*, Technology and Regulation 2021, s. 55; Küzeci, s. 237-239; An Coimisiun Um Chosaint Sonrai: *Principles of Data Protection*, (<https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>, Erişim Tarihi: 20.06.2023).

kişisel verilerin işlenmesi suretiyle, yapılmasını ölçülülük ilkesine aykırı bulmuştur⁸⁸. Bu ilke; asgari veri işlenmesi, veri minimizasyonu, veri ekonomisi gibi farklı şekillerde de isimlendirilmektedir.

İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi, kişisel verilerin ulaşılmak istenen amaç için gereksiz hale gelmesi durumunda yok edilmesi yükümlülüğünü getirmektedir. Bu durum üç şekilde ortaya çıkabilir; istenen amaca ulaşmak için kişisel veriye ihtiyaç olmadığı anlaşılabilir, işleme faaliyeti ile ulaşılmak istenen amaç ortadan kalkabilir ya da amaca ulaşıldığı için kişisel verinin tutulması gereksiz hale gelebilir⁸⁹. Orantılılık ilkesinin zamansal düzenlemesi olan bu ilke uyarınca mevzuatta verilerin saklanması için bir süre öngörülmüşse kişisel verilerin muhafaza edilmesinde bu süreye riayet edilmesi gerekmektedir⁹⁰.

C. Kişisel Verilerin İşlenme Şartları

2010 Anayasa değişikliği neticesinde Anayasanın özel hayatın gizliliği başlıklı 20. maddesine kişisel verilerin korunması ile ilgi 3. fıkra eklenerek kişisel verilerin korunması bir temel hak olarak kabul edilmiştir. Maddede belirtildiği üzere, “*kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir*”. Bu

⁸⁸ “Belediyede memur olarak görev yapan ilgili kişinin, veri sorumlusu bünyesinde işe giriş çıkış takibinin biyometrik veri işlenerek yapılması” hakkında Kişisel Verileri Koruma Kurulunun 01/12/2020 tarihli ve 2020/915 sayılı Karar Özeti için bkz. (<https://www.kvkk.gov.tr/Icerik/6872/2020-915>, Erişim Tarihi: 20.06.2023).

⁸⁹ Küzeci, s. 245.

⁹⁰ Ersoy Kekevi, s. 150.

bağlamda, kural olarak, kişisel verilerin işlenmesi yasaktır ve yalnızca, bir hukuka uygunluk nedeninin varlığı halinde kişisel veriler işlenebilmektedir. Bu düzenlemeye paralel olarak, kişisel verilerin korunması ile ilgili mevzuatta çeşitli veri işleme şartları, yani hukuka uygunluk nedenleri sınırlı olarak sayılmaktadır^{91,92}. Bu bağlamda, idarenin düzenleyici işlemler ile yeni bir hukuka uygunluk hali belirlemesine imkân bulunmamaktadır. Ancak, kanundaki açık bir hüküm ile ikincil mevzuata yönlendirme yapılması yani genel çerçevenin kanunla belirlenmesi ve bu sayede yasal dayanak kanun olup, düzenleyici işlem hükümleri uyarınca da veri işlenmesi mümkündür⁹³. Ayrıca kamu “kurum ve kuruluşlar(ınca)ca hazırlanan ve kişisel verilere ilişkin hükümler içeren mevzuat tasarıları hakkında Kişisel Verileri Koruma Kurulu'ndan görüş alınması şart(tır)”⁹⁴.

Düzenleyici işlemlerde veri işlenmesine ilişkin kurallar belirlenmesinin bir örneği Dernekler Yönetmeliğinde yapılmıştır. Ancak, derneklere üyelik yapan veya üyelikten çıkan kişilerle ilgili birçok kişisel veriyi mülki idari amire bildirme yükümlülüğünü inceleyen Danıştay, Dernekler Yönetmeliğindeki değişikliği; “Kanunda düzenlenmediği halde, davalı idareye tanınan yetkinin sınırlarını genişleten ve kişisel verilerin ve özel nitelikteki kişisel verilerin açık rıza alınmadan işlenmesini sağlayacak dava konusu düzenlemede hukuki isabet (bulunmadığı)” gerekçesiyle iptal etmiştir. Her ne kadar sonradan Dernekler Kanunu’nda yapılan değişiklik ile ilgili yönetmeliğe yasal dayanak oluşturulmuş olsa da yasaların geçmişe yürümezliği ilkesi

⁹¹ KVKK m. 5, GDPR m. 6.

⁹² İlgilinin açık rızası veya kanunda açık bir düzenleme olmadan belediye bünyesinde parmak izi kayıt sistemi ile mesai takibi yapılmasının özel hayata saygı hakkının ihlal ettiği yönünde karar için bkz. AYM, Ramazan Şahin Başvurusu, B. No: 2018/11988, T. 10.3.2022, (Lexpera).

⁹³ Kişisel Verileri Koruma Kurumu, Kişisel Verilerin İşlenme Şartları, s. 6 (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf>, Erişim Tarihi 17.06.2023).

⁹⁴ Dan. 15 D, T. 14.3.2018, E. 2018/844 K. YD, (Lexpera).

uyarınca yapılan kanun deęiřiklięi, Yönetmelik hükmünün hukuka aykırılıęını ortadan kaldırmamaktadır⁹⁵.

Bunun yanında, kiřisel verilerin korunması Anayasa'nın ikinci kısmının ikinci bölümünde düzenlenen bir temel hak olduęundan dolayı Anayasa m. 104/17 uyarınca kiřisel verilere iliřkin Cumhurbaşkanlıęı Kararnamesi ile düzenleme yapılamamaktadır⁹⁶.

Ayrıca, Kanun'da sayılan hukuka uygunluk nedenleri idarenin veri iřleme faaliyetlerinin yasal dayanaęını oluřturmaktadır. Zira, idarenin kanunilięi ilkesinin bir uzantısı olan kanuna dayanma ilkesine göre *“bireyin özgürlüklerini etkileyen idari eylem ve iřlemlerde idarenin pozitif bir hukuki dayanaęının bulunması zorunludur”*⁹⁷. Belirtmek gerekir ki, ulusal ve uluslararası düzenlemelerde özel nitelikli kiřisel veriler ile kiřisel verilerin iřlenmesi ayrı řekilde düzenlenmekte ve özel nitelikli kiřisel veriler daha sıkı iřleme řartlarına tabii olmaktadır.

KVKK m. 5'te belirlenen hukuka uygunluk sebepleri ařaęıdaki gibidir:

- “• *İlgili kiřinin açık rızasının varlıęı,*
- *Kanunlarda açıkça öngörülmesi,*
- *Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kiřinin kendisinin ya da bir başkasının hayatı veya beden bütünlüęünün korunması için zorunlu olması,*

⁹⁵ Dan. 10 D., T. 15.4.2021, E. 2018/5223, K.2021/1866, (Lexpera).; Danıřtay ayrıca “E-nabız” projesi konulu genelgeyi benzer gerekçelerle iptal etmiřtir. Bkz. Dan. 15. D, T. 14.11.2017, E. 2015/3035, K. 2017/6611, (Lexpera).

⁹⁶ İlgili AYM kararları için bkz. AYM, T. 29.12.2022, E. 2018/149, K. 2022/163, RG. 03.08.2023, S. 32268.

⁹⁷ Akyılmaz, B. /Sezginer, M. /Kaya, C.: Türk İdare Hukuku, 16. Baskı, Ankara 2023, s. 148.

- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması(dır) ”⁹⁸

İdare veri işleme faaliyeti gerçekleştirirken bu şartlardan herhangi birine dayanabilmekle beraber, çalışmada idare bakımından özellikle önemli olan açık rıza, kanunlarda açıkça öngörülmesi ve meşru menfaat kavramları incelenecektir.

1. Açık Rıza

Hem Anayasada hem de mevzuatta düzenlenen ilk veri işleme şartı ilgili kişinin açık rızasıdır. KVKK’daki tanım uyarınca açık rıza “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı*” ifade etmektedir. Bu tanımdaki unsurlar uyarınca açık rıza; belirli, bilgilendirmeye dayalı ve özgür iradeyle açıklanan bildirim anlamına gelmektedir⁹⁹. Ancak, bu noktada KVKK ve GDPR birbirinden ayrılmaktadır. GDPR’da veri işleme şartı olarak rıza ve açık rıza olarak iki terim kullanılmakta ve özel nitelikli kişisel verilerin işlenmesi bakımından açık rıza

⁹⁸ Bkz. KVKK m. 5.

⁹⁹ Çekin/Berktaş/ Akıncı, s. 159; Ayrıca ilgili Kanun’un gerekçesinde bu tanımın mülga 95/46/EC sayılı Yönergeye dayandırıldığı belirtilmektedir.

aranırken diğer kişisel veriler için rızanın varlığı yeterli kabul edilmektedir. Buna karşın KVKK’da rıza kavramı kullanılmayıp hem özel nitelikli kişisel veriler hem de diğer veriler için açık rıza şartı aranmaktadır. GDPR’daki tanıma göre rıza “*veri sahibinin bir beyanla veya açık bir olumlu eylemle kendisiyle ilgili kişisel verilerin işlenmesini kabul ettiğini belirttiği, özgürce verilmiş, spesifik, bilinçli ve açık bir şekilde isteklerini belirtmesi*” anlamına gelmektedir¹⁰⁰. Açık rızanın ise GDPR kapsamında bir tanımı yapılmamakla birlikte, normal bir rızadan daha katı şartlara bağlandığı kabul edilmektedir¹⁰¹. Bu bağlamda KVKK’daki her türlü veri işleme faaliyeti için açık rıza aranması, veri sorumlularını ölçsüz şekilde sınırlayarak menfaat dengesini ilgili kişi lehine bozduğu gerekçesiyle eleştirilmektedir¹⁰². Çalışmanın ilerleyen kısımlarındaki açık rıza kavramı, GDPR kapsamındaki rıza kavramı yerine kullanılacaktır.

GDPR ve KVKK arasındaki bir diğer fark ise, GDPR’da rızanın hukuka uygunluk sebeplerinden biri olarak sayılması iken KVKK’da açık rızaya dayalı kişisel veri işlenmesinin kural olması, diğer hallerinse istisna olarak sayılmasıdır¹⁰³. Ancak,

¹⁰⁰ Bkz. GDPR m. 4/11.

¹⁰¹ Açık rızanın varlığının hangi durumlarda kabul edileceği hakkında ayrıntılı bilgi için bkz EDPB, *Guidelines 05/2020 On Consent Under Regulation 2016/679*, Version 1.1, 2020, s. 20-22 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, Erişim Tarihi: 22.06.2023); ICO, *What Is Valid Consent?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/>, Erişim Tarihi: 22.06.2023).

¹⁰² Çekin, s. 84-85.

¹⁰³ 6698 sayılı KVKK m. 4:

- (1) *Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.;*
- (2) *Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:*
 - a) *Kanunlarda açıkça öngörülmesi.*
 - b) *Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.*
 - c) *Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*
 - ç) *Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.*
 - d) *İlgili kişinin kendisi tarafından alenileştirilmiş olması.*
 - e) *Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.*

KVKK her ne kadar böyle bir düzenleme yoluna gitse de bu durum veri işleme şartları arasında hiyerarşik bir ilişki olduğu anlamına gelmemektedir. Veri işleme faaliyetinin meşruluğu bakımından, açık rızaya veya kanunda düzenlenen diğer hukuka uygunluk sebeplerine dayanılması arasında bir fark bulunmamakta, kanundaki tüm haller işleme faaliyetini eşit derecede meşru kılmaktadır¹⁰⁴.

Her ne kadar aralarında hiyerarşi olmasa da açık rıza ile ilerleyen kısımlarda ele alınmış olan diğer hukuka uygunluk sebepleri arasındaki ilişkinin incelenmesi gerekmektedir. Başka bir hukuka uygunluk sebebi varken yine de açık rızaya dayanılıp dayanılmayacağı konusu doktrinde tartışmalıdır. Başka bir deyişle, örneğin, veri işlemenin kanunlarda açıkça öngörülmesi durumunda ilgili kişilerden yine de açık rıza alınıp veri işleme faaliyetinin kanun yerine söz konusu rızaya dayandırılıp dayandırılmayacağı belirsizdir. Kişisel Verileri Koruma Kurumu’nun benimsediği bir görüşe göre, açık rıza ile diğer hukuka uygunluk sebepleri bir arada bulunamamaktadır. Bu nedenle, eğer veri sorumluları açık rıza haricinde bir sebebe dayanarak veri işleyebiliyorlarsa açık rızaya dayanabilmek mümkün değildir.

Kişisel Verileri Koruma Kurumu’nun yayınladığı rehberde belirtildiği üzere *“kişisel veri işleme, Kanunda bulunan açık rıza dışındaki şartlardan birine dayanıyorsa, bu durumda ilgili kişiden açık rıza alınmasına gerek bulunmamaktadır. Veri işleme faaliyetinin, açık rıza dışında bir dayanakla yürütülmesi mümkün iken açık rızaya dayandırılması; ilgili kişinin yanıltılması ve yanlış yönlendirilmesi dolayısıyla aldatıcı ve veri sorumlusunca hakkın kötüye kullanımı niteliğinde olacaktır. Nitekim,*

f) *İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”.*

¹⁰⁴ Çekin/ Berktaş/Akıncı, s. 159; An Coimisiun Um Chosaint Sonrai, Guidance Note: *Legal Bases for Processing Personal Data*, (<https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data>, Erişim Tarihi: 17.06.2023).

ilgili kiři tarafından verilen açık rızanın geri alınması halinde veri sorumlusunun diğeri kişisel veri işleme şartlarından birine dayalı olarak veri işleme faaliyetini sürdürmesi hukuka ve dürüstlük kurallarına aykırı işlem yapılması anlamına gelecektir”¹⁰⁵.

Avrupa Veri Koruma Kurulu’nun (EDPB) kabul ettiğı diğeri bir görüşe göre ise, açık rıza ve diğeri hukuka uygunluk sebepleri, aralarında hiyerarşı olmadığından dolayı bir arada bulunabilmektedir. Başka bir deyişle, veri sorumlusunun birden çok hukuka uygunluk sebebine dayanabilme imkânı varsa, veri sorumlusu bunlardan birini seçmekte özgürdür. Ancak, veri sorumlusunun işleme faaliyeti için rızaya dayanmayı seçmesi halinde, bu seçime saygı göstermesi ve bireyin rızasını geri çekmesi halinde işleme faaliyetini durdurması gerekmektedir. Yani, veri sorumlusu, yasal dayanaklar arasında geçiş yapamamakta ve seçimiyle bağılı olmaktadır. Aksi bir kabul, ilgili kişilere kişisel verilerinin açık rıza temelinde işleneceğı yönünde yanıltıcı bir mesaj vererek adaletsiz bir uygulamaya sebep olacaktır¹⁰⁶.

Son olarak, açık rıza metninin bulundurması gereken asgari içeriğinin ne olduğunun belirtilmesi gerekmektedir. EDPB’ye göre rıza metni asgari olarak aşağıdaki bilgileri içermelidir¹⁰⁷:

- Veri sorumlusunun kimliğı,
- Rızanın talep edildiğı işleme faaliyetlerinin her birinin amacı,
- Hangi tür verilerin toplanacağı ve kullanılacağı,
- Rızayı geri çekme hakkının varlığı,

¹⁰⁵ Kişisel Verileri Koruma Kurumu (Kişisel Verilerin İşlenme Şartları), s. 3-4.

¹⁰⁶ EDPB, s. 25; Çekin/Berktaş/ Akıncı, s. 178-179.

¹⁰⁷ EDPB, s. 15.

- Verilerin münhasıran otomatik sistemlerle işlenip işlenmeyeceği hakkında bilgi,
- Güvenli ülke kararı ile uygun güvenceler olmaksızın verilerin yurtdışına aktarıldığı durumlarda, olası riskler hakkında bilgi.

Veri sorumlusu olarak idarenin gerçekleştirdiği işleme faaliyetlerinde genellikle kanunun verdiği bir yetkiye dayanılsa da¹⁰⁸ açık rızaya dayanılmasının önünde herhangi bir engel bulunmamaktadır¹⁰⁹. Örneğin, kamu sitelerinde zorunlu olmayan çerezlerin toplanması¹¹⁰ veya belediyelerin anket yapması idarenin açık rızaya dayanarak gerçekleştirdiği veri işleme faaliyetleridir. Ancak, kanımızca, idari işlemin tanımı dolayısıyla idari işlemler ile açık rızaya dayalı kişisel veri işlenmesi mümkün gözükmemektedir. İdari işlemler tanımı gereği idarenin tek yanlı irade açıklaması ile ilgililerin izni veya rızası olmadan, idarenin hukuki durumlarda değişiklik yapabilmesidir¹¹¹. Tek yanlılık ile ilgili kişinin açık rızasının alınması zorunluluğunun kanımızca birbiriyle uyuşmamaktadır. Benzer şekilde, ilgili kişinin rızasını geri alması halinde veri işleme faaliyeti geri alma tarihinden itibaren hukuka aykırı hale gelmektedir. Ancak, bir idari işlemin hukuki sonuç doğurduğu kişinin beyanı ile hukuka aykırı hale gelmesi kabul edilebilir değildir. Bu hususta dikkat edilmesi gereken konu bazı durumlarda kişilerin idareye başvurarak bir işlem yapılmasını talep etmesidir. Örneğin memurluğa atanmak için bireyler idareye bir başvuruda bulunmaktadır ve idarenin memur olmak için başvuru yapmayan bir kişiyi

¹⁰⁸ Altındağ, H.: *Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi 2019, C. XVIII, S. 2, s. 390.

¹⁰⁹ ICO, *When is Consent Appropriate?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/>, Erişim Tarihi: 28.06.2023).

¹¹⁰ Bkz. s. 74-76.

¹¹¹ Gözübüyük/Tan, s. 340-341.

ataması söz konusu değildir. Bu durumda her ne kadar idari işlemin yapılması için ilgilinin rızasının alınması gerekiyor gibi gözükse de kanaatimizce bu durum işlemin tek yanlılığını ortadan kaldırmamaktadır. Zira, bu durumda vatandaş idareden bir istekte bulunmakta ve idareyi belirli bir işlemi yapmaya yönlendirmektedir. Ancak işlemin yapılıp yapılmayacağı kararını yine idare vermektedir. Başka bir deyişle, bu tip durumlarda vatandaş bir idari işlemin gerçekleşmesini istemekte ve bu doğrultuda idareden bir talepte bulunmaktadır. Buna karşın, açık rızaya dayalı veri işleme faaliyetlerinde ise, idare bir faaliyette bulunmak istemekte ancak bu faaliyeti hukuka uygun olarak gerçekleştirebilmesi için zorunlu olarak ilgili kişiden bir rıza/onay olması gerekmektedir. Bu bağlamda, kanımızca idarenin açık rızaya dayanarak gerçekleştirdiği işleme faaliyetlerinin idari işlem olarak değerlendirilmemelidir.

2. Kanunlarda Açıkça Öngörülmesi

Kanunda açıkça öngörülme, idarenin veri işleme uygulamalarının önemli bir dayanağını oluşturmaktadır. Açık kavramından anlaşılması gereken, kanunla verilen genel bir yetkinin meşru işleme haline vücut vermeyeceğidir. KVKK’da sayılan bu şart GDPR’da öngörülmemekle birlikte, *“kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması”* şeklinde benzer nitelikte bir düzenleme bulunmaktadır¹¹².

¹¹² Küzeci, s. 395.

KVKK'nın gerekçesinde bu duruma örnek olarak “*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 verilerini işlemesi*” halleri sayılmıştır^{113,114}. Esasen, madde gerekçesinde belirtilen ceza mahkumiyetine ilişkin veriler özel nitelikli kişisel veri olarak sayıldığından m. 5 kapsamında işlenememektedir. Ancak, KVKK m. 6’ da ceza mahkumiyetine ilişkin verilerin kanunda açıkça öngörülmesi halinde işlenebileceği düzenlendiğinden kanun koyucunun yaptığı bu nitelendirme pratik veya teorik bir sorun yaratmamaktadır¹¹⁵.

Kanunda açıkça düzenleme olan hallerde idarenin kanundaki sınırlarla bağlı kalması gerekmektedir. Örneğin, 5352 sayılı Kanun m. 10 uyarınca “*on sekiz yaşından küçüklerle ilgili adli sicil ve arşiv kayıtları; ancak soruşturma ve kovuşturma kapsamında değerlendirilmek üzere Cumhuriyet başsavcılıkları, hâkim veya mahkemelerce istenebilir*”. Bu bağlamda, 18 yaşından küçükken işlenen bir suça ilişkin arşiv kayıtlarının idari makamlar ile paylaşılmasına imkân bulunmamaktadır.

¹¹³6698 sayılı Kişisel Verilerin Korunması Kanunu m. 5 gerekçesi için bkz. (<https://www.lexpera.com.tr/mevzuat/gerekceler/kisisel-verilerin-korunmasi-kanunu-madde-gerekceleri/1>, Erişim Tarihi: 17.06.2023).

¹¹⁴ Bu düzenlemelere ek olarak şu düzenlemelerde örnek gösterilebilir: “*Türkiye Cumhuriyeti vatandaşlarının nüfus kayıtları arasında bağ kurmak, kişilerin kaydına ulaşmak ve kamu kuruluşlarında tutulan kayıtlar arasında ilişki sağlamak amacıyla taşıyan bir numara sistemi olan ve kişiye bir defa verilip sonrasında değiştirilemeyen Türkiye Cumhuriyeti kimlik numarası ile ilgili olarak 5490 sayılı Nüfus Hizmetleri Kanunu’nun 47’nci maddesinde, kişiler adına düzenlenecek olan her türlü form, beyanname, kimlik kartı, vergi kimlik kartı, sürücü belgesi, pasaport gibi bütün tanıtıcı belgelerde Türkiye Cumhuriyeti kimlik numarasına yer verileceği belirtilmek suretiyle, kanun hükmüyle kimlik numarasının işlenmesi öngörülmektedir. Yine 1111 sayılı Askerlik Kanunu’nun 14’üncü maddesinde yoklama işlemi için yükümlülerin öğrenim durumlarının, mesleklerinin ve niteliklerinin belirleneceği söylenmektedir. Anılan hükümde de Askerlik Kanunu’nun getirdiği kural gereği yükümlülerin sayılan kişisel verileri işlenmektedir. Keza 5271 sayılı Ceza Muhakemesi Kanunu’nun 137’nci maddesindeki hüküm gereği, Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi tarafından, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılması istediğinde, bu istem derhal yerine getirilecektir*”. Bkz. (Başar, s. 63).

¹¹⁵ Başar, s. 63.

Danıştay, bu konuda önüne gelen bir davada ilgili verilerin güvenlik soruşturması için paylaşılmasını ve bu verilere dayanılarak öğretmen olan davalı hakkında tesis edilen atama işleminin kaldırılması yönündeki işlemi hukuka aykırı bulmuştur¹¹⁶.

3. Meşru Menfaat

İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun (kendi) meşru menfaatleri için veri işlenmesinin zorunlu olması halinde de kişisel verilerin işlenmesi mümkündür. Bu durumun varlığının tespiti için iki aşamalı bir test yapılarak öncelikle meşru menfaatin varlığı tespit edilmeli, ardından bu meşru menfaatin ilgili kişinin temel hak ve özgürlüklerine zarar vermediği saptanmalıdır. Kişisel Verileri Koruma Kurumu'na göre meşru menfaatin varlığı tespit edilirken;

- *“Kişisel verinin işlenmesi sonucunda elde edilecek menfaat ile ilgili kişinin temel hak ve hürriyetlerinin yarışabilir düzeyde olması,*
- *Söz konusu menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesi,*
- *Meşru menfaatin halihazırda mevcut, belirli ve açık olması,*
- *İlgili kişinin temel hak ve hürriyetleri ile yarışabilir nitelikte olan meşru menfaatin elde edilmesi halinde bir yarar sağlanacak olması ve kişisel veri işlenmeksizin başkaca bir yol ve yöntemle bu yararın ortaya çıkmasının mümkün olmaması,*

¹¹⁶ Dan. 2. D, T. 16.3.2021, E. 2019/324, K.2021/632, (Lexpera).

- *Meşru menfaat belirlenirken söz konusu yararın çok sayıda kişiyi etkilemesi, yalnızca kâr elde edilmesi ya da ekonomik yararın sağlanması amacına yönelik olmaması, iş süreçlerini ya da bir işleyişi kolaylaştırması (örneğin bir birim ya da az sayıda personel nezdinde değil, kurumsal olarak geneli etkileyecek şekilde) gibi şeffaf ve hesap verilebilir nitelikleri haiz kriterlerin esas alınması,*
 - *Bu açıdan ilgili kişinin başta kişisel verilerinin korunması olmak üzere 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,*
 - *Bu kapsamda, kişinin temel hak ve hürriyetleri ile veri sorumlusunun meşru menfaatinin karşılaştırılarak denge testinin yapılması”* gerekmektedir¹¹⁷.
- Görüleceği üzere bu veri işleme şartının tespiti ölçülülük ilkesiyle yakın bağlantı içindedir.

Söz konusu hukuka uygunluk nedenine örnek olarak, kamu kurumlarının güvenlik amacıyla kamu binalarına kamera yerleştirmesi ve kayıt yapması gösterilebilir. Zira güvenliğin sağlanmasında kamu tüzel kişinin üstün gelen bir menfaati bulunmaktadır¹¹⁸. Ancak meşru menfaate dayanarak veri işleyebilmesi için

¹¹⁷ Bkz. Kişisel Verileri Koruma Kurumu, “Veri sorumlusunun kanuni yükümlülüğünü yerine getirmek için işlediği kişisel verileri meşru menfaat çerçevesinde kullanma talebiyle Kuruma yapmış olduğu başvuru” Kişisel Verileri Koruma Kurulunun 25/03/2019 tarihli ve 2019/78 Sayılı Karar Özeti, (<https://www.kvkk.gov.tr/Icerik/5434/2019-78>, Erişim Tarihi: 17.06.2023).

¹¹⁸ Başar, s. 75.

idarenin yukarıda açıklanan standartlara da uyması gerekmektedir. Bu bağlamda, idarenin kamera kaydı yanında ses kaydı da alması¹¹⁹ veya güvenlik kameralarını çalışma alanları da içerecek şekilde kamu binalarının tamamını izleyecek şekilde yerleştirmesi¹²⁰ üstün bir menfaat olarak değerlendirilmemektedir. Çünkü, güvenlik binaların sadece belirli yerlerine ses kaydı almayan kameralar yerleştirilerek sağlanabilecekken, aksi bir uygulama özel hayatın gizliliğine ölçsüz bir müdahale oluşturmaktadır.

GDPR’da da benzer bir düzenleme olmakla beraber, KVKK’dan farklı olarak, kamu makamlarının görevlerinin ifası nedeniyle gerçekleştirdiği işleme faaliyetlerinde meşru menfaate dayanması yasaklanmıştır. GDPR’ın giriş bölümünün 47. paragrafında bu istisnanın nedeni, kamu makamlarına kişisel verileri işlemeleri için yasal dayanak sağlamanın yasama organına ait olması olarak açıklamaktadır. Yani, bir kamu makamı, görevlerini yerine getirirken kişisel verileri yalnızca kanun koyucunun yetki vermesi durumunda işleyebilmelidir. Ancak, bu yasak kamu makamlarının sadece asli görevleri olarak anlaşılmalıdır. Kamu makamları asli görevleriyle ilgili olmayan, örneğin ofis yönetimi gibi, başka amaçlar için GDPR uyarınca da meşru menfaate dayanarak kişisel veri işleyebilmektedir¹²¹.

Yukarıda Kişisel Verileri Koruma Kurumu’nun belirlediği standartlar evrensel olmayıp, yalnızca ülkemiz açısından geçerlidir. Bu bağlamda, örneğin, İrlanda Veri

¹¹⁹ Bkz. Kişisel Verileri Koruma Kurumu, “Ses kayıt özelliği bulunan güvenlik kamerası kullanılması” ile ilgili Kişisel Verileri Koruma Kurulunun 12/03/2020 tarihli ve 2020/212 sayılı Karar Özeti”, (<https://www.kvkk.gov.tr/Icerik/6892/2020-212>, Erişim Tarihi: 17.06.2023).

¹²⁰ Dan. 10. D, T. 14.5.2018, E. 2015/5219, K. 2018/1739, (Lexpera); Dan. 10. D, T. 11.1.2021, E. 2019/10118, K. 2021/43, (Lexpera).

¹²¹ An Coimisiun Um Chosaint Sonrai: *Guidance Note: Legal Bases for Processing Personal Data*, 2019, s. 21, (<https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data>, Erişim Tarihi: 26.07.2023).

Koruma Kurumu meşru menfaatin, diğer hukuka uygunluk nedenlerine tam olarak dayanılamaması halinde uygulanabilen bir işleme şartı olduğunu kabul ederken, Kurum meşru menfaatin bir son çare aracı olmadığını belirtmektedir¹²². Ayrıca, İrlanda Veri Koruma Kurumu ülkemizden farklı olarak, meşru menfaatten sağlanacak yararın çok sayıda kişiyi etkilemesini meşru menfaatin belirlenmesinde bir kriter olarak değerlendirmemektedir¹²³. Benzer şekilde, Kişisel Verileri Koruma Kurumu’nun yaklaşımından farklı olarak, Avrupa Komisyonu, yalnızca kar elde edilmesi ya da ekonomik yarar sağlanması amacına yönelik faaliyetlerin meşru menfaat kapsamında değerlendirilebileceği görüşündedir¹²⁴.

IV. İlgili Kişinin Hakları ve İdareye Başvuru

KVKK m. 11’de ilgili kişinin sahip olduğu haklar düzenlenmektedir¹²⁵. Söz konusu madde uyarınca, ilgili kişi; kişisel verilerin işlenip işlenmediğin, öğrenmek, verilerinin silinmesinin talep etmek veya verilerin aktarıldığı kişileri öğrenmek gibi

¹²² Kişisel Verileri Koruma Kurumu (Kişisel Verilerin İşlenme Şartları), s. 16.

¹²³ An Coimisiun Um Chosaint Sonrai, (Guidance Note: Legal Bases for Processing Personal Data), s. 22.

¹²⁴ Hollanda Veri Koruma Otoritesine, uygulamalarının hatalı olduğu yönünde yazılan açık mektup için bkz. (<https://static.nrc.nl/2022/pdf/letter-dutch-dpa-legitimate-interest.pdf>, Erişim Tarihi: 23.07.2023).

¹²⁵ Bkz. 6698 sayılı KVKK m. 11:“ (1) *Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;*

a) Kişisel veri işlenip işlenmediğini öğrenme,
b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir”.

birçok hakka sahiptir. Ancak, bu hakların kullanılabilmesi için bireylerin kişisel verilerinin işlendiği hususunda bilgi sahibi olması gerekmektedir. Bu bağlamda, veri koruma mevzuatı veri sorumlularına aydınlatma yükümlülüğü getirerek bu yükümlülüğün asgari içeriğini belirlemektedir¹²⁶. Veri sorumlusu idare bakımından ise, aydınlatma yükümlülüğünün yerine getirilmesi kanuni bir zorunluluğun yanında idarenin şeffaflığının bir gereği olarak kabul edilmelidir¹²⁷. Yukarıda belirtildiği üzere, aydınlatma yükümlülüğünün yerine getirilmemesi hukuka ve dürüstlük kurallarına aykırılık teşkil edeceğinden veri işleme faaliyetini hukuka aykırı hale getirecektir.

İlgili kişinin bu haklarını kullanması iki şekilde gerçekleşebilmektedir: ya ilgili kişi veri sorumlusuna karşı dava açacak ya da KVKK da öngörülen iki aşamalı yargı dışı başvuru yolunu kullanacaktır. KVKK m. 13'te düzenlenen ve yargı dışı başvuru yollarının ilk aşaması olan veri sorumlusuna başvuru yöntemi uyarınca, ilgili kişi taleplerini veri sorumlusuna iletmek, veri sorumlusu ise en geç 30 gün içerisinde başvuruyu cevaplandırmakla yükümlüdür. Başvurunun usul ve esasları Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de (VSBT) düzenlenmektedir. Veri sorumlusunun başvuruyu reddetmesi, süresinde cevap vermemesi veya cevabın yetersiz bulunması halinde ise KVKK m. 14 uyarınca cevap tarihinden itibaren 30 ve herhalde başvuru tarihinden itibaren 60 gün içerisinde Kişisel Verileri Koruma Kurulu'na başvurulabilmektedir. Belirtmek gerekir ki, veri sorumlusuna başvuru Kurul'a şikayet için tüketilmesi zorunlu olan bir yol olmakla birlikte dava şartı olarak düzenlenmemektedir. Bu bağlamda, ilgili kişi veri

¹²⁶ Bkz. GDPR m. 14, KVKK m. 10.

¹²⁷ Küzeci, s. 248.

sorumlusuna başvurduktan sonra, hatta veri sorumlusuna başvuru yapmadan önce dahi genel hükümlere göre dava açabilmektedir¹²⁸.

Bu noktada veri sorumlusu olan idareye KVKK m. 13 kapsamında yapılan başvurunun hukuki niteliğinin belirlenmesi önemlidir. Başvurunun bir idari başvuru olduğu açık olmakla birlikte, idari usul bakımından niteliğine ilişkin genel bir tanımlama yapmak mümkün değildir. Zira, başvurunun tasnifi içeriğe göre değişiklik gösterecektir.

KVKK m. 11'in ilk dört bendindeki haklar ilgili kişinin kişisel verilerin işlenmesi hakkında bilgi talep etmesini içermektedir. Dolayısıyla, bilgi almak amacıyla yapılan başvuruda, idareden, idari davaya konu olabilecek bir işlem veya eylemin yapılması istenmediğinden başvuru İdari Yargılama Usulü Kanunu (İYUK) m. 10 kapsamında değerlendirilemeyecektir. Başvuru, Anayasa'da düzenlenen bilgi edinme hakkının bir kullanımı olarak kabul edilmelidir¹²⁹. Ancak, KVKK uyarınca yapılan başvuru 4982 sayılı Bilgi Edinme Hakkı Kanunu (BEHK) kapsamındaki başvuruya benzer bir nitelik taşısa da bu kanun kapsamında değerlendirilmemelidir. Zira, KVKK özel kanun niteliği taşımakta ve BEHK uyarınca sadece idareye başvurulabilirken, KVKK kapsamındaki başvurunun muhatabının idare olması gibi bir zorunluluk bulunmamaktadır¹³⁰. Uygulamada sorun yaratabilecek bir husus, başvurunun KVKK kapsamında yapıldığının belirtilmemesidir. Bilgi Edinme Hakkı

¹²⁸Bkz. Kişisel Verileri Koruma Kurumu, İlgili Kişinin Hak Arama Yöntemleri, s.3 (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df-4c91-b08e-b4f0991a80f4.pdf>, Erişim Tarihi: 17.06.2023); Us Doğan, E.: *Başvuru ve Şikayet Usulleri ile Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü*, iç. Kişisel Verilerin Korunmasına Akademik Bakış - KVKK Akademi Derleme Çalışması (ed. Aksoy, Pınar Çağlayan/ Aksoy, Hüseyin Can), Ankara 2023, s. 213.

¹²⁹ Anayasa m. 74:“(4): Herkes, bilgi edinme ve kamu denetçisine başvurma hakkına sahiptir.”

¹³⁰ Us Doğan, s. 220.

Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik m. 9/5 uyarınca “*Başka bir kanun uyarınca yapıldığı belirtilmeyen başvurular, Bilgi Edinme Hakkı Kanunu kapsamında yapılmış sayılır*”. Bu sebeple, KVKK kapsamında yapıldığı belirtilmeyen başvuruların Kurul tarafından, şikâyet yolu için aranan ön koşul olarak kabul edilip edilmeyeceği konusunda bir belirsizlik bulunmaktadır. Katıldığımız görüşe göre, başvurunun VSBT’de düzenlenen şartları sağlaması halinde ilgili kişinin yaptığı başvurunun KVKK kapsamında değerlendirilmesi gerekmektedir¹³¹.

Başvurunun reddi halinde dava açılmasını düzenleyen bir hüküm bulunmadığından bilgi edinme talebiyle yapılan başvurunun iptal davasına konu edilip edilemeyeceği tartışmalı olsa da¹³² Saygı’ya göre BEHK kapsamındaki başvurulara benzerliği nedeniyle veri sorumlusuna bilgi edinmek için yapılan başvuruların reddi iptal davasına konu olabilmelidir¹³³.

Bu kapsamda, örneğin, Köln Yüksek Eyalet Mahkemesi 2022 yılında verdiği bir kararda veri sorumlusuna bilgi edinmek için yapılan başvurunun süresi içerisinde cevaplanmamasını tazminat bakımından değerlendirmiş ve ilgili kişinin bilgi talep etme hakkının ihlal edilmesini yani GDPR’ın getirdiği bir yükümlülüğe uymamayı başlı başına bir tazminat sebebi olarak kabul etmiştir¹³⁴. Ancak, ABAD 04.05.2023 tarihli kararında GDPR’ın ihlal edilmesinin başlı başına bir tazminat sebebi olamayacağına hükmetmiştir¹³⁵.

¹³¹ Us Doğan, s. 220.

¹³² Us Doğan, s. 227.

¹³³ Saygı, s. 40.

¹³⁴ Çekin/Berktaş/Akıncı, s. 269.

¹³⁵ ABAD, C-300/21, 04.05.2023, Österreichische Post- Préjudice moral lié au traitement de données personnelles, (<https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=175085>, Erişim Tarihi: 17.06.2023).

Veri sorumlusuna yapılan başvuru sadece bilgi alma talepleri yanında verilerin silinmesi veya yanlış işlenen kişisel verilerin düzeltilmesi gibi birtakım talepleri de içerebilmektedir. Bu durumda teorik olarak İYUK m. 10 veya m. 11 hükümleri uygulama alanı bulabilecektir. İlgili kişinin hakkında idari davaya konu olabilecek bir idari işlem veya eylem yapılmasını talep ettiği durumlarda İYUK m. 10 kapsamında bir başvuru gündeme gelecektir. Verilerin korunması hakkında yapılan talepler veya kişisel verilerinin silindiğinin/düzeltilindiğinin 3. kişilere duyurulması yönündeki talepler bu kapsamda değerlendirilebilecektir. Uygulamada ortaya çıkabilecek bir diğer durum ise başvurunun İYUK m. 11 kapsamında olmasıdır. Ancak, veri sorumlusu idareye yapılan başvurunun İYUK m. 11 kapsamında olması pratik olarak daha zor bir ihtimaldir. Zira, bunun için maddede sayılan şartların sağlanması gerekmektedir. Bu cümleden olarak, ilgili kişi hakkında daha önceden bir idari işlem olması; talebin işlemin değiştirilmesi, kaldırılması veya yeni bir işlem tesisi yönünde olması ve bu talebin üst makama, üst makam yoksa işlemi yapmış olan makama yöneltilmesi gerekmektedir¹³⁶. KVKK m. 13 kapsamındaki başvurular veri sorumlusu olan idareye yapıldığından dolayı üst makama yapılan başvuruların bu kapsamda değerlendirilemeyeceği belirtmek gerekir.

Veri sorumlusuna tazminat talebiyle bir başvuru yapılması durumunda ise, idari eylemler dolayısıyla zarar görenlerin tam yargı davası açmasını düzenleyen İYUK m. 13 kapsamında bir başvuru gündeme gelebilecektir. İlgili madde uyarınca, zarara uğrayan kişiler zararın öğrenildiği tarihten itibaren bir ve herhalde eylem tarihinden itibaren beş yıl içerisinde idareye başvurarak zararın tazminini istemeli, yani bir ön karar almalıdır. İstemin kısmen veya tamamen reddi durumunda bu konudaki işlemin

¹³⁶ Saygı, s. 40-41; Eser Us, s. 224-225.

tebliğini izleyen günden veya istek hakkında otuz gün içinde cevap verilmediği takdirde bu sürenin bittiği tarihten itibaren, süresi içinde dava açılmalıdır. *Saygı*’nın görüşüne paralel biçimde, kanımızca da zarar bir idari eylem sonucunda ortaya çıkmışsa, veri sorumlusu idareye yapılan başvurunun İYUK m. 13 kapsamındaki bir başvuru olarak kabul edilerek dava açma süresini başlatması gerekmektedir¹³⁷. Aksi bir kabul, KVKK kapsamında tazminat başvurusu reddedilen kişinin İYUK kapsamında aynı taleple aynı idareye tekrar başvurması gibi bir durum ortaya çıkartacaktır.

Veri sorumlusuna başvuru yolunun kullanılmasının ardından ise başvurunun hukuki niteliği ne olursa olsun, KVKK m. 14 uyarınca yargı dışı başvuru yollarının ikinci aşaması olan Kurul’a şikâyet yoluna gidilebilmektedir. KVKK m. 15 uyarınca Kurul tarafından 60 gün içerisinde cevap verilmemesi halinde başvuru reddedilmiş sayılmaktadır. Kurul inceleme sonucunda bir ihlal tespit ederse hukuka aykırılığın veri sorumlusu tarafından giderilmesine karar verir. Bu bağlamda, Kurul’un tazminat talepleriyle ilgili başvuruları kabul etme yetkisi bulunmamaktadır. Kurul sadece hukuka aykırılıkları değerlendirip bunların giderilmesine hükmedebilir¹³⁸. İdare hukuku açısından dikkat edilmesi gereken nokta ise Kurul’a yapılan şikâyetin dava açma süresini durdurmamasıdır. Veri sorumlusuna yapılan başvuru ardından dava açma süresi başlayan durumlarda ilgili kişilerin şikâyetle cevabı beklemeden süresi içerisinde dava açması gerekmektedir. Kurul’a şikâyetin İYUK m. 11 kapsamında değerlendirip, dava açma süresini durduracağını ileri süren yazarlar olmakla beraber¹³⁹, kanımızca İYUK. m. 11 kapsamında üst makama, üst makam yoksa işlemi

¹³⁷ Saygı, s. 41.

¹³⁸ Altındağ, s. 399.

¹³⁹ Us Doğan, s. 232.

yapmış olan makama başvurulması gerektiğinden Kurul’a yapılan başvurular bu kapsamda değerlendirilemeyecektir. Ancak, şikâyet üzerine verilecek Kurul kararları da idari karar niteliğinde olduğundan, verilen kararlara karşı idare mahkemelerinde dava açılabilmesi mümkündür¹⁴⁰. Bu bağlamda, şikâyet yolunun idari dava açma süresini durdurmamasının pratik bir sonucu bulunmamaktadır. Zira, dava açmak yerine şikâyet yolunu tercih eden ilgililer, dava süresini kaçırmış olsalar dahi, Kurul kararına karşı 60 gün içerisinde dava açabileceklerdir.

V. KVKK İstisna Hükümleri

KVKK m. 28’de tam ve kısmi istisna hükümleri düzenlenmektedir. Bu bağlamda, Kanun koyucu bazı konulardaki veri işleme faaliyetlerini tamamen KVKK’daki koruma kapsamı dışında bırakmış bazı faaliyetleri de KVKK’nın belirli hükümlerinden muaf tutmuştur.

İdare açısından önemli olabilecek tam istisnalar “*Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi*” ile “*Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen*

¹⁴⁰ Kişisel Verileri Koruma Kurumu: *Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı*, s.5

(<https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20KORUNMASINA%20İLİŞKİN%20BAŞVURU%20VE%20ŞİKÂYET%20HAKKI.pdf>, Erişim Tarihi: 17.06.2023).

önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi” halleridir. Bu veri işleme faaliyetlerine KVKK’nın hiçbir maddesi uygulanmamaktadır.

İdare açısından önemli olabilecek kısmî istisna halleri ise “*Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*” ile “*Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması*”dır. Kısmî istisna durumlarında aydınlatma yükümlülüğü, ilgili kişinin hakları (tazminat talepleri hariç) ve veri sorumluları siciline kayıt yükümlülüğüne ilişkin düzenlemeler uygulanmamaktadır.

Benzer istisnalar sadece bizim mevzuatımıza özgü olmayıp hem GDPR’da¹⁴¹ hem de 108 sayılı Sözleşme’de de yer almaktadır¹⁴². Ancak, tam istisna halleri kapsamındaki veri işleme faaliyetlerinin KVKK’daki korumadan muaf olması veri işleyen idarenin hiçbir kısıtlamaya tabi olmayacağı anlamına gelmemektedir. Belirttiğimiz üzere kişisel verilerin korunması Anayasa’da özel hayatın gizliliği kapsamında düzenlenen bir haktır. Bu bağlamda, Anayasa m. 13 uyarınca bu hakka yapılan sınırlamalar hakkın özüne “*(...) dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz*”.

¹⁴¹ GDPR, m. 23.

¹⁴² Bkz. 108 sayılı Sözleşme m. 3-9 ve beyanları.

İKİNCİ BÖLÜM

KAMU HİZMETİ KAPSAMINDA VERİ İŞLENMESİ

I. Kamu Hizmeti

A. Kamu Hizmeti Kavramı ve Unsurları

1. Kamu Hizmeti Kavramı

Kamu hizmeti, idare hukukunun temel kavramlarından olup; idarenin faaliyet alanının tespit edilmesine yardımcı olmaktadır¹⁴³. Kamu hizmeti, idare hukukunun kapsamının alanını ve idari yargının görev alanının tespit edilmesi bakımından ölçüt olarak kabul edilmesine rağmen; söz konusu kavramın yasal düzenlemelerde, yargı kararlarında veya doktrinde üzerine anlaşılmış bir tanımı bulunmamaktadır¹⁴⁴. Doktrinde bu durumun, yasa koyucunun kavramı tanımlamaya ihtiyaç duymaması; yargı organlarının kavramı net bir şekilde tanımlayarak değerlendirme serbestliğini

¹⁴³ Gözübüyük/Tan, s. 557.

¹⁴⁴ Gözübüyük/Tan, s. 558.

yitirmek istememesi; doktrinin ise kavramı tanımlama çabasının başarısız olmasından kaynaklandığını belirtilmektedir¹⁴⁵.

Kamu hizmeti, net bir tanımı olmamakla birlikte, farklı anlamlarda kullanılan bir kavramdır. Söz konusu kavram, faaliyet, iş, uğraş gibi anlamlara gelecek şekilde kullanılabilirken¹⁴⁶; bu faaliyeti yerine getiren kamu kuruluşları anlamında da kullanılabilmektedir¹⁴⁷. Doktrinde, bazı yazarlar; kamu hizmetinin, ilk tür anlama gelmesi durumunda ‘*maddi anlamda/fonksiyonel anlamda kamu hizmeti*’; ikinci tür anlama gelmesi durumunda ‘*organik anlamda kamu hizmeti*’ kavramlarının kastedildiğini savunmaktadır¹⁴⁸.

Doktrinde, kavrama ilişkin yapılan bir tanımlama; “(...) idarenin toplumun ortak bazı gereksinmelerini karşılamak amacıyla doğrudan veya yakın gözetimi ve sorumluluğu altında, kamusal yetki ve usuller kullanarak yürüttüğü faaliyet” şeklindedir¹⁴⁹. Başka bir tanımlama; “Kamu hizmeti, bir kamu tüzel kişisi tarafından üstlenilen ve doğrudan doğruya onun tarafından veya onun görevlendirmesi ve denetimi altında bir özel kişi tarafından yürütülen kamu yararı amacına yönelik faaliyetlerdir.” ifadeleriyle yapılmaktadır¹⁵⁰. Diğer bir tanımlama; “Siyasal organlar tarafından kamuya yararlı olarak kabul edilen, bir kamu kuruluşunun ya kendisi ya da yakın denetimi ve gözetimi altında özel kesim tarafından yürütülen faaliyetlerdir”

¹⁴⁵ Gözübüyük/Tan, s. 558; Akyılmaz,./ Sezginer/ Kaya,, s. 585.

¹⁴⁶ Bu duruma örnek olarak; Anayasa m. 128: ‘Devletin, kamu iktisadî teşebbüsleri ve diğer kamu tüzelkişilerinin genel idare esaslarına göre yürütmekle yükümlü oldukları kamu hizmetlerinin gerektirdiği aslî ve sürekli görevler, memurlar ve diğer kamu görevlileri eliyle görülür.’

¹⁴⁷ Bu duruma örnek olarak; Anayasa m. 70: ‘Her Türk, kamu hizmetlerine girme hakkına sahiptir.’

¹⁴⁸ Gözler, K. /Kaplan, G.: İdare Hukuku Dersleri, Güncellenmiş 22. Baskı, Bursa 2020, s. 476; Günday, M.: İdare Hukuku, 11. Baskı, Ankara 2017.

s. 330; Akyılmaz/Sezginer/Kaya, s. 585

¹⁴⁹ Gözübüyük/ Tan, s. 561.

¹⁵⁰ Gözler, K. /Kaplan, G.: İdare Hukuku Dersleri, Güncellenmiş 22. Baskı, Bursa 2020, s. 477.

biçimindedir¹⁵¹. Ayrıca, “(...) kamu hizmeti, yasama organınca kamu hizmeti olarak nitelendirilen idare ya da onun denetim ve gözetimi altında özel kişilerce, kamu yararı amacıyla, toplumun ortak ve genel ihtiyaçlarını tatmin için yapılan faaliyete verilen isimdir.” şeklinde de ifade edilmektedir¹⁵².

2. Kamu Hizmetinin Unsurları

Kamu hizmeti, doktrindeki çoğunluk tarafından, üç unsura ayrılarak incelenmektedir¹⁵³. Bu unsurlar; organik unsur, maddi unsur ve biçimsel unsur/hukuki rejim şeklindedir. Buna karşılık, bazı yazarlar; biçimsel unsuru kamu hizmetinin unsurlarından biri olarak kabul etmemektedir¹⁵⁴. Ayrıca, söz konusu unsurların birbirinin alternatifi olmadığı; yani, kamu hizmetinin varlığının kabulü için bu unsurların hep birlikte/kümülatif şekilde bulunması gerektiği belirtilmelidir¹⁵⁵.

Kamu hizmetinin organik unsuru, kamu hizmeti faaliyetinin doğrudan idare tarafından veya onun görevlendirdiği özel hukuk kişisi tarafından yerine getirilmesini ifade etmektedir¹⁵⁶. Zamanla farklı hukuki rejimler geliştirerek özel kişilerin kamu hizmeti ile görevlendirilmeleri artsa da hizmetin asli sahibi niteliğine idarenin haiz olduğu belirtilmelidir¹⁵⁷. Bu konu, Danıştay’ın bir kararında; “Anayasa ve Yasada kamu hizmeti olduğu belirtilen bir hizmetin, özel hukuk hükümlerine tabi gerçek veya

¹⁵¹ Günday, s. 332.

¹⁵² Akyılmaz/Sezginer/Kaya, s. 586.

¹⁵³ Gözübüyük/Tan, s. 561.

¹⁵⁴ Gözler/Kaplan, s. 477, 482.

¹⁵⁵ Gözler/Kaplan, s. 477.

¹⁵⁶ Gözler/Kaplan, s. 480.

¹⁵⁷ Gözübüyük/Tan, s. 561.

tüzel kişilerince veyahutta bunların çalışanlarınca görülmesi, bu kişilerce görülen hizmetin, kamu hizmeti olduğu gerçeğini değiştirmeyeceği gibi, kamu hizmeti gören kişinin kamu hizmeti görevlisi kabul edilmesine de bir engel oluşturmamaktadır.” ifadeleriyle belirtilmektedir¹⁵⁸. AYM de benzer şekilde, kamu hizmetinin idare kuruluşları tarafından görülmesinin şart olmadığını; özel kişiler tarafından da gerçekleştirilebileceğini ifade etmektedir¹⁵⁹.

Kamu hizmetinin maddi unsuru, kamu hizmeti faaliyetinin niteliğine ilişkin bir husustur. Doktrinde, kamu hizmeti faaliyetlerinin toplunun ortak ihtiyaçlarını gidermeye yönelik olduğu ve fakat hangi faaliyetlerin nitelikleri gereği bu tür faaliyetlerden kabul edilebileceğini belirlemenin olanaksız olduğu ifade edilmektedir¹⁶⁰. Doktrinde, niteliği gereği bir faaliyeti kamu hizmeti saymanın mümkün olmadığı; bu nitelemenin hizmeti görenlerin iradesine bağlı yapılabileceği ifade edilmektedir¹⁶¹. Bu sebeple, her türlü sosyal faaliyetin, kamu hizmetini belirlemeye yetkili kamu otoritesi olarak yasama organının iradesine bağlı olarak kamu hizmeti niteliğine haiz olabileceği savunulmaktadır¹⁶².

AYM, birçok kararında, niteliği gereği kamu hizmeti sayılan faaliyetlere ilişkin genel bir tanım vermeye çalışmaktadır. Bu kararlara göre; *“kişilerin su, elektrik, havagazı gibi ihtiyaçlarının karşılanması”*¹⁶³, *“elektrik üretimi, iletimi ve dağıtımı ile ilgili etkinlikler”*¹⁶⁴, *“sağlık hizmeti”*¹⁶⁵, *“eğitim ve öğretim hizmeti”*¹⁶⁶, *“radyo-*

¹⁵⁸ Dan. 10. D, T. 15.9.2009, E. 2009/11303 K. 2009/8021, (Lexpera).

¹⁵⁹ AYM, T. 12.4.1990, E. 990/4, K. 990/6 (Anayasa Mahkemesi Kararlar Dergisi 1990, C. I, S. 26, s. 135); Bu konuda bkz. Akyılmaz/Sezginer/Kaya, s. 586.

¹⁶⁰ Gözübüyük/Tan, s. 561.

¹⁶¹ Gözübüyük/Tan, s. 562.

¹⁶² Gözübüyük/Tan, s. 562.

¹⁶³ AYM, T. 26.03.1974, E. 973/32, K. 974/11, (Anayasa Mahkemesi Kararlar Dergisi, S. 12, s. 122 vd.)

¹⁶⁴ AYM, T. 09.12.1995, E.994/43, K.994/42-2, R.G.: 20.03.1996, S. 22586.

¹⁶⁵ AYM, T. 19.04.1988, E.987/16, K.988/8, R.G.: 23.08.1988, S. 19908.

¹⁶⁶ AYM, T. 12.04.1990, E.990/4, K.990/6, R.G.: 17.06.1990, S.20551.

televizyon yayını”¹⁶⁷ gibi faaliyetler, AYM tarafından kamu hizmeti niteliğinde kabul edilmektedir. AYM, bir kararında; “(...) *kamusal ihtiyaçların gerekli kıldığı hallerde yasama organı, herhangi bir alanı yasal statü içine alarak bir kamu hizmeti tahsis edebilir.*” ifadeleriyle kamu hizmetini belirleme yetkisinin yasama organına ait olduğunu belirtmektedir¹⁶⁸. Bunun yanı sıra, kamu hizmetini belirleme yetkisi, bazı durumlarda idareye de verilebilmektedir¹⁶⁹. Kamu hizmetinin maddi unsurunu açıklamaya çalışan görüşlerden bir diğeri, kamu faaliyetinin kamu yararı amacı gütmesi gerektiğini ifade etmektedir¹⁷⁰. Bu görüşe göre, sadece kamu yararı amacına yönelik faaliyetler kamu tüzel kişileri tarafından yerine getirilerek kamu hizmeti biçiminde görülebilir. Ayrıca, kamu yararı amacı bulunmayan ve kamu tüzel kişilerinin özel yararına yönelik yapılan faaliyetler, kamu hizmeti olarak kabul edilemez¹⁷¹.

Kamu hizmetinin biçimsel unsuru, kamu hizmetinin hukuki rejimine ilişkin bir unsurdur. Kamu hizmeti, kamusal yönetim biçimine göre yürütülen bir faaliyet olup; böylece, idare hukukunun uygulama alanının belirlenmesinde kullanılan bir ölçüttür. AYM kararlarında, kamu hizmetinin hukuki rejimi ile idare hukuku arasında mutlak bir bağ kurarken¹⁷²; Danıştay ve Uyuşmazlık Mahkemesi kararlarında, kamu hizmetlerinin hukuki rejiminin bu kavramın zamanla gelişmesiyle birlikte değiştiğini ve idare hukuku ile arasında eşlik olduğunun kabul edilemeyeceğini ifade etmektedir¹⁷³. Kamu hizmetlerinin hukuki rejiminin değişmesi, kavramın “*idari kamu*

¹⁶⁷ AYM, T. 18.05.1990, E.989/9, K.990/8, R.G.: 26.07.1990, S. 20586.

¹⁶⁸ AYM, T. 26.11.1985, E.985/2, K.985/22, R.G.: 21.01.1986, S. 18995.

¹⁶⁹ Gözübüyük/Tan, s. 563.

¹⁷⁰ Gözler/Kaplan, s. 478.

¹⁷¹ Gözler/Kaplan, s. 479.

¹⁷² AYM, T. 25.05.1976, E.976/1, K.976/38, (Gözübüyük/Tan, s. 563).

¹⁷³ AYM, T. 21.01.1971, E.969/33, K.971/7, (Gözübüyük/Tan, s. 564); AYM, T. 23-25.10.1969, E.967/41, K.969/57, (Gözübüyük/Tan, s. 564); Uyuşmazlık Mahkemesi, 26.10.1992, E.992/33, K.992/36, (Gözübüyük/Tan, s. 564).

hizmeti”, “*endüstriyel kamu hizmeti*” ve “*kamu hizmeti olmaya yatkın hizmet*” gibi çeşitlenmesine sebep olmaktadır. Doktrinde, bu durumunun idare hukukunda yapısal esnekliği desteklediği ifade edilmektedir¹⁷⁴.

B. Kamu Hizmetinin Genel İlkeleri

Kamu hizmetlerinin görülmesi, yerine getirilme şekline bağlı olmaksızın birtakım ilkelere tabidir. Kamu hizmetinin genel ilkeleri olarak adlandırılan bu ilkeler; süreklilik, eşitlik, değişkenlik ve uyum olarak sıralanabilir. Doktrinde, zamanla kamu hizmeti ilkelerine şeffaflık, basitlik, katılma, sorumluluk ve ulaşılabilirlik gibi bazı ilkelerin de eklendiği savunulmaktadır¹⁷⁵. Kamu hizmetinin genel ilkeleri her ne kadar içtihatlar ile geliştirilmiş olsa da bu ilkeler hukuki düzenlemelerde de yer almaktadır¹⁷⁶.

Süreklilik ilkesi, bir diğer deyişle devamlılık ilkesi, toplumun ortak ihtiyaçlarını gidermeye yönelik olan kamu hizmetlerinin, sürekli ve düzenli bir şekilde yerine getirilmesini ifade eder¹⁷⁷. Kamu faaliyetleri düzenli ve sürekli bir biçimde görülmediği takdirde, kamunun ihtiyaçları karşılamaz ve kamu yararına hizmet edilemez¹⁷⁸. Süreklilik ilkesinin, eşitlik ilkesi ile bir bağı da kamu hizmetlerinin

¹⁷⁴ Gözübüyük/Tan, s. 564.

¹⁷⁵ Gözübüyük/Tan, s. 568; Akyılmaz/Sezginer/Kaya, s. 587; Günday, s. 334-337.

¹⁷⁶ Örnekler için bkz: Gözübüyük/Tan, s. 574.

¹⁷⁷ Gözler/Kaplan, s. 487; Akyılmaz/Sezginer/Kaya, s. 587-588.

¹⁷⁸ Günday, s. 334.

coğrafi sürekliliğine işaret etmektedir¹⁷⁹. Belirtilmesi gerekir ki, süreklilik ifadesi kesintisizliği değil; hizmetlerin devamlılığını ve düzenliliğini ifade etmektedir¹⁸⁰.

Değişkenlik ve uyum ilkesi; süreklilik ilkesinden kaynaklanmakta olup, kamu hizmetlerinin gelişen teknolojiye, değişen koşullara ve toplumun ihtiyacına uygun olarak yerine getirilmesi anlamına gelmektedir¹⁸¹. Doktrinde bazı yazarlar tarafından uyarlama ilkesi olarak da adlandırılan bu ilke, kamu hizmetinin zamanın ihtiyaç ve koşullarına göre en uygun ve iyi şekilde görülmesini ifade etmektedir¹⁸². Kanaatimizce, değişkenlik ilkesi, kazanılmış haklar ile çatışmamakta; aksine kamu hizmetlerinin örgütlenme ve işleyişinin, bu hizmetlerden yararlananlar için uyumlaştırılmasına fayda sağlamaktadır. Nitekim doktrinde belirtildiği üzere; kamu hizmetlerinde geçerli olan değişim ilkesi, idarenin takdir yetkisinin sebeplerindendir ve böylece, idare kamu hizmetlerini ihtiyaçlara ve gelişmelere uyarlayabilir¹⁸³.

Eşitlik ilkesi; idarenin kamu hizmetini, eşit konumdaki kişilere eşit ve farklı konumdaki kişilere farklı şekilde sunması gerektiğini ifade etmekte olup, bu hususta idarenin somut koşullara göre eşitlik kurması gerektiğini, yani idarenin hizmet sunmak konusunda mutlak bir eşitlik değil, adil bir eşitlik kurması gerektiğini belirtmektedir¹⁸⁴. Nesnellik ilkesi olarak da adlandırılan bu ilke, idarenin kamu hizmetlerini görürken bireysel değil; kamu yararını gözeterek objektif davranma gerekliliğini ifade etmektedir¹⁸⁵. Doktrinde söz konusu ilkenin, Anayasa'nın 10.

¹⁷⁹ Gözübüyük/Tan, s. 568.

¹⁸⁰ Günday, s. 334; Gözler/Kaplan, s. 488.

¹⁸¹ Gözübüyük/Tan, s. 571; Gözler/Kaplan, s. 489; Akyılmaz/Sezginer/Kaya, s. 587-588.

¹⁸² Günday, s. 335.

¹⁸³ Günday, s. 335.

¹⁸⁴ Gözübüyük/Tan, s. 572-573; Akyılmaz/Sezginer/Kaya, s. 557.

¹⁸⁵ Günday, s. 336.

maddesinde düzenlenen kanun önünde eşitlik ilkesinden kaynaklandığı savunulmaktadır¹⁸⁶.

Söz konusu ilkelerin yanı sıra, eşitlik ilkesinden kaynaklanan bir ilke daha bulunmaktadır. Tarafsızlık ilkesi olarak adlandırılan bu ilke, ayrımcılık yapmama ve çoğulculuğa saygı gösterme unsurlarını içinde barındırmaktadır¹⁸⁷.

II. İdarenin Veri İşleme Uygulamaları

A. Genel Olarak İdarenin Veri Kullanımı ve Büyük Veri

Günümüze kadar küresel olarak oluşturulan, yakalanan, kopyalanan ve tüketilen toplam veri miktarı katlanarak artmış ve 2022 yılında global ölçekteki toplam veri hacmi 97 zettabayt boyutuna ulaşmıştır. Önümüzdeki 3 yıl içinde ise bu sayının 181 zettabayta ulaşacağı öngörülmektedir¹⁸⁸. Hemen hemen her cihazın çevrimiçi olmaya başladığı, internette sunulan ve tüketilen veri hacminin kat kat arttığı ve veri akışının sürekli olduğu bu çağda, bilgiyi etkili bir şekilde yönetme ve anlama yeteneği çoğu kuruluşun piyasada kalabilmesi ve diğer aktörlerle rekabet edebilmesi için

¹⁸⁶ Gözler/Kaplan, s. 489; Akyılmaz/Sezginer/Kaya, s. 557.

¹⁸⁷ Gözübüyük/Tan, s. 574; Gözler/Kaplan, s. 490.

¹⁸⁸ Söz konusu istatistik için bkz. Taylor, P.: *Amount of data Created, Consumed, and Stored 2010-2020, with Forecasts to 2025 (Veri Kümesi)*”, Statista (<https://www.statista.com/statistics/871513/worldwide-data-created/>, Erişim Tarihi: 17.06.2023).

zorunlu bir unsur olarak değerlendirilmektedir¹⁸⁹. Zira, bilgi toplumunun dinamik gelişimi ve daha kaliteli hizmet ve ürünlere yönelik artan talep, dijital ekonominin hayatın çeşitli alanlarında yaygın bir şekilde gelişmesine neden olmuştur¹⁹⁰. Veri miktarının ve dijital teknolojilerin hızla gelişmesi sadece özel sektör için değil, kamu için de büyük değişimlere gebe dir. İdarenin kamu yararı amacıyla en doğru kararı alması ve eylemlerde bulunması, doğru zamanda doğru bilgilere sahip olması ve bu bilgileri doğru bir şekilde kullanabilmesi halinde mümkündür. Yaşlanan nüfus, artan eşitsizlik ve iklim değişikliği gibi uzun vadeli sorunların yanı sıra göç ve güvenlik gibi konuların öngörülemeyen zorlukları da vatandaşların refahını etkilemektedir. Bu da hükümetlerin uzun vadeli vizyon geliştirmelerini, kanıta dayalı yatırım yapmalarını¹⁹¹ ve eylemlerini koordine etmelerini gerektirmektedir. Hükümetler, verilerin daha iyi kullanılmasının bu zorluklara nasıl yanıt verilebileceğini ve aynı zamanda politika ve hizmetlerin verimliliğini, performansını ve kapsayıcılığını nasıl artırabileceğinin giderek daha fazla farkına varmaktadır¹⁹². İdarenin her gün gerçekleştirdiği trafik verilerini işlemek, sosyal yardımları yönetmek, vergi toplamak, ulusal sağlık ve eğitim sistemlerini izlemek gibi eylem ve işlemleri çok büyük miktarda veri üretilmesini ve toplanmasını sağlamaktadır. İdarenin elindeki bu bilgiler, kamu kurumlarının ilgilenmeleri gereken alanları belirlemesine, daha hızlı ve daha bilinçli kararlar

¹⁸⁹ Cavanillas, J. M./ Curry, E./ Wahlster, W.: *The Big Data Value Opportunity*, iç. New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe (ed. Cavanillas, José María/ Curry, Edward/ Wahlster, Wolfgang), New York 2016, s. 3.

¹⁹⁰ Zakrzewska, M/ Ireneusz M.: *Using E-government Services and Ensuring the Protection of Sensitive Data in EU Member Countries*, Procedia Computer Science 2021, C. CXCI, s. 3459.

¹⁹¹ Kanıta dayalı yatırım araştırmalara ve geçmiş verilere dayanarak karar verme sürecidir. Kısa vadeli piyasa trendlerine veya mevcut iklime bakmak yerine, piyasaların uzun vadeli gözlemine dayanan bir yaklaşımdır. Bkz: Hinton Jones, N.: *Evidence-based investing: What it is and Why It's Awesome*, 2022, (<https://www.timeline.co/blog/evidence-based-investing-what-it-is-and-why-it-awesome#:~:text=What%20is%20evidence-based%20investing,long-term%20observation%20of%20markets>, Erişim Tarihi: 17.06.2023).

¹⁹² Welby, B./ Ubaldi B./ van Oijen, C.: *A Data-driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance*, OECD Working Papers on Public Governance No: 33 2019, s. 6 (<https://doi.org/10.1787/09ab162c-en> Erişim Tarihi: 17.06.2023).

almalarına ve gerekli deęişiklikleri uygulamalarına olanak tanımaktadır¹⁹³. Örneęin, Amerika Birleşik Devletleri (ABD) veri analizini, gelecekte oluşabilecek grip salgınlarını tahmin edebilmek için kullanmaktadır. Bu sayede idare grip salgını sırasında hastaneye yatışlardaki artışlar gibi oluşacak deęişikliklere hazırlanabilmektedir¹⁹⁴. Kanımızca, böyle bir uygulamanın kamu kaynaklarının daha etkili ve verimli bir şekilde kullanımını sağlayarak dięer önceliklerin ele alınmasına olanak tanıdığı açıktır.

Bu noktada idarenin hangi tür verileri kullandığına değinilmesi gerekmektedir. İdarenin kullandığı veriler birçok farklı kaynaktan gelmekte ve birçok farklı şekilde elde edilmektedir. Kamu kuruluşları, vatandaşlar, işletmeler, araştırmacılar ve dięer toplumsal paydaşların hepsi, bilerek veya bilmeyerek, açık veya kapalı formatlarda, büyük veya küçük miktarlarda, yapılı veya yapısız, kişisel veya kişisel olmayan nitelikte veri üretimine katkıda bulunmaktadır¹⁹⁵. Verilerin kaynağı ve türü çok çeşitli olmakla beraber bu çalışmada idarenin veri işleme uygulamalarından bahsederken verilerle ilgili dört özelliğe yoğunlaşılmaktadır: Kişisel-kişisel olmayan veriler, açık veri ve büyük veri. Kişisel-kişisel olmayan veri ile açık veri kavramları çalışmanın ilgili yerlerinde açıklanmış olmakla beraber büyük veri tanımına değinmekte yarar vardır.

¹⁹³ Sahu, M: *Big Data in the Public Sector: Applications and Benefits*. Analyticssteps, 2021, (<https://www.analyticssteps.com/blogs/big-data-public-sector-applications-and-benefits> Erişim Tarihi: 15.01.2023).

¹⁹⁴ İlgili haber için bkz. CDC: *About CDC's Flu Forecasting Efforts*, Centres For Disease Control And Prevention (<https://www.cdc.gov/flu/weekly/flusight/how-flu-forecasting.htm>, Erişim Tarihi: 04.06.2023).

¹⁹⁵ Welby/ Ubaldi/van Oijen, s. 12.

Büyük verinin doktrinde kesin kabul görmüş bir tanımı yapılamamış olsa da¹⁹⁶ bazı özelliklerine yönelik fikir birliği bulunmaktadır¹⁹⁷. Büyük veriyi diğer verilerden ayırmak için kullanılan üç özellik; hacim, hız ve çeşitlilik¹⁹⁸. Bazı yazarlar bu üç özelliğin yanına değişkenlik ve karmaşıklık unsurlarını da eklemektedir¹⁹⁹. Büyük veri kişisel veri içerebileceği gibi tamamen kişisel olmayan verilerden de oluşabilmektedir²⁰⁰. Bunun yanı sıra, büyük veri idarenin veri işleme uygulamaları bağlamında çalışmada ele alınacak tüm veri işleme yöntemleriyle bağlantılıdır. Zira, küçük veri setleri değerli olsa da veri işleme faaliyetlerinden beklenen faydayı sağlamak ve veriden değer elde etmek için büyük veriye ihtiyaç duyulmaktadır²⁰¹. Bu bağlamda, çalışmada incelenen idarenin veri işleme uygulamalarının büyük veriyi de içerdiği göz önünde bulundurulmalıdır. Büyük verinin özellikleri ve teknik yönü bu

¹⁹⁶ Büyük verinin ilk tanımlarından birinde büyük veri üçlü bir perspektifle tanımlanmıştır. Buna göre, “Büyük veri, gelişmiş karar verme, içgörü keşfi ve süreç optimizasyonu sağlamak için yeni işleme biçimleri gerektiren yüksek hacimli, yüksek hızlı ve/veya yüksek çeşitlilikte bilgi varlıklarıdır. Başka yazarlarsa büyük veriyi “büyüklüğü bizi o anda yaygın olan denenmiş ve doğru yöntemlerin ötesine bakmaya zorlayan veri” olarak tanımlamıştır. Bkz.: Curry, E.: *The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches*, iç. New Horizons for a Data-Driven Economy (ed. Cavanillas, José María/ Curry, Edward/ Wahlster, Wolfgang), New York, 2016, s. 30; Madde 29 çalışma grubu da büyük veriyi şu şekilde tanımlamıştır: Büyük veri, şirketler, hükümetler ve diğer büyük kuruluşlar tarafından tutulan ve daha sonra bilgisayar algoritmaları kullanılarak kapsamlı bir şekilde analiz edilen devasa dijital veri kümelerini ifade eder. Büyük veri, daha genel eğilimleri ve korelasyonları tespit etmek için kullanılabilir gibi, bireyleri doğrudan etkilemek amacıyla da işlenebilir. Bkz.: Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, 2013, s. 35, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, Erişim Tarihi: 11.07.2023)

¹⁹⁷ Desouza, K. C./ Jacob, B.: *Big Data in the Public Sector: Lessons for Practitioners and Scholars*, Administration & Society 2014, C. XLIX, S. 7, s. 1045.

¹⁹⁸ -Hacim (veri miktarı): veri işlemede büyük ölçekli verilerle ilgilenme (örn. Küresel Tedarik Zincirleri, Küresel Finansal Analiz).

- Hız (veri hızı): Yüksek frekansta gelen gerçek zamanlı veri akışlarıyla ilgilenme (örn. Sensörler, Yaygın Ortamlar, Elektronik Ticaret, Nesnelerin İnterneti).

- Çeşitlilik (veri türleri/kaynakları aralığı): Farklı sözdizimsel formatlar (ör. Elektronik Tablolar, XML, DBMS), şemalar ve anlamlar kullanan verilerle ilgilenme. Bkz: Curry, s. 30.

¹⁹⁹ Doğan, K./ Arslantekin, S.: *Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum*, Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 2016, C. LVI, S. 1, s. 23-24; Fredriksson, C./ Mubarak, F./ Tuohimaa, M./ Zhan, M.: *Big Data in the Public Sector: A Systematic Literature Review*, Scandinavian Journal of Public Administration 2017, C. 21, S. 3, s. 45-46.

²⁰⁰ ICO: *Big Data and Data Protection*, 2014, s. 10-11. (<https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220> Erişim Tarihi: 04.06.2023)

²⁰¹ Curry, s. 29.

çalışma kapsamı dışında kaldığından ayrıntılı şekilde incelenmeyecektir. Ancak, kanımızca büyük verinin kamu sektörü için önemine kısaca değinmekte fayda vardır.

Hükümetler, büyük veriyi kamu hizmeti, ekonomi, sağlık hizmetleri, istihdam, doğal afetler ve terörle ilgili önemli sorunları çözecek bir araç olarak görmektedir²⁰². Gerçekten de geleneksel veri tabanları ile işlenilmesi mümkün olmayan hacim, hız ve çeşitlilikte verinin işlenebilmesi idarenin karar alma süreçlerini etkin bir şekilde yönetmesi, kolluk faaliyetini yerine getirmesi veya idari faaliyetlerin en iyi şekilde optimize edilmesi bakımından büyük bir potansiyel barındırmaktadır²⁰³. Büyük Veri Kamu Özel Forumu, yayınladığı raporda, kamu sektöründe, büyük verinin kullanım alanlarına yönelik dört potansiyel uygulama göstermiştir: Çevrimiçi kumar operatörleri için düzenlenmiş faaliyetlerin izlenmesi ve denetlenmesi, iş kurumlarında operasyonel verimliliğin sağlanması, akıllı şehirlerde kamu güvenliğinin sağlanması ve açık veriyi kullanarak öngörücü kolluk faaliyetinin yerine getirilmesidir²⁰⁴. Ayrıca büyük verinin açık veri yoluyla şeffaflığın ve hesap verilebilirliğin artması gibi faydaları da bulunmaktadır²⁰⁵. Açık veri ile sağlanan faydalara çalışmanın ilerleyen kısımlarında değinilecektir.

²⁰² Kim, G. U./ Trimi, S./ Chung, J.: *Big-Data Applications in The Government Sector*, Communications of the ACM 2014, C. LVII, S. 3, s. 84

²⁰³ Tansuğ, Ç.: *Türkiye'de İdari Faaliyetlerde Büyük Veri Uygulamaları*, iç. Gelişen Teknolojiler ve Hukuk III (Ed. Aksoy Retornaz, Eylem/ Güçlütürk, Osman Gazi), İstanbul 2021, s. 247-249.

²⁰⁴ Zillner, S./ Bretschneider, C./ Oberkamp, H./ Neurerer, S./ Munné, R./ Lippell, H., /Paradowski, D.: *Final version of Sector's Roadmap* (318062), 2014, (https://www.big-project.eu/sites/default/files/BIG_D2_4_2_FINAL_v0_851.pdf, Erişim Tarihi: 15.01.2023)

²⁰⁵ Shastri, A./ Deshpande, M.: *A Review of Big Data and Its Applications in Healthcare and Public Sector*, iç. Big Data Analytics in Healthcare, Studies in Big Data (ed. Kulkarni, Anand J./ Siarry, Patrick/ Singh, Pramod Kumar/ Abraham, Ajith/ Zhang, Mengjie/ Zomaya, Albert/ Baki, Fazle), C. 66, Cham 2020, s. 62-63; Cavanillas/ Curry / Wahlster, s. 6.

B. E-Devlet

1. Tanım ve E-Devletin Gelişimi

Bilgi ve iletişim teknolojilerinin (BİT) gelişmesiyle birlikte klasik anlamda kamu hizmetlerinin yürütülmesi/sunulması yetersiz kalmaya başlamış ve kamu hizmeti sunumunda değişiklik bir zorunluluk halini almıştır. Bu zorunluluğun bir sonucu olarak da kamu hizmetlerini kâğıt üzerinden elektronik ortama taşıyan ve e-devlet olarak adlandırılan kavram ortaya çıkmıştır²⁰⁶. En dar anlamıyla bilgi teknolojilerinin hükümetler tarafından kullanılması olarak tanımlanabilecek²⁰⁷ e-devleti OECD “*daha iyi bir devlet yönetimi için internet başta olmak üzere BİT’lerin kullanılması*” olarak tanımlamıştır²⁰⁸. Türkiye.gov internet sitesinde ise e-devletin “*vatandaşlara devlet tarafından verilen hizmetlerin elektronik ortamda sunulması*” olduğu ifade edilmiştir²⁰⁹. Geleneksel olarak idarenin verimliliğini artırmak ve devlet hizmetlerini çevrimiçi olarak sunmak için BİT’lerin kullanılması olarak tanımlanan e-devletin çerçevesi, zaman içerisinde vatandaşlar ve işletmelerle çeşitli etkileşimlerin yürütülmesi amacıyla devlet tarafından BİT kullanımının yanı sıra açık devlet verilerini ve yönetimde inovasyonu sağlamak için de BİT kullanımını içerecek şekilde genişlemiştir. Bu bağlamda geniş tanımıyla e-devlet, çevrimiçi devlet

²⁰⁶ Çarıkçı, O.: *Türkiyede E-Devlet Uygulamaları Üzerine Bir Araştırma*, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 2010, C. XII, S. 12, s. 97-98.

²⁰⁷ Viana, A. C. A.: *Digital transformation in Public Administration: From E-Government To Digital Government*, International Journal Of Digital Law 2021, C. II, S. 1, s. 32.

²⁰⁸ OECD: *Background Paper: Implementing E-Government In OECD Countries: Experiences And Challenges*, 2008, s. 2, (<https://www.oecd.org/mena/governance/36853121.pdf>), Erişim Tarihi: 04.06.2023).

²⁰⁹ Türkiye.gov.tr: *Sıkça Sorulan Sorular*, (<https://www.turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar#s01>), Erişim Tarihi: 25.04.2023).

hizmetlerinden; vatandaşlar, işletmeler ve devletin diğer kolları ile elektronik ortamda bilgi ve hizmet alışverişine kadar her şeyi ifade etmek için kullanılmaktadır²¹⁰. Kırac ve Bayrakçı'nın belirttiği üzere e-devlet “*geleneksel devlet yapılanmasına göre daha fazla bilgiyi ön plana çıkaran ve hatta var olan bilginin daha hızlı ve etkin bir şekilde kullanılmasını sağlamak üzere kurgulanmış bir sistemattir*”²¹¹.

Her ne kadar ilk bakışta e-devlet uygulamalarının sadece vatandaşlara yönelik olduğu izlenimi uyansa da e-devlet farklı etkileşim türlerini içermektedir. Devletten devlete (G2G) olarak adlandırılan etkileşim kamu sektöründeki aktörler arasında elektronik bilgi paylaşımı ve değişimini tanımlamak için kullanılmaktadır. Devletten iş dünyasına terimi (G2B) iş dünyasındaki özel sektör aktörleri ile idarenin etkileşime girmesini ifade etmektedir. Devletten Vatandaşa (G2C) etkileşim ise, bilginin devletten halka sunulması anlamına gelmektedir. e-devlet uygulamalarının halk açısından daha kullanılabilir olması için müşteri/tüketici merkezli bir e-devlet modeli izlenmelidir. Bu üç etkileşim türüne ek olarak bazı yazarlar devletten çalışana (G2E) olarak adlandırılan dördüncü bir etkileşim türünü de kabul etmektedir²¹².

Görece yeni bir kavram olan e-devletin ilk uygulamaları internet ve teknolojinin hızla gelişmeye başladığı 90'lı yılların son dönemlerine doğru kendisini göstermeye başlamıştır²¹³. İlk başlarda genellikle yerel yönetimlerde kendini gösteren ve sınırlı imkanlar sağlayan e-devlet uygulamaları zaman içerisinde gelişerek farklı bir

²¹⁰ UN e-Government Knowledgebase: “Overview.”, (<https://publicadministration.un.org/egovkb/en-us/Overview#what-is>, Erişim Tarihi: 25.04.2023).

²¹¹ Kırac, S./ Bayrakçı E.: *E-Devlet Uygulamaları Bağlamında Türkiye’de E-Belediyeçilik Anlayışı*, Balıkesir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2020, C. II, S. 2, s. 115.

²¹² Viana, s. 32-33; Yılmaz, D./ Türkoğlu, İ.: *Türkiye’de E-Devlet Uygulamalarının Bazı Yönetim Süreçlerine Etkisinin Örnek Projeler Bağlamında Değerlendirilmesi*, Uluslararası Yönetim İktisat ve İşletme Dergisi 2010, C. X, S. 22, s. 240.

²¹³ Grönlund, Å./ Horan, T.A.: *Introducing e-Gov: History, Definitions, and Issues*, Communications of the Association for Information Systems, Association for Information Systems 2004, C. XV, S. 39, s. 714.

boyut kazanmış ve ulusal düzeyde birçok kamu hizmetinin internet ortamında gerçekleştirilebileceği bir hal almıştır. Doktrinde e-devlet uygulamalarının gelişim evreleri farklı şekillerde tasnif edilmiştir²¹⁴. E-devlet uygulamalarının gelişimini dört evreye ayıran *Layne* ve *Lee*'ye göre bu uygulamalar kural olarak; kataloglama, işlem, dikey entegrasyon ve yatay entegrasyon aşamalarından geçerek gelişmektedir²¹⁵:

1) Kataloglama: Bu aşamada bazı resmî web siteleri oluşturularak halkla bilgi paylaşımı yapılmaktadır. Kullanıcılar aktif şekilde işlem yapamamakta sadece sağlanan bilgileri öğrenip bazı formlar indirebilmektedirler.

2) İşlem: Web sitelerinin gelişmesi ve yaygınlaşmasıyla beraber internetin bir hizmet kanalı olarak potansiyelinin farkına varılmış ve kamu siteleri vatandaşların çevrimiçi olarak kamu hizmetlerinden yararlanabileceği bir yapıya dönüştürülmüştür. Elektronik hizmetlerin kamu sektörü açısından faydalarının asıl olarak anlaşıldığı ve idare ile vatandaş arasındaki etkileşimin değişmeye başladığı evre de burasıdır. Bu evreyle beraber vergi ve idari para cezalarının ödenmesi gibi yenilikler sağlanmış, vatandaşların tüm işlemleri için fiziksel olarak bir yerlere giderek vakit harcamasının önüne geçilmiştir.

3) Dikey Entegrasyon: Bu evrede mevcut kamu hizmetlerinin otomatikleştirilmesi ve dijitalleşmesinden ziyade kamu hizmetlerinin kendisinin dönüşümü söz konusudur. 2.

²¹⁴ Doktrinde iki, üç, dört ve beş evreli e-devlet modelleri de bulunmaktadır. Bu konuda detaylı bilgi için bkz. Reddick, C. G.: *A Two-stage Model of E-government Growth: Theories and Empirical Evidence for U.S. Cities*, Government Information Quarterly 2004, C. XXI, S. 1, s. 51–64; Word Bank Group: *The e-government handbook for developing countries: a project of InfoDev and the Center for Democracy and Technology*, 2002, (<https://documents1.worldbank.org/curated/en/317081468164642250/pdf/320450egovhandbook01public12002111114.pdf>, Erişim Tarihi: 17.06.2023).

²¹⁵ Layne, K. / Jungwoo L.: *Developing Fully Functional E-government: A Four Stage Model*, Government Information Quarterly 2001, C. XVIII, S. 2, s. 123–134.

aşamada hizmetlerin çoğu birbirinden bağımsız ve ayrı konumdadır. Buna karşın, 3. aşamada dağınık haldeki bu sistemlerin birbiriyle etkileşime geçmesi, birbirlerine entegre olması söz konusudur. Bu durum dikey ve yatay şekilde gerçekleşmektedir. Dikey entegrasyonda aynı işlevi yerine getiren farklı sistemler örneğin farklı yerel idarelerin sağladığı benzer hizmetler tek bir çatı altında birleştirilmektedir. Aynı işlevi yerine getiren farklı platformların tek bir yerde toplanması teknik açıdan daha kolay olduğundan dikey entegrasyon daha önce gerçekleşmektedir.

4) Yatay entegrasyon: Tipik olarak çevrimiçi sunulan kamu hizmetlerinin her birine ayrı platformlardan ulaşılmaktadır. Bu sebeple vatandaşların her farklı işlemi için ayrı ayrı web sitelerine girip işlemlerini gerçekleştirmesi gerekmektedir. Ancak BİT'lerin kamu hizmetleri yönünden sağladığı faydalardan tam verim alabilmek için bu farklı platformlar arasındaki duvarların yıkılması ve tüm hizmetlerin tek bir platform üzerinden sunulması gerekmektedir.

Günümüzde, özellikle de OECD'nin raporlarında e-devlet teriminin yerini dijital devlet terimine bıraktığı, e-devletten dijital devlete bir geçiş olduğu yönünde görüşler de mevcuttur. E-devletin bir sonraki aşaması olarak da kabul edilebilecek dijital devlet, kamu değeri²¹⁶ yaratmak için dijital teknolojilerin hükümetlerin modernizasyon stratejilerinin entegre bir parçası olarak kullanılmasını ifade etmektedir. Bu bağlamda dijital devlet; idare, sivil toplum kuruluşları, işletmeler,

²¹⁶ OECD'nin 2014 yılında yayınladığı Dijital Devlet Stratejilerine İlişkin Tavsiyesinde belirtildiği üzere kamu değeri, aşağıdakiler de dahil olmak üzere, bakış açısına veya aktörlere göre değişebilen toplum için çeşitli faydaları ifade eder: 1) vatandaşların ve müşterilerin arzularını tatmin eden mallar veya hizmetler; 2) vatandaşların adalet, hakkaniyet, verimlilik ve etkinlik beklentilerini karşılayan üretim seçenekleri; 3) vatandaşların arzularını ve tercihlerini yansıtan uygun şekilde düzenlenmiş ve üretken kamu kurumları; 4) dağıtımın adillliği ve verimliliği; 5) kamu amaçlarını gerçekleştirmek için kaynakların meşru kullanımı; 6) değişen tercihlere ve taleplere yenilik ve uyum sağlama. Bkz. OECD: *Recommendation of the Council on Digital Government Strategies*, 2014, (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406>, Erişim Tarihi: 17.06.2023).

dernekler ve bireylerden oluşan ve devletle etkileşim yoluyla veri, hizmet ve içerik üretimini ve bunlara erişimi destekleyen dijital bir ekosisteme dayanmaktadır²¹⁷. OECD 2020 yılında yayınladığı Hükümet Politikası Çerçevesi’nde insan odaklı ve sürdürülebilir dijital hükümetleri altı boyutta ele almış²¹⁸ ve Dijital Devlet Endeksi’nde bu altı boyut çerçevesinde devletlerin gelişimini değerlendirmektedir²¹⁹.

Ülkemizde de internet alt yapısı kurulduktan sonra e-devlet projeleri hızlı bir şekilde geliştirilmeye başlanmıştır. Bu kapsamda 1998/13 sayılı Başbakanlık Genelgesi ile KamuNet Üst Kurulu ve KamuNet Teknik Kurulu kurulmuş ve 1999/34 sayılı KamuNET Projesi Genelgesi yayınlanmıştır. Kamu kurumları arasındaki yazışmaların elektronik ortamda yapılmasını öngören bu proje gerek e-Avrupa+ gerekse e-devlet projeleri kapsamında Türkiye’de idarenin dijitalleşmesi açısından büyük bir adımdır²²⁰.

Türkiye’de e-dönüşüm projeleri kapsamında 2002 yılında organizasyon yapısında köklü değişikliklere giden KamuNet Teknik Kurulu ana görevlerini kısaca şu şekilde özetlemektedir:

“KamuNet Teknik Kurulunun ana görevlerinden biri; bilgi toplumuna geçiş sürecinde bilgi ve iletişim teknolojilerinin getirdiği olanaklardan yararlanarak, devletin etkin, şeffaf, güvenli, hızlı ve kesintisiz hizmet sunacak; e-Kurumların oluşturulmasını

²¹⁷ OECD: *Government at a Glance 2019*, s. 149 (<https://doi.org/10.1787/8ccf5c38-en>, Erişim Tarihi: 17.06.2023).

²¹⁸ Dijital devleti oluşturan altı boyut: 1) tasarımda mahremiyet, 2) veri odaklı kamu sektörü, 3) bir platform olarak hükümet, 4) varsayılan olarak açık, 5) kullanıcı odaklı, 6) proaktiflik. Ayrıntılı bilgi için bkz: OECD: *The OECD Digital Government Policy Framework: Six dimensions of a Digital Government*, OECD Public Governance Policy Papers No. 02, 2020 (<https://www.oecd.org/governance/the-oecd-digital-government-policy-framework-f64fed2a-en.htm>, Erişim Tarihi: 17.06.2023).

²¹⁹ OECD: *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, s. 139, (<https://doi.org/10.1787/ce08832f-en>, Erişim Tarihi: 17.06.2023).

²²⁰ Çarıkçı, s. 102-103.

sağlamak, devlet ve vatandaş arasındaki ilişkileri elektronik ortama taşımak için Devlet e-Kapısını (portalını) oluşturmaktır”²²¹

Ardından, 2003 tarihinde yayınlanan acil eylem planında e-Dönüşüm Türkiye Projesi’ne yer verilmiş, 2003/12 sayılı Başbakanlık Genelgesi ile bu projenin amaçları ve uygulama esasları belirlenmiştir. Bu kapsamda, e-devlet uygulamalarının gelişimi bir ivme kazanmış, birçok e-devlet uygulaması faaliyete geçmiştir²²².

2008 yılına gelindiği ise e-devlet uygulamalarının birbirlerine entegre olarak çalışabilmesi ve tek bir portaldan birçok hizmete ulaşılabilmesi için e-devlet kapısı kullanıma açılmıştır. 2012 yılında ilk yerel yönetim entegrasyonunu gerçekleştiren e-devlet kapısı sürekli gelişmeye, yeni özellikler ve hizmetler sunmaya devam etmektedir. 2023 yılı için e-Devlet Kapısı’nın yönetilmesi görevi T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’ne verilmiş olup²²³, sistemin geliştirilmesi ve işletilmesi Türksat A.Ş. tarafından yapılmaktadır²²⁴. Son olarak belirtmek gerekir ki 2009 yılında yürürlüğe giren “Kamu Hizmetlerinin Sunumunda Uyulacak Usul ve Esaslara İlişkin Yönetmelik” uyarınca basılı ortamdaki bilgi ve belgeler ile idareye yapılacak başvuruların elektronik ortama taşınmasının esas olduğu kabul edilmiştir²²⁵.

²²¹ Devlet Planlama Teşkilatı Yönetim Bilgi Merkezi Dairesi KamuNet Teknik Kurulu Başkanlığı: *e-Devlet’e Geçiş Sürecinde KamuNet Çalışmaları*, 2002, s. 1 (http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/e-Devlete_Gecis_Surecinde_KAMU-NET_Calismalari.pdf), Erişim Tarihi: 17.06.2023).

²²² Türkiye Bilgi ve İletişim Teknolojileri Dairesi Başkanlığı: *E-Dönüşüm*, 20.01.2015, (www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi), Erişim Tarihi: 28.04.2023); Çarıkçı, s. 103.

²²³ Bkz. 1 Sayılı Cumhurbaşkanlığı Kararnamesi m. 527: (1) *Dijital Dönüşüm Ofisinin görevleri şunlardır:*

a) *Cumhurbaşkanı tarafından belirlenen amaç, politika ve stratejilere uygun olarak kamunun dijital dönüşümüne öncülük etmek, Dijital Türkiye (e-devlet) hizmetlerinin sunumuna aracılık etmek, kurumlar arası işbirliğini artırmak ve bu alanlarda koordinasyonu sağlamak.*

²²⁴ Türkiye.gov.tr: *Sıkça Sorulan Sorular*, (<https://www.turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar#s01>), Erişim Tarihi: 28.04.2023).

²²⁵ Bkz. RG, T. 31.07.2009, S. 27305.

2. E-Devletin Faydaları ve Riskleri

Yukarıdaki açıklamalardan anlaşılabileceği üzere, e-devlet, temelde kamu hizmetlerinin dijitalleştirilmesi, hizmet sunumunun gelişen teknolojilere ve çağın gerekliliklerine ayak uydurmasıyla ilgilidir. İdarenin dijitalleşmesinin getirdiği birçok fayda bulunmaktadır. Literatür incelendiğinde e-devletin sağladığı faydaları aşağıdaki gibi sıralamak mümkündür²²⁶.

- Kamusal hizmetlerin yaygınlaşması, vatandaşlara daha hızlı ve kolay erişilebilen hizmetlerin sunulması,
- Klasik anlamda kamu hizmetinde sadece belirli saat ve günlerde hizmet alınabilirken e-devlet ile kamu hizmetinin 7/24 sağlanan bir yapıya dönüşmesi,
- İdarenin işleyişinin hızlandırılması ve bu sayede verimliliğin artırılması,
- Kırtasiye giderleri ve bürokrasinin azaltılması ile hem mali hem de zamansal olarak tasarruf sağlanması,
- Hükümetler ve işletmeler arasında daha iyi ve kolay iletişim sağlanarak daha açık bir pazar ve daha güçlü bir ekonomi yaratılması,
- Şeffaflık ve hesap verilebilirliğin artması,
- İdare ve vatandaş arasındaki etkileşimin artması.

²²⁶ Çarıkçı, s. 101; Maraş, G.: *Kamu Yönetimlerinde E-Devlet ve E-Demokrasi İlişkisi*, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2011, C. XXXVII, s. 128-129; Civelek, M.E.: *Elektronik Devletin Gelişim Evreleri*, Opus Uluslararası Toplum Araştırmaları Dergisi, 2019, C. XIII, S. 19, s. 2537-2539; Yılmaz/ Türkoğlu, s. 248-254; Agbozo, E.: *Personal Data and Privacy Barriers to E-Government Adoption, Implementation and Development in Sub-Saharan Africa*, Electronic Governance and Open Society: Challenges in Eurasia (Ed. Voigt, P./ von dem Bussche, A.), 5th International Conference 2018, s. 83 (https://doi.org/10.1007/978-3-030-13283-5_7 Erişim Tarihi: 17.06.2023).

Ancak, e-devlet her ne kadar birçok fayda sağlasa da bazı riskleri de beraberinde getirmektedir. Bireyler farkında olmasa da internet ortamındaki her hareket ile veri üretilmektedir. İnternet hizmetleri ne kadar çok kullanılırsa kullanıcı hakkında o kadar fazla veri elde edilmekte ve bu bilgiler veri tabanlarında saklanmaktadır. İnternet sitelerinde toplanan bu kişisel verileri, kullanıcının sisteme kişisel bilgilerini kendi kaydetmesi ve kullanıcının bir etkileşimi, hatta bazen haberi bile olmadan kişisel verilerin internet sitesi tarafından toplanması olarak ikiye ayırmak mümkündür. İlk kategoriye giren ve genellikle bir hizmet sunan sitelerin kullanılabilmesi için çoğunlukla kayıt zorunluluğu getirilmekte ve kayıt işleminden sonra da adres ve telefon bilgisi gibi birtakım veriler sağlanmalıdır. Bunlara örnek olarak e-satış platformları gösterilebilir. İkinci kategoriye ise internet sitelerinde toplanan çerezler oluşturmaktadır²²⁷. Çerezlerle ilgili ayrıntılı inceleme çalışmanın ilerleyen kısımlarında yapılacaktır.

Amaçlarını gerçekleştirmek ve fayda sağlayabilmek için çok büyük miktarda veri işleyen e-devlet kapsamındaki internet siteleri de bu bağlamda başka herhangi bir siteden farklı değildir. Özel sektörle kıyaslandığında devlet veri tabanındaki veri miktarının büyüklüğü, verilerin türü ve idare içindeki veri paylaşımı sebebiyle kişisel verilerin gizliliği noktasında e-devlet büyük endişeler ve problemler doğurmaktadır²²⁸.

2002 yılında yaptığı bir çalışmada McDnagh veri gizliliği noktasında e-devletin yarattığı problemleri şöyle özetlemiştir²²⁹:

²²⁷ Küzeci, s. 37-38.

²²⁸ Wu, Y.: *Personal Data Protection in E-Government: Globalization or Glocalization? A Comparative Study Of The United States, Germany And China*, Yayınlanmamış Doktora Tezi, Michigan State University, 2010, s. 14.

²²⁹ McDonagh, M: *E-Government in Australia: The Challenge to Privacy of Personal Information*, International Journal of Law and Information Technology, C. X, S. 3, 2002, (327–343)’den naklen Wu, s. 15.

1) Toplama sorunları: Çerezlerin kullanımı, e-posta adreslerinin toplanması ve e-postaların posta listelerine dahil edilmesi yoluyla veri sahiplerine haber verilmeksizin kişisel verilerinin otomatik olarak toplanması.

2) Kullanım ve açıklama sorunları: Entegre portalların geliştirilmesi nedeniyle devlet kurumları arasında veri paylaşımı ve çapraz referanslama; kamu ve özel sektör arasında veri iletimi; genel anahtar dizini ve sertifika iptal listeleri aracılığıyla kişisel bilgilerin kullanımı ve açıklanması²³⁰.

3) Güvenlik sorunları: Güvenli bir altyapının bulunmadığı durumlarda e-devlet uygulamalarında özel anahtarların güvenliği tehlikeye düşmekte ve bu olası kimlik hırsızlıklarının önünü açmaktadır. Bu gibi sorunlarının önüne geçebilmek adına idare uygun veri koruma politikaları ve önlemleri belirleyip uygulamalıdır.

McDnagh'ın e-devletin ilk yaygınlaşmaya başladığı dönemlerde ortaya koyduğu bu problemler günümüz için de güncelliğini korumaktadır. Zira, her ne kadar bu problemlere sürekli çözüm üretilmeye çalışılsa da teknoloji ve e-devletin yapısı da

²³⁰ Genel anahtar, aynı şifreleme algoritmasını kullanan ve “*Dijital İmza*”rı doğrulamak ve dosyaları veya mesajları şifrelemek için kullanılabilen, “*Özel Anahtar*” ile arayüz oluşturacak şekilde tasarlanmış, herkese açık şifreli bir elektronik veri dosyası anlamına gelir. “*Dijital Sertifika*” ise, ilgili genel anahtarın oluşturulduğu kişiyle “*Genel Anahtar*” arasında bağlantı kuran ve o kişinin kimliğini onaylayan elektronik bir tasdik anlamına gelmektedir. Bkz. Law Insider: *Public Key Definition*, (www.lawinsider.com/dictionary/public-key, Erişim Tarihi 28.04.2023). Law Insider, *Digital Certificate Definition*, (www.lawinsider.com/dictionary/digital-certificate, Erişim Tarihi 28.04.2023). Belirtmek gerekir ki açık anahtarlar bazı durumlarda kişisel veri olabilmektedir. Bkz: Schroers, J.: *Are Public Keys Personal Data?*, *CITIP Blog*, 2018, (www.law.kuleuven.be/citip/blog/are-public-keys-personal-data, Erişim Tarihi: 28.04.2023); Bunun yanında sertifika iptal listeleri de kimi durumlarda kişisel verilerin açıklanması/ifşa edilmesi durumunu doğurabilir. Avrupa Birliği hukukuna bakıldığında sertifika iptal listelerinin kişisel veri içermesinin bazı hallerde açık bir şekilde yasaklandığı görülmektedir. Örneğin: COVID-19 salgını sırasında serbest dolaşımı kolaylaştırmak için birlikte çalışabilir. COVID-19 aşılama, test ve iyileştirme sertifikalarının (AB Dijital COVID Sertifikası) düzenlenmesi, doğrulanması ve kabulüne yönelik bir çerçeveye ilişkin 4 Haziran 2021 tarihli ve 2021/953 sayılı tüzüğün 4. maddesinde sertifika iptal listelerinin herhangi bir kişisel veri içermeyeceği açık bir şekilde düzenlenmiştir.

sürekli gelişmekte, veri işleme faaliyeti ile veri güvenliği farklı bir boyuta evrilmektedir.

E-devletin kişisel verilerin gizliliği noktasında yarattığı riskleri teknolojiyen kaynaklanan ve devletin kendisinden kaynaklanan riskler olarak ikiye ayırmak mümkündür²³¹. Teknolojiden kaynaklanan risklerin nedeni günümüzde “yeni petrol” olarak nitelendirilen kişisel verilerin ekonomik değere sahip olması dolayısıyla bazı kişi veya grupların siber saldırılar yoluyla²³² e-devlet üzerinde tutulan bu verileri ele geçirmeye çalışmasıdır²³³. Örneğin, 2019 yılında Bulgaristan Ulusal Gelir Ajansı’na yapılan bir siber saldırı neticesinde, Bulgaristan’ın bugüne kadarki en büyük kişisel veri ihlali olan ve yaklaşık beş milyon vatandaşın özel nitelikli kişisel verilerini de içeren bir veri sızıntısı yaşanmıştır. Veri ihlali neticesinde; maaş ve gelir kayıtları, ulusal kimlik numaraları, vergi ödemeleri, sosyal güvenlik bilgileri, kişisel borç bilgileri, sağlık ve emeklilik ödemeleri gibi veriler sızdırılmış ve bu verilerin bir kısmı çeşitli platformlarda paylaşılmıştır²³⁴. Nitekim, Türkiye’de de kamu kurum ve kuruluşlarının internet sitelerine saldırılar yapıldığı görülmektedir²³⁵.

²³¹ Al-Jamal, M./ Abu-Shanab, E.: *Privacy Policy of E-Government Websites and the Effect on Users’ Privacy*, International Conference on Information Technology 2015, s. 339.

²³² Belirtmek gerekir ki e-devlet nezdinde tutulan kişisel verileri siber saldırıların yanında fiziksel saldırılarla da ele geçirmek mümkündür. Örneğin, 2020 yılında kimliği belirsiz hırsızlar, Hollanda nüfusunun neredeyse yarısı tekabül eden 6,9 milyon kayıtlı organ bağışçısının kişisel verilerini içeren iki sabit disk Hollanda hükümetinin kasa deposundan çalmıştır. Ancak bu tarz fiziksel saldırılar çalışma kapsamı dışında kalmaktadır. Bkz: Cimpanu, C.: *Dutch Government Loses Hard Drives With Data of 6.9 Million Registered Donors*, ZDNET 2020, (www.zdnet.com/article/dutch-government-loses-hard-drives-with-data-of-6-9-million-registered-donors), Erişim Tarihi: 02.05.2023).

²³³ Zakrzewska/Miciula, s. 3458.

²³⁴ Chin, K.: *Biggest Data Breaches in Europe [Updated 2023]*, (www.upguard.com/blog/biggest-data-breaches-europe), Erişim Tarihi: 02.05.2023).

²³⁵ Türkiye’deki idarelere yapılan siber saldırılar sonucu yapılan veri ihlal bildirimleri için bkz. 2022/1271-Pamukkale Belediyesi (<https://www.kvkk.gov.tr/Icerik/7504/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Pamukkale-Belediyesi>), Erişim Tarihi: 11.07.2023); 2022/990 -Marmara Üniversitesi, (<https://www.kvkk.gov.tr/Icerik/7451/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Marmara-Universitesi>), Erişim Tarihi: 11.07.2023); 2022/155- Şişli Belediye Başkanlığı, (<https://www.kvkk.gov.tr/Icerik/7183/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Sisli-Belediye-Baskanligi>), Erişim Tarihi: 11.07.2023); 2019/384- Küçükçekmece Belediyesi,

Siber saldırılar doğrudan sisteme dışarıdan müdahale edilerek yapılabileceği gibi sistemdeki açıkların ve özensizliklerin kullanılması şeklinde de gerçekleşebilmektedir. Örneğin, Ketizmen ve Ülküderner 2007 yılında yaptıkları bir çalışmada Türkiye’de bir devlet sitesinden edinilen bilgiyle bir kişi hakkındaki birçok başka kişisel verinin başka devlet sitelerinden nasıl öğrenilebileceğini ayrıntılı bir şekilde açıklamıştır²³⁶. Her ne kadar bu çalışmada gösterilen açıklar günümüzde düzeltilmiş olsa da benzer olaylara hala rastlanılmaktadır. 2023 Cumhurbaşkanı ve 28. dönem milletvekili genel seçimi için e-devlet portalı üzerinden yapılan yurt içi seçmen kaydı sorgulaması yapan herkese, aynı binada oturan tüm seçmenlerin isim ve soy isimleri görünmüştür. Olayın sosyal medyaya yansımaları üzerine bu açık düzeltilerek sadece aynı hanede oturan seçmenlerin bilgisi görünecek şekilde düzeltilmiştir. Bu gibi güvenlik açıkları kişisel veri ihlallerine yol açarak vatandaşlara zarar vermenin yanında idare için de sorunlar doğurmaktadır. IBM Security tarafından yayınlanan “Veri İhlalinin Maliyeti Raporları” incelendiğinde, kamu sektöründeki veri ihlallerinin toplam küresel maliyetinin 2020 ve 2022 yılları arasında yaklaşık %92 arttığı ve 2022 yılı için ortalama veri ihlali maliyetinin 1,93 milyon dolar olduğu görülmektedir²³⁷. Ayrıca, veri ihlalleri idareye ekonomik yönden zarar vermenin yanında e-devlet uygulamalarına duyulan güveni azaltmakta ve uluslararası düzeyde veri akışını olumsuz etkileyebilmektedir. Yukarıda örneği verilen 2019 Bulgaristan veri ihlali sonrasında, aralarında İsviçre, Almanya, Singapur gibi ülkelerin de bulunduğu “Vergi

(<https://www.kvkk.gov.tr/Icerik/6584/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Kucukcekmece-Belediyesi>, Erişim Tarihi: 11.07.2023).

²³⁶ Ketizmen, M./ Çağlar Ü.: *E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması*, XII. Türkiye’de İnternet Konferansı 2007, (<http://inet-tr.org.tr/inetconf12/bildiri/2.pdf>, Erişim Tarihi: 17.06.2023).

²³⁷ IBM Security: *Cost of a Data Breach Report 2021*, 2021, s. 4, 15, (www.ibm.com/downloads/cas/OJDVQGRY, Erişim Tarihi: 17.06.2023); IBM Security: *Cost of a Data Breach Report 2022*, 2022, s.11, (www.ibm.com/downloads/cas/3R8N1DZJi, Erişim Tarihi: 17.06.2023).

Amaçlı Şeffaflık ve Bilgi Değişimi Küresel Forumu”, Bulgaristan ile bilgi alışverişini durdurmuştur²³⁸.

Bahsi geçen riskleri, dijital güvenlik ve çevrimiçi hizmetlerle ilgili yasal çerçeveyi geliştirerek çözmek veya gerçekleşme olasılıklarını daha aza indirmek mümkündür²³⁹. Hem GDPR hem de KVKK incelendiğinde veri güvenliğinin sağlanması için teknik ve idari önlemlerin alınmasıyla ilgili hükümler olduğu görülmektedir. Her şeyden önce veri işleme şartlarını düzenleyen GDPR m. 5 kişisel verilerin uygun teknik veya idari tedbirler alınarak; yetkisiz/yasa dışı işleme, kazara kaybetme, imha veya hasara karşı koruma dahil olmak üzere uygun güvenliğin sağlanacak şekilde işleneceğini düzenlemektedir²⁴⁰. Bunun yanında GDPR varsayılan değer olarak güvenliği (*protection by design*) yasal bir gereklilik olarak kabul etmektedir. GDPR m. 25, işleme amaçlarının belirlenmesi ve işlemenin kendisi sırasında, kuruluşların veri korumasını etkili bir şekilde uygulamak ve gerekli güvenceleri işleme sürecine entegre etmek için uygun teknik ve idari tedbirleri uygulamaya koymasını zorunlu kılmaktadır. Son olarak işlemenin güvenliği başlıklı m. 32, gerektiğinde anonimleştirme yapılması gibi bazı özel güvenlik önlemleri öngörmektedir.

Düzenlemelerden anlaşıldığı üzere GDPR, kişisel verilerin uygun teknik ve idari önlemler kullanılarak güvenli bir şekilde işlenmesini zorunlu kılmakta, veri sorumlusu olarak idareye birtakım yükümlülükler getirmektedir²⁴¹. Buna karşın,

²³⁸ Chin, s. 2; State Secretariat for International Finance: *Switzerland Suspends AEOI With Bulgaria*, (www.sif.admin.ch/sif/en/home/documentation/specialist-information/archive/suspension-aeoi-bulgaria.html Erişim Tarihi: 02.05.2023).

²³⁹ Al-Jamal/ Abu-Shanab, s. 339.

²⁴⁰ Bkz. KVKK m. 12/1-ç

²⁴¹ GDPR’ın getirdiği bu yükümlülükler sadece idareyi değil özel sektör aktörlerini de bağlamaktadır. Ancak, çalışmanın kapsamı bakımından sadece idare ele alınmaktadır.

GDPR uygun önlemlerin ne olduğunu açık bir şekilde belirtmemekte, sadece yeterli güvenliğin sağlanması gerektiğine değinmektedir. Bu bağlamda, yeterli güvenlik, işlenen verilerin niteliği ve ortaya çıkabilecek riskler göz önüne alınarak yani her veri işleme faaliyetinin kendi özelliklerine göre değerlendirilecektir²⁴². Ancak, asgari düzeyde bir güvenliğin sağlanması gerektiği açıktır²⁴³. Hem ulusal hem de uluslararası kuruluşlar siber güvenliğin nasıl sağlanması gerektiğiyle ilgili raporlar ve öneriler yayınlamaktadır²⁴⁴. Örneğin, bilginin dijitalleşmesi karşısında ciddi güvenlik risklerinin doğması sonucunda 2019 yılında Cumhurbaşkanlığı bu güvenlik risklerini azaltmak ve özellikle de gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda kamu düzenini veya milli güvenliği tehdit edebilecek verilerin güvenliğinin sağlanması için 2019/12 sayılı Genelge ile birtakım tedbirler belirlemiştir²⁴⁵. Bu bağlamda, idarenin; olası ihlalleri önceden tespit edebilmek adına risk analizleri yapmak, çalışanlarını “ortalama” gibi olası saldırılar hakkında bilinçlendirmek için veri ve siber güvenlik eğitimleri gerçekleştirmek, veri minimizasyonu ilkesine uyarak verileri toplamak, düzenli şekilde sistem güvenliğini test etmek²⁴⁶ gibi birtakım eylemlerde bulunması gerekmektedir. Örneğin, Kişisel Verileri Koruma Kurumu’nun yayınladığı Veri Güvenliği Rehberi Uyarınca, uzaktan erişilebilen veriler için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir. Kurum bu bağlamda, bazı

²⁴² Bkz. GDPR m. 32.

²⁴³The National Cyber Security Centre: *General Data Protection Regulation (GDPR)*, (www.ncsc.gov.uk/information/gdpr#:~:text=What%20does%20the%20GDPR%20mean,to%20take%20%27appropriate%27%20action), Erişim Tarihi: 02.05.2023).

²⁴⁴ Jacobi, A./ Lund, M./ Kool, L./ Munnichs, G./ Weber, A.: *Security of eGovernment Systems: Final Report*, European Parliament, 2013; OECD: Recommendation of the Council on Digital Security Risk Management, 2022, (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479>), Erişim Tarihi: 02.05.2023); Kişisel Verileri Koruma Kurumu: Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), 2021, (https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf), Erişim Tarihi: 11.07.2023)

²⁴⁵ 2019/12 sayılı Cumhurbaşkanlığı Genelgesi, RG, T. 06.07.2019, S. 30823.

²⁴⁶ Zakrzewska/Miciula, s. 3464; Kişisel Verileri Koruma Kurumu (Kişisel Veri Güvenliği Rehberi), s. 19.

belediyeler tarafından çevrimiçi olarak sunulan emlak vergisi ödeme/hızlı ödeme veya borç sorgulama sayfalarında yalnızca T.C. kimlik numarası girilerek (tek aşamalı doğrulama) vatandaşın emlak bilgilerine ulaşılabilmesini KVKK m. 12’de düzenlenen “*kişisel verilere hukuka aykırı olarak erişilmesini önlemek*” yükümlülüğünün ihlali olarak kabul etmiş ve ilgili belediyelerin uygulamaları düzeltmesine karar vermiştir²⁴⁷.

Devletin kendisinden kaynaklanan riskler ise, idarenin bu verileri toplanma amaçlarından farkı sebeplerle kullanmasına dayanmaktadır. E-devlet vasıtasıyla elde edilen kişisel verilerin idare ve idare içerisindeki kamu görevlileri tarafından şahsi veya siyasi amaçlar için kullanılma tehlikesi her zaman mevcuttur. Örneğin, 2023 seçimleri için milletvekili adayı olan Çevre, Şehircilik ve İklim Değişikliği Bakanı Murat Kurum katılacağı bir televizyon programının haberini SMS yoluyla yurttaşlara duyurmuştur. Benzer şekilde 2021 yılında Elmalı belediye başkanı, bir yarışma programına katılan bir belde sakininin desteklenmesi için Antalya bölgesinde ikamet eden birçok vatandaşa SMS yollamıştır. Hem ilgili kişilerden hem de KVKK’dan kişilerin telefon bilgilerine nasıl ulaşıldığı hakkında bir bilgilendirme henüz yapılmamış olsa da bu verilerin devlet veri tabanlarından elde edilmiş olma ihtimali yüksektir²⁴⁸. Danıştay bu konuda önüne gelen bir davada, Esnaf ve Sanatkarlar Odası seçimlerinde kullanılmak üzere üyelerin adres, telefon ve işkolu bilgilerinin Türkiye Esnaf ve Sanatkarlar Konfederasyonu’nun 2009/74 sayılı Genelgesi’ne²⁴⁹

²⁴⁷ Kişisel Verileri Koruma Kurumu, *Kamuoyu Duyurusu (Belediyeler)*, 05.11.2021, (<https://www.kvkk.gov.tr/Icerik/7073/BELEDIYELERE-ILISKIN-KAMUOYU-DUYURUSU>, Erişim Tarihi: 01.07.2023); Kişisel Verileri Koruma Kurulu. İlke Kararı, T. 21.04.2022, S. 2022/388, (<https://www.kvkk.gov.tr/Icerik/7252/2022-388>, Erişim Tarihi: 11.07.2023).

²⁴⁸ Cumhuriyet Gazetesi: *Hukukçulardan Murat Kurum’un SMS Yollamasına İlişkin Açıklama*, 2023, (www.cumhuriyet.com.tr/turkiye/hukukculardan-murat-kurumun-sms-yollamasina-iliskin-aciklama-2077190, Erişim Tarihi: 03.05.2023).

²⁴⁹ Genelge uyarınca, “*Seçme ve seçilme hakkını kullanmak isteyen üyelere, 4982 sayılı Bilgi Edinme Hakkı Kanunu’nun 5.maddesi gereğince, oda üye listelerinin, listede bulunan üyelere ait özel nitelikli bilgilerin (T.C. kimlik no, doğum tarihi, doğum yeri gibi) çıkartılarak talep sahibine*”

dayanılarak paylaşılmasını hukuka aykırı bulmuştur²⁵⁰. Ayrıca, doktrinde bazı yazarlar BİT’ler vasıtasıyla toplanan kişisel veriler sayesinde devletin, daha doğrusu devlet mekanizmasını kullanan siyasal iktidarın, kişilerin özel hayatı üzerinde orantısız bir gözetim gerçekleştirebilmekte olduğunu ve bu durumun kişi hak ve özgürlüklerini tehdit eden baskıcı bir rejime geçiş tehlikesi doğurduğuna değinmektedir²⁵¹.

Veri koruma mevzuatı incelendiğinde e-devlet üzerinden toplanan kişisel verilerin farklı amaçlarla kullanmasını engellemek için çeşitli düzenlemeler yapıldığı görülmektedir. Örneğin hem GDPR hem de KVKK’da esas alınan, amaca bağlılık ilkesinin gayesi Çekin’in belirttiği üzere “*verinin işleme amaçlarını baştan belirlemekle ilgili kişinin neye rıza gösterdiğini bilmesini ve veri sorumlusunun da belirttiği amaç çerçevesinde gerekli ve ölçülü miktarda veri işlemesini sağlamaktır*”²⁵². Bu ilkeye paralel olarak, TCK’de verileri hukuka aykırı olarak yaymak, vermek veya ele geçirmek bir suç olarak sayılmış²⁵³ ve bu suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle kullanılması nitelikli hal olarak düzenlenmiştir²⁵⁴. Bu bağlamda, e-devlet vasıtasıyla toplanan kişisel verilerin kamu görevlileri veya idarenin kendisi tarafından farklı amaçlarla kullanılmasının hukuka aykırı olacağı açıktır. Bunlara ek olarak, kamu görevlilerinin kişisel verileri kendi amaçları için kullanması idarenin KVKK m. 12’de düzenlenen veri güvenliğine ilişkin yükümlülükleri yerine getirmediği anlamına gelmektedir. KVKK’nın veri sorumlusu

verilebilmektedir. Bkz. (<https://www.tesk.org.tr/view/mevzuat/goster.php?Guid=70804499-7dac-11ec-95b3-000c29b32a85>, Erişim Tarihi: 09.07.2023).

²⁵⁰ Dan. 8. D, T. 17.02.2021, E. 2016/3610, K. 2021/945, (Lexpera).

²⁵¹ Işıkcı, Y. M.: *E-Devlet Uygulamalarının Hukuk Devletine Etkisi: Yeni Kamu İşletmeciliği Paradigması Üzerinden Bir Değerlendirme*, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2017, C. XXII, S. Kayfor15 Özel Sayısı, s. 1904.

²⁵² Çekin, s. 71.

²⁵³ Bkz. TCK m. 136.

²⁵⁴ Bkz. TCK m. 137.

nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişime yetkisi olanlar tarafından, yetkilerini aşarak ve işleme amacı dışında söz konusu verilerin işlendiği yönündeki şikayetler üzerine verdiği 31.05.2018 tarih ve 2018/63 sayılı ilke kararında belirttiği üzere;

“Bir veri sorumlusu nezdinde bulundukları pozisyon veya görev itibariyle kişisel verilere erişme yetkisi olanlar tarafından, yetkileri aşmak ve/veya yetkilerini kötüye kullanmak suretiyle, kişisel amaçlara veya nedenlere bağlı olarak işleme amacı dışında söz konusu kişisel verilerin işlenmesi ve/veya bu verilerin üçüncü kişilerle paylaşılması 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrasına aykırılık teşkil edeceğinden, bu kapsamdaki eylemlerin önlenmesi amacıyla veri sorumlularınca uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirin alınması gerektiği hususunda veri sorumlularının bilgilendirilmesine (...) karar verilmiştir”²⁵⁵.

Buna paralel olarak Kurul, Sosyal Sigortalar Kurumu personelinin boşanma aşamasında olan eşinin maaş bilgisine SGK sisteminden ulaşarak bu veriyi mahkemeye sunmasını m. 12’deki yükümlülüğün ihlali kabul ederek, personel hakkında disiplin hükümleri uyarınca işlem yapılması gerektiğine hükmetmiştir²⁵⁶.

Son olarak cevaplanması gereken bir diğer sorun teknolojiden veya devletin kendisinden kaynaklanan riskler neticesinde ilgili kişilerin verilerinin hukuka aykırı olarak işlenmesi durumunda idarenin ne tür bir sorumluluğunun doğacağıdır.

²⁵⁵ Kişisel Verileri Koruma Kurulu, *İlke Kararı*, T. 31/05/2018 S.2018/63, (<https://www.kvkk.gov.tr/Icerik/5248/2018-63>, Erişim Tarihi: 11.07.2023)

²⁵⁶ İlgili kararın özeti için bkz.: Kişisel Verileri Koruma Kurumu, “İlgili kişinin kişisel verisinin kamu kurumu personeli olarak görev yapan eski eşi tarafından sorgulanarak elde edilmesi ve adli makamlar ile paylaşılması” hakkında Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/230 sayılı Karar Özeti, (<https://www.kvkk.gov.tr/Icerik/7119/2021-230>, Erişim Tarihi: 01.07.2023).

Verilerin güvenliğini sağlanması hususunda idarenin birtakım yükümlülükleri olduğuna yukarıda değinmiştik. Bu bağlamda, idarenin bu yükümlülüklerini hiç ya da gereği gibi yerine getirmemesi idarenin olumsuz eylemi olarak kabul edilecek ve hizmet kusuru oluşturacaktır. İlgili kişiler kamu veri tabanlarındaki verilerin çalınması nedeniyle uğradıkları zararları bu kapsamda tazmin ettirebileceklerdir. Ancak, idare veri güvenliğini sağlanması için mevcut tüm idari ve teknik tedbirleri alsa bile teknolojik gelişmeler sebebiyle, daha önceden mevcut olmayan ve idarenin öngöremeyeceği güvenlik açıkları oluşabilmektedir. Bu noktada, idarenin sorumluluğu bakımından kanımızca iki yorum yapılması mümkündür: İlk olarak, idarenin teknolojik gelişmeleri yakalaması ve veri güvenliğini sürekli gelişen teknolojilere uygun şekilde geliştirmesi bir zorunluluk olarak kabul edilebilecektir. Bu bağlamda, idarenin gelişen teknolojiler nedeniyle veri ihlaline sebebiyet vermesi hizmet kusurunu doğuracaktır.

Gelişen teknolojilere yeterince hızlı entegre olamamak hizmet kusuru kapsamında değerlendirilmediğinde ise, idarenin kusursuz sorumluluk hallerinden hasar/risk ilkesi gündeme gelebilecektir. Hasar/risk ilkesi idarenin bünyesinde tehlike taşıyan bir faaliyeti veya kuruşu dolayısıyla doğan zararlar nedeniyle sorumluluğunu ifade etmektedir. Olumsuz sonuçları ne idarenin önleyebildiği ne de bireylerin korunabildiği durumlarda sorumluluğun faaliyetten yarar sağlayan kamuda olduğu kabul edilmektedir²⁵⁷. İdarenin dijital ortamda veri işleyerek yerine getirdiği hizmetler ise gelişen teknolojiler sebebiyle her zaman saldırıya maruz kalabileceğinden bu hizmetlerin bünyesinde risk taşıdığının kabul edilmesi gerekmektedir²⁵⁸. Yeni

²⁵⁷ Gözübüyük/Tan, Genel Esaslar s. 721-722.

²⁵⁸ Altındağ, s. 396.

teknolojiler sayesinde dijital ortamda büyük miktarda veriyi kolay bir şekilde işleyebilme olanağına kavuşan, yani teknolojinin nimetlerinden faydalanan, idarenin ise bu teknolojilerin risklerine de katlanması hakkaniyet ilkesinin bir gereğidir²⁵⁹. Zira, idarenin gelişen teknoloji ve ihtiyaçlara bağlı olarak yürüttüğü hizmetlerin bazılarının bünyesinde risk taşıdığı, bu sebeple hizmetin niteliği gereği risk barındıran faaliyetlerden doğan zararların idarenin kusursuz sorumluluk ilkesi uyarınca tazmin edilmesi Danıştay’ca da kabul edilmektedir²⁶⁰.

Hasar/risk ilkesinin yanında, ayrıca, veri sorumlusu idareye yapılan siber saldırıların sosyal risk kuramı çerçevesinde tazmin edilmesi de düşünülebilir. Ancak, kanımızca, hasar/risk ilkesi kapsamında değerlendirilebilecek siber saldırıların terör saldırısı olarak kabul etmeye çalışmak zorlama bir yorum olacaktır²⁶¹. Üstelik, veri tabanlarına siber saldırı yapıldığı tespit edilebilse bile, bu saldırıyı gerçekleştirenlerin kimliğini tespit etmek bir hayli güçtür.

3. Kamu İnternet Sitelerinde Çerez Uygulaması:

²⁵⁹ Gürpınar, D.: *Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 2017, Prof. Dr. Şeref Ertaş’a Armağan, C. XIX, Özel Sayı, s. 691.

²⁶⁰ Dan., 10. D., T. 23.06.1997, E.1996/3996, K.1997/2544, (Lexpera); İlgili karara atıf yapan daha güncel tarihli AYM kararı için bkz. AYM, *Bilal Turan Ve Diğerleri Başvurusu*, B.No: 2013/1942, 04.12.2013, (Lexpera).

²⁶¹ Siber saldırıların sosyal risk ilkesi kapsamında değerlendirilemeyeceği yönünde görüş için bkz: Altındağ s. 396.

3.a Çerez Kavramı ve Türleri

Çerezler, bilgisayarınızı ağı tanıtmak için kullanılan ve benzersiz tanımlayıcılar içeren küçük metin dosyalarıdır. Bir web sitesini ziyaret ettiğinizde, bilgisayarın sabit diskinde bir çerez dosyası oluşturur. Aynı web sitesini bir sonraki ziyaretinizde, internet tarayıcınız daha önceki bilgilerinizi, eylemlerinizi ve tercihlerinizi hatırlamak ve kişiselleştirilmiş bir deneyim sunmak için bu çerez dosyasını kullanmaktadır²⁶². Çerezler aracılığıyla kullanıcılardan hem kişisel hem de kişisel olmayan veriler toplanmaktadır. Örneğin, tercih edilen dil ayarlarını saklayan çerezler kişisel veri içermezken, kullanıcı adı veya IP adresi bilgilerini saklayan çerezler kişisel veri içermektedir. Kullanıcı hakkında çeşitli bilgiler toplayan ve depolayan çerezlerin ise kişisel verilerin korunması ve mahremiyet ile bağlantılı olduğu açıktır. Benzersiz tanımlayıcılar kullanan çerezler bir kişinin ismi bilinmese bile diğer kişilerden ayırt edilebilmesini sağlamaktadır. Kişinin özelliklerine ve davranışlarına ilişkin olan bu bilgiler ise davranışsal reklamcılık gibi kişiyi etki altında bırakmak amacıyla kullanılabilir²⁶³.

Çerezlerin kişisel verilerle nasıl bağlantılı olduğunun anlaşılabilmesi için çerez türlerinin bilinmesi gerekmektedir. Zira, bir internet sitesinde genellikle birbirinden farklı çok fazla çerez türü kullanılmaktadır. Bu bağlamda, çerezleri süresine, kaynağına ve amacına göre üç ana başlıkta incelemek mümkündür²⁶⁴.

²⁶² Nguyen, S. J.: *What Are Internet Cookies and How Are They Used?*, All About Cookies, 2023, (<https://allaboutcookies.org/what-is-a-cookie>, Erişim Tarihi: 06.05.2023).

²⁶³ Aksoy, H.C./ Halıcıoğlu, M.: *AB ve Türk Hukuklarında Çerezler*, Kişisel Verileri Koruma Dergisi 2021, C. 3, S. 1, s. 63.

²⁶⁴ Çerez türleriyle ilgili devam eden kısımdaki açıklamalar şu kaynaklardan derlenmiştir: Koch, R.: *Cookies, the GDPR, and the ePrivacy Directive*, 2019, (<https://gdpr.eu/cookies/>, Erişim Tarihi: 06.05.2023); Aksoy/Halıcıoğlu, s. 63-64; Kişisel Verileri Koruma Kurumu, *Çerez Uygulamaları Hakkında Rehber*, 2022, (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf>, Erişim Tarihi: 17.06.2023).

İlk olarak, süresine göre çerezler oturum çerezleri ve kalıcı çerezler olarak ikiye ayrılmaktadır. Geçici çerez olarak da adlandırılan oturum çerezleri tarayıcı kapatıldığında sona ererler. Bu bakımdan kullanıcı gizliliği açısından bir problem yaratmamaktadırlar. Kalıcı çerezler ise, son kullanma tarihine bağlı olarak şahsen veya tarayıcı tarafından silinene kadar sabit diskte kalan tüm çerezleri ifade etmektedir. Kalıcı çerezler yoluyla, internet sitesine her girişte kullanıcının bilgileri sunucuya iletilmektedir ve bu çerezler profil oluşturma gibi amaçlarla kullanılabilir. Sayılan özellikleri nedeniyle izleme çerezleri olarak da adlandırılan kalıcı çerezlerin kodlarında yazılı bir son kullanma tarihi bulunmaktadır. Pratikte, manuel olarak bu çerezler silinmezse cihazlarda çok daha uzun süre kalabilmektedir.

İkinci olarak, kaynağına göre çerezler ise birinci taraf ve üçüncü taraf çerezleri olarak ayrılmaktadır. Adından da anlaşılacağı üzere, birinci taraf çerezleri doğrudan ziyaret edilen web sitesi tarafından cihaza yerleştirilen çerezlerdir. Üçüncü taraf çerezleri ise, ziyaret edilen web sitesi tarafından değil bir reklam veren veya analitik sistem gibi üçüncü bir tarafça cihaza yerleştirilen çerezlerdir. Web sitelerinin sahipleri, üçüncü kişilere oluşturdukları çerezleri kullanmaları için izin vermekte ve bu sayede bu çerezlerin sahipleri kullanıcıları izleyebilmektedir. Üçüncü taraf çerezleri, veri gizliliği açısından muhtemelen en tartışmalı çerez türüdür. *Aksoy/Halıcioğlu'nun belirttiği üzere üçüncü taraf çerezleri, "üçüncü kişilerin kontrolünün çok zor olması ve ilişki yapısının çok daha karmaşık olması sebebiyle önemli gizlilik risklerini muhtevasında barındırmaktadır"*²⁶⁵.

²⁶⁵ Aksoy/Halıcioğlu, s. 63.

Son olarak, amacına göre erezler; kesinlikle gerekli (zorunlu) erezler, iřlevsel/tercih erezler, reklam/pazarlama erezleri ve performans/analitik erezler olmak zere drde ayrılmaktadır. Zorunlu erezler, web sitesini kullanabilmek ve sunduėu hizmetlerin dzgn alıřmasını saėlamak iin gerekli olan erezlerdir. Bu kategorideki erezler genellikle birinci taraf oturum erezleridir. İřlevsel erezlerse, sitenin alıřması iin zorunlu olmamakla beraber kiřiselleřtirilmiř bir deneyim sunmak iin kullanılan erezlerdir. Bu erezlere rnek olarak dil tercihi, blge seimleri, kullanıcı adı ve řifrelerin hatırlanması gsterilebilir. İstatistik/performans erezleriye hangi sayfaları ziyaret ettiėiniz ve hangi baėlantılara tıkladıėınız gibi bir web sitesini nasıl kullandıėınız hakkında bilgiler toplar. Sitenin iyileřtirilmesi iin kullanılan bu erezler anonimleřtirilmekte dolayısıyla kiřisel veri iermemektedir. Pazarlama erezleriye evrimii davranıřsal reklamcılık kapsamında daha kiřisel reklamlar sunabilmek adına kiři hakkında bilgileri depolamakta ve bu verileri reklam verenlerle paylařmaktadır. Bu erezler oėunlukla, kalıcı, nc taraf erezleridir.

3.b Veri Koruma Hukuku ve E-Devlet Baėlamında erezler

erezler web uygulamalarının ayrılmaz bir parası olmakla birlikte, kullanıcı gizliliėi zerinde nemli etkilere sahiptirler. Veri aracılıėı firmalarının ve evrimii reklamcıların ncelikli hedeflerinden biri, hedeflenmiř reklamlar sunma amacı doėrultusunda kullanıcılar hakkında mmkn olduėunca fazla bilgi toplamaktır. Kullanıcı gizliliėi ve web erezleri ile ilgili endiřeler yıllar boyunca basında ve doktrinde dile getirilmiřtir. Bu durum, erez ynetimini ve kaldırılmasını kolaylařtıran

çeşitli araçların yanı sıra kullanıcı gizliliğini düzenleyen hukuki düzenlemelerin geliştirilmesine yol açmıştır²⁶⁶.

AB hukukunda çerezlerle ilgi ilk hukuki metin 2002/58/EC sayılı E-Gizlilik Direktifidir (ePrivacy Directive). Haberleşme alanında kişisel verilerin korunması amacıyla ortaya çıkan bu Direktif 2009 yılında köklü değişikliklere uğrayarak Çerez Yasası, Çerez Bayrağı (*Banner*) Kanunu veya Çerez İzni Kanunu gibi isimlerle de anılmaya başlanmıştır. İlgili direktifte “*web üzerinden kullanıcıların terminal cihazlarına çerez yerleştirilebilmesi ve bu cihazlarda halihazırda yerleşik olan çerezlere erişilebilmesi, kural olarak kullanıcıların rızaları şartına bağlanmıştır*”²⁶⁷. Her ne kadar E-Gizlilik Direktifinde rıza kural olsa da m. 5 ile bu kurala iki istisna getirilmiştir. İlgili madde uyarınca;

- i) Çerezin sadece, iletişimin elektronik haberleşme şebekesi üzerinden sağlanması amacıyla kullanılması,
- ii) Çerez kullanımının, abonenin veya kullanıcının hizmet almak için açıkça talep ettiği bilgi toplum hizmetleri için kesinlikle gerekli olması, durumlarından birinin varlığı halinde rıza alınmadan da çerezler kullanılabilir. Bu bağlamda, kesinlikle gerekli çerezler bakımından kullanıcıdan rıza alınmasına gerek bulunmamaktadır.

Çerez Yasası bir Direktif olduğundan dolayı direktif hükümleri üye devletlerin hukukunda doğrudan uygulamakta, üye ülkelerin direktifin amaç ve ilkelerine uygun şekilde iç hukuk düzenlemeleri gerçekleştirmesi gerekmektedir. Bu sebeple, ülke bazında çerezlerle ilgili düzenlemeler az da olsa birbirinden farklılık

²⁶⁶ Cahn, A/ Alfeld, S./ Barford, P. R./ Muthukrishnan, S.: *An Empirical Study of Web Cookies*, Proceedings of the 25th International Conference on World Wide Web 2016, s. 891.

²⁶⁷ Aksoy/Halicioğlu, s. 64.

gösterebilmektedir²⁶⁸. Ancak, ilgili direktifin temel amaçlarından ve düzenlemelerinden bariz bir şekilde sapılması söz konusu olmamaktadır. Bu bağlamda, E-Gizlilik Direktifi uyarınca çerezlerin kullanımına yalnızca kullanıcıya verilerinin neden izlendiği hakkında açık ve kapsamlı bilgi verilmesi ve kullanıcının onayının alınması halinde izin verilmektedir²⁶⁹. Açık ve kapsamlı bilginin ne anlama geldiği tanımlanmasa da direktifin ilgili maddesinde açık ve kapsamlı bilgilerin veri koruma yasasına uygun olarak sağlanması gerektiği belirtilmektedir. Bu durumda çerezlerin kişisel veri içerip içermediğine bakılmaksızın GDPR kapsamındaki bilgilendirme yükümlülüğünün yerine getirilmesi gerekmektedir. Bu bağlamda, kullanılan çerez türleri, bunların kullanım amaçları, kullanıcının cihazında depolanan veya cihazdan erişilen bilgileri işleyebilecek üçüncü taraflar, çerezlerin tutulma süresi gibi bilgilerin kullanıcılara sunulması bir zorunluluktur²⁷⁰. Açık rızanın çerezler bakımından değerlendirildiği, ABAD'ın Planet49 kararında belirtildiği üzere, açık rızanın kabul edilebilir olması için kişinin çerezler konusunda bilgilendirilmesi, ayrıca rızanın özgürce ve aktif bir davranış ile verilmiş olması gerekmektedir. Bu kapsamda, bir web sitesinde kullanıcının rızayı reddetmek için aktif olarak seçimini kaldırması gereken önceden seçilmiş bir onay kutusu veri koruma kanunu kapsamında geçerli bir rıza teşkil etmemektedir²⁷¹.

²⁶⁸ Cookie Script: *Cookie Law Explained*, 2022, (<https://cookie-script.com/blog/cookie-law>, Erişim Tarihi: 11.07.2023); Ülke bazındaki farklılıklar için bkz: Aksoy/Halicioğlu, s. 64-66.

²⁶⁹ Bond, R.: *The EU E-Privacy Directive and Consent to Cookies*, Business Lawyer 2012, C. LXVIII, S. 1, s. 215.

²⁷⁰ ICO: *What Are the Rules on Cookies and Similar Technologies?*, (<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules4>, Erişim Tarihi: 08.05.2023).

²⁷¹ ABAD, C-673/17, 01.10.2019; Planet49, (<https://curia.europa.eu/juris/documents.jsf?language=EN&critereEcli=ECLI:EU:C:2019:801>, Erişim Tarihi: 11.07.2023)

Her ne kadar E-gizlilik direktifi zaman içerisinde yapılan değişikliklerle beraber çerez kullanımında kişisel verilerin korunması açısından önemli düzenlemeler getirirse de teknoloji ve dijital dönüşümün çok hızlı gerçekleşmesi direktifin beklenen etki ve değişimi sağlamasının önüne geçmiş, yeni bir düzenleme yapılması zorunlu hale gelmiştir²⁷². Bu zorunluluğun sonucu olarak da 2017 yılında E-Gizlilik Tüzüğü taslağı hazırlanmıştır. Tüzük taslağı çalışmanın hazırlandığı 2023 yılında henüz yürürlüğe girmemiş olsa da yakın bir gelecekte yürürlüğe girmesi beklenmektedir. E-Gizlilik Direktifinin tüm hükümleri E-Gizlilik Tüzüğü kapsamında da geçerli olacaktır. Bununla birlikte, E-Gizlilik Tüzüğü taslağı birkaç yeni değişiklik getirmektedir²⁷³. *Aksoy ve Halıcıoğlu*’in belirttiği üzere Tüzük ile beraber “çerez kullanım istisnalarının daha net bir çerçeveye oturtulması ve Direktif uygulamalarındaki yoruma açık ve belirsiz konuların önemli ölçüde azalması beklenmektedir. Zira, Tüzük taslağı, çerez uygulamalarına ilişkin olarak, Direktif’ten farklı bir çerçeve ve daha uzun bir istisnalar listesi öngörmektedir”²⁷⁴.

Türk hukukunda ise AB’nin aksine çerezlerle ilgili ayrı bir genel düzenleme bulunmamaktadır²⁷⁵. Ancak, yukarıda açıklandığı üzere çerezler kişisel veri içerebileceğinden KVKK çerezler bakımından da uygulama alanı bulmaktadır. Bu bağlamda, Türk hukuku uyarınca da çerez kullanan site ve uygulamaların KVKK’da

²⁷² Aksoy/Halıcıoğlu, s. 70.

²⁷³ Cookieyes: *ePrivacy Regulation: What Is It & How Does It Affect Cookies*, 2022, (www.cookieyes.com/blog/eprivacy-regulation, Erişim Tarihi: 08.05.20203).

²⁷⁴ Aksoy/Halıcıoğlu, s. 70.

²⁷⁵ Türk hukukunda çerezlerle ilgili tek düzenleme 5809 sayılı Elektronik Haberleşme Kanunu m. 51/3’tür. Ancak ilgili düzenleme sadece elektronik haberleşme hizmeti sunan şirketler yani işletmeciler için getirilmiştir. Bu bağlamda, ilgili madde, idarenin web siteleri için uygulama alanı bulmadığından çalışma kapsamında değerlendirilmeyecektir. 5809 s. Elektronik Haberleşme Kanunu m. 51/3: *Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.*

düzenlenen veri işleme şartlarından birine dayanması gerekmektedir. Hukukumuzda da çerez vasıtasıyla veri işleme faaliyeti kural olarak açık rızaya dayansa da E-gizlilik Direktifinden farklı olarak çerezler bakımından istisnai haller düzenlenmemektedir. Ancak, Kişisel Verileri Koruma Kurumunun yayınladığı çerez rehberi incelendiğinde Direktifte verilen istisna hallerinin KVKK m. 5/2-f’de düzenlenen meşru menfaat kapsamında değerlendirildiği görülmektedir. Bu bağlamda, Kişisel Verileri Koruma Kurumu’nun uygulamasıyla çerezler bakımından veri işleme faaliyeti AB’ye yakınlaştırılmaya çalışılmıştır.

Buna ek olarak, bir hukuka uygunluk sebebine dayanıldığı her durumda KVKK m. 10 uyarınca veri sorumlularının aydınlatma yükümlülüğü bulunmaktadır²⁷⁶. Dolayısıyla, çerez kullanan veri sorumluları çerezler vasıtasıyla kişisel verilerin işlendiğini en geç verilerin elde edildiği sırada kullanıcılara bildirmekle yükümlüdür. Aydınlatma yükümlülüğünün ayrıntıları ise 10 Mart 2018 tarihinde yayınlanan “Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ”de belirlenmiştir²⁷⁷.

Kişisel Verileri Koruma Kurumu’nun 23.12.2022 tarihli ve 2022/1358 sayılı Kararından görüleceği üzere, Kurum çerezlerle ilgili açık rıza ve aydınlatma metninin sunulması gerektiği, açık rızanın ise aktif bir hareketle verilmesi gerektiğini kabul etmektedir²⁷⁸.

²⁷⁶ Kişisel Verileri Koruma Kurumu: *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu*, (<https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU>, Erişim Tarihi: 11.05.2023).

²⁷⁷ Bkz: RG, T. 10.03.2018, S. 30356.

²⁷⁸ Kişisel Verileri Koruma Kurulunun 23/12/2022 tarihli ve 2022/1358 sayılı Karar Özeti, (<https://www.kvkk.gov.tr/Icerik/7595/2022-1358>, Erişim Tarihi: 17.06.2023).

E-devlet kapsamında hizmet veren kamu kurumlarının web sitelerinin de yukarıdaki düzenlemelere uyması gerektiği açıktır. Zira, kamu web siteleri de farkında olarak veya olmadan birçok çerez barındırmaktadır. Vatandaşlar için zorunlu ve vazgeçilmez hizmetlerin sunulduğu ve ülkenin büyük bir çoğunluğunun kullandığı²⁷⁹ bu sitelerdeki çerezlerin gerektiği gibi denetlenmemesi de veri koruma hukuku bakımından büyük sorunlara sebebiyet verecektir. Ancak, E-devletin potansiyel riskleri şu ana kadar çok çalışılmış bir konu olsa da kamu sitelerinde çerez toplanması konusu yeterince dikkat çekmemiş ve hem idare nezdinde hem de doktrinde göz ardı edilmiştir. *Gotze/Matic/ Iordanou/Smaragdakis/Laoutaris*'in G20 ülkelerine ait 5.5 bin devlet sitesini²⁸⁰ inceledikleri çalışmada ortaya koyduğu üzere, bazı ülkelerde kamu sitelerinin %90'ı kullanıcıdan herhangi bir rıza almadan üçüncü taraf çerezlerini kullanmaktadır. Bunun yanında G20 devlet web sitelerinde oluşturulan çerezlerin %50'sinden fazlası üçüncü taraflara aittir²⁸¹. Ülkemizdeki kamu web siteleri de genel olarak incelendiğinde neredeyse hiçbir sitede çerez bildirimi yapılmadığı ve bazı sitelerde pazarlama çerezlerinin de kullanıldığı görülmektedir²⁸². Benzer bir durum yaşanan Fransa'da veri koruma otoritesi *National Commission on Informatics and Liberty* (CNIL) 01.10.2020 tarihinde bir çerez rehberi yayınlayarak tüm kamu

²⁷⁹ Bu kapsamda, Nisan 2023 itibarıyla e-Devlet Kapısı'nın kullanıcı sayısı 63.193.741'dir. Bkz: Türkiye.gov.tr, *e-Devlet Kapısı Kullanıcı İstatistikleri*, (<https://www.turkiye.gov.tr/edevlet-istatistikleri?kullanici=Istatistikleri#:~:text=33.271.014&text=Son%201%20Yıla%20Ait%20Aylara,kadin%20ve%20erkek%20kullanici%20sayısıdır>, Erişim Tarihi: 01.07.2023).

²⁸⁰ Çalışma kapsamında incelenen ülkeler; Arjantin, Avustralya, Brezilya, Kanada, Çin, Fransa, Almanya, Hindistan, Endonezya, İtalya, Japonya, Meksika, Rusya, Suudi Arabistan, Güney Afrika, Güney Kore, Türkiye, İngiltere ve ABD'dir.

²⁸¹ Gotze, M./ Matic, S./ Iordanou, C./ Smaragdakis, G./ Laoutaris, L.: *Measuring Web Cookies in Governmental Websites*, WebSci '22: 14th ACM Web Science Conference 2022, s. 44-45.

²⁸² İnternet sitelerinde kullanılan çerezleri kontrol edebilmek için çeşitli uygulamalar bulunmaktadır. Bkz: <https://www.cookiebot.com>.

kurumlarına internet siteleri ve uygulamalarını rehberine uygun hale getirmeleri için altı aylık bir süre tanımıştır²⁸³.

Özel sektördeki veri sorumluları bakımından çerez yükümlülüklerine uyulmaması idari para cezası ile yaptırıma bağlanırken, kamu kurumları için, en azından ülkemiz bakımından, böyle bir durum söz konusu değildir. Bazı ülke düzenlemelerinde veri koruma mevzuatına uymayan kamu kurumlarına idari yaptırım uygulanabilmesi mümkün kılınsa da²⁸⁴ KVKK’da idari yaptırımlar sadece gerçek kişiler ile özel hukuk tüzel kişilerine uygulanmaktadır. KVKK m. 18/1’de düzenlenen eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde ise kamu görevlileri hakkında disiplin hükümlerinin uygulanacağı öngörülmektedir.

Bu noktada kamu kurumlarına veri koruma hukuku kapsamında idari para cezası kesilememesinin altında yatan düşüncenin kısaca açıklanmasında kanımızca fayda bulunmaktadır. Kamu kurum ve kuruluşlarına idari para cezası uygulanması olasılığı caydırıcı bir etkiye sahip olsa da aynı zamanda kurumların kamu hizmeti sunması için mevcut bütçelerini azaltacaktır. Para cezalarının ödenmesinden kaynaklanan herhangi bir açık, muhtemelen ek bütçe taleplerine yol açacak, bu da

²⁸³ Wessel-Tolvig, B.: *CNIL to Enforce Cookie Rules in France*, Cookie Information 2021, (<https://cookieinformation.com/resources/blog/cnil-to-enforce-cookie-rules-in-france/>, Erişim Tarihi: 27.06.2023); Altı aylık süreden sonra ise yükümlülükler uymayan kurumlara yaptırım tehdidiyle tekrar bildirim yapılmıştır. Bkz: CNIL: *Refusing Cookies Should Be as Easy as Accepting Them: The CNIL Continues Its Action and Issues New Orders*, (www.cnil.fr/en/refusing-cookies-should-be-easy-accepting-them-cnil-continues-its-action-and-issues-new-orders, Erişim Tarihi: 17.06.2023).

²⁸⁴ GDPR kamu kurumlarına idari para cezası kesilip kesilemeyeceği konusunda takdir yetkisini üye devletlere bırakmaktadır (m. 83/7). Örneğin, Almanya’da federal kamu kurumlarına idari para cezası verilemezken, eyaletlerin kamu kurumlarına idari para cezası verilebilmektedir. Bkz: Federal Data Protection Act (BDSG) m. 43. İrlanda Veri Koruma Kanunu Taslağı’nda da kamu kurumlarına idari para cezası kesilemeyeceği öngörülmekteyken gelen tepkiler sonucunda yürürlükteki kanun metninde kamu kurumlarına da idari para cezası verilebileceği açık şekilde düzenlenmektedir. Bkz. Irish Data Protection Act 2018 m. 141.

süregelen bir fon akışına neden olacaktır. Ayrıca kamu kurum ve kuruluşlarına idari para cezası uygulanmaması, kamu ve özel kuruluşların aynı pazarda faaliyet gösterdiği alanlarda (örneğin, özel ve kamu hastaneleri), rekabetin bozulmasına yol açabilecektir²⁸⁵.

Bunun yanında, kanuni yükümlülüğünü yerine getirmeyen idarenin bu davranışının bir hizmet kusuru oluşturduğu açıktır. Ancak, çerez yoluyla e-devlet üzerinden kişisel verileri işlenen bireylerin tam yargı davası açarak idareden manevi tazminat talebinde bulunmaları da mümkün gözükmemektedir. Danıştayın belirttiği üzere manevi zarar;

*“(...) kişinin fizik yapısının ve iç huzurunun bozulmasını, yaşama gücünün ve sevincinin azalmasını, kişilik haklarının zedelenmesini, şeref ve haysiyetinin rencide edilmesini, duyulan acı ve ızdırabı, kişinin günlük yaşamını zorlaştıran her türlü üzüntü ve sıkıntıyı ifade etmekte, fiziki veya manevi acılar duyan, ruhsal dengesi bozulan, yaşama sevinci azalan kişinin manevi yönden zarara uğramış olduğu kabul edilmektedir”*²⁸⁶.

Kısacası manevi zarar kişinin şahsiyet haklarına karşı bir tecavüz sonucunda bireyin elem, acı ve ızdırıp duyması anlamına gelmektedir. Ancak, kişilik haklarına yapılan her tecavüzün birey nezdinde böyle bir etki yaratacağını söylemek mümkün değildir²⁸⁷. Kanımızca, çerezler vasıtasıyla hukuka aykırı şekilde kişisel verilerin işlenmesi bireyler üzerinde manevi zarar doğuracak kadar bir acı yaratmamaktadır. Kişisel verilerin korunmasının ülkemizde Anayasal bir hak olarak düzenlendiği de göz

²⁸⁵ Data Protection Bill 2018: Second stage. Seanad E’ ireann debate, 08,02,2018, C. 255 S. 14, <https://www.oireachtas.ie/en/debates/debate/seanad/2018-02-08/9/> (Erişim Tarihi: 02.07.2023).

²⁸⁶ Dan.,15. D, T. 08.06.2016, E. 2016/399, K. 2016/4145, (Lexpera).

²⁸⁷ Oğuzman,M. K./ Öz, T.: Borçlar Genel Hükümler Cilt II, İstanbul 2014 s. 264.

ardı edilmemelidir. Bu bağlamda, çerezler vasıtasıyla özel hayata saygı hakkının ihlal edildiği ve kişilerin bireysel başvuru yoluyla AYM'ye başvurabileceği akla gelen bir diğer olasılıktır. Fakat kanımızca, *de minimis non curat preator* (küçük şeyler hâkime götürülemez) ilkesi gereğince çerezler dolayısıyla doğduğu iddia edilen zararları bireysel başvuru yoluyla tazmin etmek de mümkün değildir.

III. Kamu Sektöründe Açık Veri ve Verinin Yeniden Kullanımı (*Data Reuse*)

Verinin yeniden kullanımı terimi bir verinin toplanma amacı dışında başka bir amaçla tekrar işlenmesini ifade etmektedir^{288,289}. Verinin yeniden kullanımının birçok faydası olduğu aşikârdır. Mevcut veri setlerinin başka verilerle birleştirilmesi sayesinde daha geniş kapsamlı ve doğru bulgular elde edilebilmesinin yanı sıra verinin yeniden kullanımı, veri toplamak için harcanan süreyi ortadan kaldırarak çalışmaları önemli ölçüde hızlandırmakta ve dolayısıyla üretkenliği arttırmaktadır. Bunun yanında, aynı verilerin birden çok kez toplanmasının önüne geçerek finansal kaynakların daha verimli kullanılmasını sağlamaktadır²⁹⁰.

²⁸⁸ Zimmerman, A.: *New Knowledge From Old Data: The Role of Standarts in the Sharing and Reuse of Ecological Data*, Science, Technology&Human Values 2008, C. XXXIII, S. 5, s.634.

²⁸⁹ Verinin yeniden kullanımı (*Reuse*) ifadesini verinin toplanma amacı dışında başka bir amaçla kullanılıp kullanılmadığına bakılmaksızın verinin bir defadan çok işlenmesi için de kullanan yazarlar bulunsu da bu çalışmada verinin yeniden kullanımı terimi için yukarıdaki tanım kabul edilmektedir. Bkz. Custers, B./ Ursic, H.: *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection*, International Data Privacy Law 2016, C. VI, S.1, s. 6-10.

²⁹⁰ Piwowar, H.A./ Vision, T.J.: *Data Reuse And The Open Data Citation Advantage*, PeerJ 2013, (<https://peerj.com/articles/175/>, Erişim Tarihi: 07.03.2023); University of Wisconsin-Madison Research Data Services: *The Benefits of Reusing Research Data*, 2020, (<https://researchdata.wisc.edu/uncategorized/the-benefits-of-reusing-research-data/#:~:text=It%20saves%20time%20and%20resources,dramatically%20accelerate%20your%20own%20work.>, Erişim Tarihi: 07.03.2023).

Kamu sektöründeki verilerin yeniden kullanımı ise ayrı bir öneme sahiptir. Zira, yukarıda belirtildiği üzere idare sosyal, siyasi, ekonomik, hukuki, coğrafi, çevresel, meteorolojik, turistik, ticari vb. birçok faaliyet alanında geniş bir yelpazede bilgi toplamakta, üretmekte, çoğaltmakta ve yaymaktadır. Bu bağlamda, idare tarafından toplanan veriler, topluma fayda sağlayabilecek geniş, çeşitli ve değerli bir kaynak havuzu oluşturmaktadır. Bu kaynak havuzunun kamu yararına en çok fayda sağlayacak şekilde kullanma yöntemi ise idarenin bu verileri açık veri olarak yayınlamasıdır. Zira, yeniden kullanımı içinde barındıran ve yeniden kullanımdan bağımsız bir şekilde düşünülemeyecek açık veri, kamu sektörü bilgisinin daha geniş kitlelere ücretsiz bir şekilde yayılmasını sağlamaktadır.

A. Açık Veri (*Open Data*) ve Kamusal Veri (*Public Data*) Kavramları:

En basit tabiriyle açık veri, herkesin erişebileceği, kullanabileceği ve paylaşabileceği veridir. Açık verinin kullanılabilir hale gelmesi için, yaygın ve makine tarafından okunabilir bir formatta sunulması gerekir. Bunun yanında, açık verinin, verileri dönüştürme, birleştirme ve başkalarıyla paylaşma dahil olmak üzere istenildiği şekilde, hatta ticari olarak bile kullanımına izin verecek şekilde lisanslanması gerekmektedir. *Data.europa*’ya göre bir veriyi “açık” olarak tanımlayabilmek için üç unsurun varlığı gerekmektedir²⁹¹:

²⁹¹ Çalışmanın ilerleyen kısmındaki Açık verinin unsurları hakkındaki bilgiler, Data.Europa: *What Is Open Data?* (<https://data.europa.eu/elearning/en/#/id/co-01>, Erişim Tarihi: 08.03.2023) kaynağından derlenmiştir.

- Sınırlama: Verilerin açık olabilmesi için belirli bir şekilde kullanılmasını engelleyecek sınırlamaların bulunmaması gerekir. Herkes verileri kullanmakta, değiştirmekte, birleştirmekte ve ticari amaçlar da dahil olmak üzere paylaşmakta özgür olmalıdır.
- Ücret: Açık verilerin kullanımı ücretsiz olmalıdır, ancak bu veriye erişimin ücretsiz olması gerektiği anlamına gelmemektedir. Ücretlendirmenin temel nedeni kullanılabilir verileri oluşturma, sürdürmenin ve yayınlamanın genellikle bir maliyeti bulunmasıdır. Bunun yanında gerçek zamanlı veriler ve büyük veriler, güvenilir hizmet sunumuyla ilgili devam eden maliyetlere neden olabilir. İdeal olarak, açık verilere erişim için belirlenen ücret, talep edilen veri biriminin makul yeniden üretim maliyetinden, yani veriyi kullanacak kişi tarafından yeniden üretilmesinden fazla olmamalıdır.
- Tekrar Kullanım: Kullanıcı açık verileri aldıktan sonra, yeniden kullanmakta ve yeniden dağıtmakta (ticari olarak amaçlar da dahil olmak üzere) özgürdür. Bu bağlamda, açık veri, nasıl kullanıma sunulduğuyla değil, ne için kullanılabileceğiyle ölçülmektedir. Biçim, yapı ve makine tarafından okunabilirlik gibi özelliklerin tümü, verileri daha kullanılabilir hale getirirse de verileri açık hale getiren bu özellikler değildir.

Açık veriden daha geniş bir kavram olan kamusal veriyse, kamusal alandaki tüm bilgiler olarak tanımlanabilir. Kamusal veri terimi devlet veri portalındaki aylık güncellenen veri setlerinden, yalnızca bilgi edinme hakkı talepleri yoluyla erişilebilen PDF dosyalarına kadar her şeyi kapsamaktadır. Bu bağlamda, açık veri esasen kamusal verinin bir alt kümesini oluşturmaktadır. Başka bir ifade ile, her açık veri aynı zamanda bir kamusal veriyken her kamusal veri açık veri değildir. Açık veriyle kamusal verinin

arasında, yukarıda sayılan unsurların yanı sıra bir diğer fark ise, açık veriye erişimin kolay olmasıdır. Buna karşın kamusal veriler her ne kadar tanımı gereği kamunun ulaşabileceği veriler olsa da bu verilere erişim pratikte her zaman kolay olmamaktadır. Çoğu durumda bu verilere erişim için bilgi edinme hakkı kapsamında başvuru yapılması ve uzun süre beklenilmesi gerekmektedir²⁹².

Tanımlardan anlaşılacağı üzere, açık veri ve kamusal veri hem kamu kurumları hem de özel sektördeki kurumlar tarafından sağlanabilmektedir. Ancak, çalışmada açık veri ve kamusal veri terimleri; kamu kurumları tarafından sağlanan veriler için kullanılacaktır. Bu bağlamda, çalışmada kullanılan açık veri tanımı şu şekildedir: Açık (Devlet) Veriler²⁹³, kamu kuruluşları tarafından toplanan, üretilen veya bedeli ödenen, kamu sektörü bilgisi olarak da adlandırılan ve herhangi bir amaçla yeniden kullanım için ücretsiz olarak kullanıma sunulan bilgilerdir²⁹⁴.

B. Açık Verinin Faydaları ve Açık Veriden Değer Yaratma

Verilerin açık bir şekilde yayınlanmasının ardında yatan motivasyon bu eylemin; vatandaşlara, işletmelere ve kamu idarelerine muazzam faydalar sağlayacağı inancıdır. Gerçekten de açık veri sağlık, gıda güvenliği, eğitim, iklim, akıllı ulaşım

²⁹² Kerle, I.: *What Is Public Data?* (<https://enigma.com/blog/post/what-is-public-data>, Erişim Tarihi: 09.03.2023); Opendatasoft: *Public Data*, 2023, (www.opendatasoft.com/en/glossary/public-data, Erişim Tarihi: 09.03.2023).

²⁹³ Türkçe’de “Açık Yönetişim Verisi” olarak da adlandırılmaktadır. Bkz. Gündem, F.: *Açık Yönetişim Verisi (Open Government Data) Uygulamaları ve İzmir’de Yerel Fiyatlar*, İzmir Büyükşehir Belediyesi Açık Veri Portalı 2022, (<https://acikveri.bizizmir.com/tr/showcase/acik-yonetisim-verisi-open-government-data-uygulamaları-ve-izmir-de-yerel-fiyatlar>, Erişim Tarihi: 09.03.2023).

²⁹⁴ Data.Europa (What Is Open Data), (<https://data.europa.eu/en/trening/what-open-data>, Erişim Tarihi: 09.03.2023).

sistemleri ve akıllı şehirler gibi çeşitli alanlarda fayda sağlamakta ve ekonomik büyüme, istihdam yaratma, toplumsal ilerleme için temel bir kaynak olarak kabul edilmektedir²⁹⁵.

Açık veriyle ilgili genel olarak kabul edilen görüş, kamu sektörünün veri sağlayıcı, özel sektörün ise, yeniden kullanıcı olduğudur. Bu görüşün arkasında yatan temel varsayımlar açık veriden bir değer yaratabilecek olanın esas olarak özel sektör olduğu ve kamu kurumları arasında verilerin serbestçe dolaştığıdır²⁹⁶. Her ne kadar özel sektörün açık veriden ekonomik değer yarattığı bir gerçek olsa da bu iki varsayım yanlıştır. Açık veri, dolayısıyla verinin yeniden kullanımı kamu sektörü için de muazzam bir kaynaktır ve büyük bir potansiyel barındırmaktadır. Çeşitli ülkelerdeki kamu kurumları da bu potansiyelin farkına varıp bu konuyla ilgili çalışmalar yürütmektedir²⁹⁷.

Dünya çapındaki ilk Açık Veri yasalarından biri, Güney Kore'nin 2013 yılında yürürlüğe koyduğu “Açık Verilerin Sağlanması ve Kullanımının Teşvik Edilmesi Yasası”dır. Bu yasa, Güney Kore'de kamu verilerine erişimin ve ticari kullanımının yasal temelini oluşturmaktadır. Kanun, Güney Kore'deki kamu kurumlarının kamu verilerini herkes için erişilebilir kılmak için çaba göstermesi ve bu verilere erişimi teşvik edecek tedbirleri alacağını düzenlemektedir²⁹⁸.

²⁹⁵Data.Europa: *The Benefits And Value Of Open Data*, Erişim Tarihi: 17.03.2023). (<https://data.europa.eu/en/publications/datastories/benefits-and-value-open-data>,

²⁹⁶ Van Ooijen, C./ da Silva Carvalho, N./ Iordache, A./Osimo, D.: *Measuring Data Demand Within the Public Sector (Güncellenmiş)*, 2022, s. 9.

²⁹⁷ Van Ooijen/ da Silva Carvalho/ Iordache/ Osimo, s.10.

²⁹⁸ Vancauwenberghe, G./ Crompvoets, J.: *Governance of Open Data Initiatives*, iç.: Open Data Exposed (ed. Bastiaan van Loenen/Glenn Vancauwenberghe/Joep Crompvoets) Information Technology and Law Series, C. XXX, Hague 2018, s. 92; United Nations Asian and Pacific Training Centre. for Information and Communication Technology: *Case Study on Open Government Data Policies and Practices in the Republic of Korea*, s. 3-4.

Başka bir örnek ise, Mayıs 2017'de kabul edilen Alman Açık Veri Kanunu'dur. E-Devlet Yasası'nın bir parçası olan kanun Almanya'daki tüm federal kamu makamlarından veri elde etmek için hukuki bir temel sağlamaktadır. Yasa, federal yönetime bağlı kamu makamlarının, kamu hukuku görevlerini yerine getirdikleri sırada veya üçüncü taraflar aracılığıyla elde ettikleri ham verileri, kamuya açık ağlar üzerinden erişime sunmaları gerektiğini belirtmektedir. Veriler, toplandıktan hemen sonra, ücretsiz olarak, herkes için sınırsız yeniden kullanıma imkân verecek şekilde, makine tarafından okunabilir bir formatta ve ulusal veri portalına dahil edilecek meta verilerle birlikte kullanıma sunulmalıdır. Buna ek olarak, Alman Açık Veri Yasası, verilerini açık veri olarak sunma konusunda diğer kamu makamlarını desteklemek için merkezi bir ofis kurulmasını öngörmektedir²⁹⁹. 2021 yılında ise e-devlet yasasında değişiklik yapan ikinci Açık Veri Yasası çıkartılmıştır³⁰⁰.

AB hukukunda ise, kamu sektörü tarafından tutulan verilere erişimi kolaylaştırmak ve düzenlemek amacıyla 2019 yılında açık veri ve kamu sektörü bilgilerinin yeniden kullanımına ilişkin Direktif (Açık Veri Direktifi) yürürlüğe girmiştir. Bununla birlikte, hükümler yalnızca Avrupa ve ulusal erişim rejimleri temelinde zaten erişilebilir olan veriler için geçerli olup, idarenin verilerini açmasıyla ilgili yeni bir düzenleme getirilmemiştir. Direktif daha ziyade, kamu sektörü organları veya belirli kamu teşebbüsleri tarafından tutulan kamu sektörü bilgilerinin ve kamu tarafından finanse edilen araştırma verilerinin, yeniden kullanımı ve yeniden

(<https://www.unapcict.org/resources/publications/case-study-open-government-data-policies-and-practices-republic-korea>, Erişim Tarihi: 17.03.2023).

²⁹⁹ Vancauwenbergh/ Cromptvoets, s. 92-93; Peters, M.: *Germany Finally Has an Open Data Law*, Open Government Partnership 2017, (<https://www.opengovpartnership.org/stories/germany-finally-has-an-open-data-law/>, Erişim Tarihi: 04.07.2023).

³⁰⁰ Germany Federal Ministry for Digital and Transport: *Open Data*, 2022, (<https://bmdv.bund.de/SharedDocs/EN/Articles/DG/open-data.html>, Erişim Tarihi: 05.07.2023).

kullanıma yönelik pratik düzenlemeleri içeren bir dizi asgari kural sağlayarak ticari veya ticari olmayan amaçlarla ücretsiz olarak yeniden kullanımını kolaylaştırmayı amaçlamaktadır. Ayrıca belirtmek gerekir ki, Açık Veri Direktifi yalnızca kişisel olmayan veriler için geçerli olup³⁰¹ fikri mülkiyet haklarıyla korunan belgeleri³⁰² veya gizli bilgi olarak nitelendirilen belgeleri³⁰³ kapsamamaktadır³⁰⁴.

Ülkemizdeyse her ne kadar açık veri yeni gelişen bir kavram ve uygulama olsa da çeşitli yerel yönetimler ve bazı kamu kurumları son yıllarda açık veri portalları kurmaya başlamıştır³⁰⁵. Ülkemizde şu ana kadar çeşitli strateji ve eylem planlarında açık veri ve kamu sektörü bilgisinin paylaşılmasına değinilmiştir³⁰⁶. Yakın zamanlı önemli bir gelişme Cumhurbaşkanlığı Dijital Dönüşüm ofisi tarafından 2023 Şubat ayında Açık Veri Projesinin duyurulmasıdır. Bu proje kapsamında kamu sektörü bilgisinin paylaşılacağı bir Ulusal Açık Veri Portalı kurulması planlanmaktadır³⁰⁷. Açık verinin kamuya sağlayabileceği faydaları; şeffaflık, kamu hizmetlerinin iyileştirilmesi ve ekonomik değer ile verimlilik sağlanması olarak sıralamak mümkündür.

³⁰¹ Bkz. Açık Veri Direktifi, m. 1/2-h.

³⁰² Bkz. Açık Veri Direktifi, m. 1/2-c.

³⁰³ Bkz. Açık Veri Direktifi, m. 1/2-d.

³⁰⁴ Leistner, M./ Antonie, L.: *IPR and The Use Of Open Data And Data Sharing Initiatives by Public and Private Actors (Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs)*, 2022, s. 39, ([https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2022\)732266](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266) , Erişim Tarihi: 07.07.2023).

³⁰⁵ Örn. İBB Açık Veri Portalı, (<https://data.ibb.gov.tr>, Erişim Tarihi: 07.07.2023); YSK Açık Veri Portalı, (<https://acikveri.ysk.gov.tr/anasayfa>, Erişim Tarihi: 07.07.2023).

³⁰⁶ 2015–2018 Bilgi Toplumu Stratejisi ve Eylem Planı m. 67; 2016–2019 Ulusal e-Devlet Stratejisi ve Eylem Planı hedef 4.2; 2020–2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı m. 19.

³⁰⁷ Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi - Proje Açıklaması, (<https://cbddo.gov.tr/projeler/acik-veri/>, Erişim Tarihi: 25.03.2023)

1. Şeffaflık

Açık verinin en büyük faydalarından biri idare üzerindeki kamu gözetimini arttırarak şeffaflık sağlamasıdır. Mevcut verilerin açık bir şekilde paylaşılması ve kolay bir şekilde işlenmesi sağlandığından, açık veri, kamu denetimi açısından yeni bir yol yaratmakta ve bu sayede hesap verilebilirliği güçlendirmektedir³⁰⁸. Bu bağlamda açık verinin paylaşılmasıyla, toplumun, kamu kaynaklarının ve vergilerin kullanımı, kamu ihalelerinin verilmesi ve siyasi partilerin finansman kaynakları gibi konuları izlemesine olanak sağlanmaktadır. Bunun sonucu olarak da hükümetlerden hesap sormak kolaylaşmakta ve rüşvet gibi yolsuzlukların önüne geçilmektedir³⁰⁹.

Açık verinin bu faydaları sağlayabilmesinin arkasında yatan sebep ise idarenin şeffaflık anlayışı ve halkın bilgiye erişim yöntemlerini değiştirmesidir. İdarenin şeffaflık ve hesap verilebilirliğini sağlamak açısından yerleşmiş bir uygulama olan bilgi edinme hakkı vatandaşların talep etmeleri halinde kamu sektörü bilgisine erişimini sağlamaktadır. Tepkisel şeffaflık (*Reactive transparency*)³¹⁰ olarak tanımlanabilecek bu yöntemde vatandaşların uzun süre beklemesi gerekmektedir. Taleplerine yanıt alamamaları ya da taleplerinin açıkça reddedilmesi durumunda ise bilgiye erişim sağlayabilmek için vatandaşlar, ret işlemine karşı dava açmak zorundadırlar. Açık veri ise, idarenin şeffaflığını tepkisel olmaktan çıkartıp proaktif

³⁰⁸ Ubaldi, B.: *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, OECD Working Papers on Public Governance 2013, No: 22, s. 12-13.

³⁰⁹ Transparency International: *Open Data: Promise, but Not Enough Progress From G20 Countries*, 2019, (<https://www.transparency.org/en/news/open-data-promise-but-not-enough-progress-from-g20-countries>, Erişim Tarihi: 22.03.2023); The World Bank: *Starting an Open Data Initiative*, (<http://opendatatoolkit.worldbank.org/en/starting.html>, Erişim Tarihi: 17.03.2023).

³¹⁰ Tepkisel şeffaflık terimiyle ilgili ayrıntılı açıklama için bkz. Yang, W./ Chuanshen, Q./ Bo, F.: *Do Institutional Pressures Increase Reactive Transparency of Government? Evidence From a Field Experiment*, Public Management Review 2022, s. 2-3.

(*proactive transparency*) hale getirmektedir. Açık verinin getirdiği proaktif şeffaflık, bir talep olmadan kamu sektörü bilgisini kamuya açık hale getirmekte ve bu sayede kişilerin kamu bilgilerine anında erişebilmelerini ve talepte bulunma veya idari usullere dahil olma gibi külfetlerden kaçınmalarını sağlamaktadır^{311,312}. Bu bağlamda, verilerin sürekli olarak, kamuya açık şekilde paylaşılması, halkın politika ve karar alma sürecine katılmak için gerekli bilgilere sahip olmasına da olanak tanımaktadır³¹³.

Her ne kadar hala önemli ve kullanışlı devlet verilerinin büyük bir kısmına erişim sağlanamasa da yolsuzluğa karşı mücadele edilmesi için açık verinin kullanılması hususunda hem ulusal hem de uluslararası kuruluşlar çalışmalarını sürdürmektedir. 2015 yılında açık verilerin yaygınlaşması için çalışan, hükümetler ve uzmanlar arasındaki bir iş birliği ile, Uluslararası Açık Veri Şartı (*International Open Data Charter*) kurulmuş³¹⁴ ve hükümetlerin verileri nasıl yayınlaması gerektiğine ilişkin 6 ilke belirlenmiştir³¹⁵. Aynı yıl G20 ülkeleri Açık Veri Şartı'nın belirlediği prensipleri baz alarak “Yolsuzlukla Mücadele Açık Veri İlkeleri (*Anti-Corruption*

³¹¹ OECD: *Government at a Glance 2011*, 2011, s.142 (https://www.oecd-ilibrary.org/governance/government-at-a-glance-2011_gov_glance-2011-en Erişim Tarihi: 11.07.2023)

³¹² Türk doktrininde bu kavramları aktif ve pasif şeffaflık olarak tanımlayan yazarlar olmakla beraber kanaatimizce tepkisel ve proaktif terimleri daha doğru bir kullanımdır. Aktif ve Pasif şeffaflık kavramları için bkz. Döner, A.: Şeffaf Devlette Bilgi Edinme Hakkı, İstanbul 2010, s. 29-32.

³¹³ Darbshire, H.: *Proactive Transparency: The Future of the Right to Information?*, World Bank Group, Governance Working Paper Series: 56598, 2010. s. 3.

³¹⁴ Uluslararası Açık Veri Şartı (*International Open Data Charter*) tarihçesi için bkz. (<https://opendatacharter.net/our-history/>, Erişim Tarihi: 22.03.2023).

³¹⁵ Bu ilkeler verilerin şu özellikleri taşımasını zorunlu kılar:

1. Varsayılan olarak açık olmak.
2. Zamanında ve kapsamlı olmak.
3. Erişilebilir ve kullanılabilir olmak.
4. Karşılaştırılabilir ve birlikte çalışabilir olmak.
5. Daha iyi yönetim ve vatandaş katılımı için olmak.
6. Kapsayıcı kalkınma ve inovasyon için olmak.

Open Data Charterın bu ilkelerine dayanarak bazı devletler de kendi açık veri politikalarını yayınlamıştır. Bkz. Queensland Government: Queensland Government Open Data Policy Statement, (<https://www.data.qld.gov.au/resources/documents/qld-data-policy-statement.pdf>, Erişim Tarihi: 06.04.2023).

Open Data Principles)”ni kabul etmiştir³¹⁶. Bunun yanında G20 Yolsuzlukla Mücadele Çalışma Grubu'nun (ACWG) talebi üzerine 2015 yılında OECD tarafından açık veri politikaları ve girişimlerinin faydaları konusunda farkındalık yaratmak amacıyla “Yolsuzlukla Mücadele İçin Açık Veri Kullanımına İlişkin İyi Uygulamalar Derlemesi” çıkartılmıştır³¹⁷.

Açık verinin yolsuzlukla mücadele için nasıl ve hangi alanlarda kullanılabileceğinin anlaşılması bakımından kamu ihaleleri iyi bir örnektir. Binlerce ihale süreci ve her gün idare tarafından gerçekleştirilen yüzlerce harcama işlemi söz konusu olduğunda, bunların her birini yolsuzluk belirtilerine karşı el ile tek tek denetlemek fiilen imkansızdır. Ancak, yapılandırılmış açık veri setleri sayesinde büyük ölçekli analizler sürekli olarak gerçekleştirilebilir. Bu konuda kullanılan bir yöntem “Kırmızı Bayrak Analizi”dir. Bu yöntemde ihale verileri gibi tek bir veri kümesi veya varlık kayıtları ve harcama verileri gibi birleştirilmiş veri kümeleri kullanılarak değerlendirilebilecek bir dizi gösterge tasarlanır. Daha sonra verileri okumak ve faaliyetleri potansiyel yolsuzluk göstergelerine göre analiz etmek için bir yazılım oluşturulur. Hazırlanan bu sistem belirli kriterler sağlandığında olası bir yolsuzluk riski olduğuna dair kullanıcıyı uyarır. Belirtmek gerekir ki, bu analiz yöntemi yolsuzluğun gerçekleştiğini kanıtlamamakta ancak istatistiksel olarak yolsuzluk gerçekleşme riski yüksek olan konularda idareyi uyarmaktadır³¹⁸. Bu kapsamda, kar amacı gütmeyen

³¹⁶ Ayrıntılı bilgi için bkz. The Group of Twenty: *G20 Anti-Corruption Open Data Principles*, (<http://www.g20.utoronto.ca/2015/G20-Anti-Corruption-Open-Data-Principles.pdf>, Erişim Tarihi: 22.03.2023).

³¹⁷ Ayrıntılı bilgi için bkz. OECD: *G20 / OECD Compendium of Good Practices on the Use of Open Data For Anti-Corruption*, <https://www.oecd.org/corruption/g20-oecd-compendium-open-data-anti-corruption.htm>, Erişim Tarihi: 22.03.2023).

³¹⁸ Open Data Charter: *Open up Guide: Using Open Data to Combat Corruption: Version 2.0*, 2018, s.31, (<https://drive.google.com/file/d/1efBzdh2A4pIOvTGuAaIMzaVm05oBjMzc/view>, Erişim Tarihi: 06.04.2023).

bağımsız bir kurum olan Açık İhale Ortaklığı (*Open Contracting Partnership*) tüm ülkelerde kullanılabilecek genel bir “kırmızı bayrak” çerçevesi çizebilmek için açık veriden faydalanarak çalışmalar yürütmektedir³¹⁹.

Açık verinin şeffaflık bakımından nasıl uygulandığına verilecek bir diğer somut örnekse Güney Afrika’dır. Güney Afrika hükümeti 2016 senesinde Belediye Parası (*Municipal Money*) açık veri portalını kurmuştur. Bu portal yerel yönetimlerin mali hareketleri hakkında verileri, hiçbir maliye eğitimi veya bilgisi olmayan vatandaşlara aktarmayı amaçlamaktadır. Bu kapsamda görselleştirerek sadeleştirme gibi yöntemler kullanıldığı gibi devlet hazinesi tarafından sağlanan veriler de tekrar kullanıma açık hale getirilmiştir³²⁰.

2. Kamu Hizmetlerinin İyileştirilmesi

Açık veri sayesinde kamu hizmetlerinin geliştirilebilme olanağı bulunmaktadır. Özel şirketler açık veriyi kullanarak mevcut kamu hizmetlerinin gelişmesini sağlayacak uygulamalar geliştirmektedirler. Örneğin, Fransız uygulaması *Tranquilien*, açık veriden yararlanarak toplu taşımada; boş koltuklar ve kalkış saatleri, optimum güzergâh gibi bilgiler sağlayarak toplu taşıma araçlarının verimli kullanımını

³¹⁹ Ayrıntılı bilgi için bkz: Wikrent, K.: *Red Flags for Integrity: Giving the Green Light to Open Data Solutions*, Open Contracting Partnership 2016, (<https://www.open-contracting.org/2016/11/30/red-flags-integrity-giving-green-light-open-data-solutions>, Erişim Tarihi: 23.03.2023).

³²⁰ Van Schalkwyk, F.: *Open Data and the Fight Against Corruption in South Africa*, Transparency International 2017, (http://webfoundation.org/docs/2017/04/2017_OpenDataSouthAfrica_EN-2.pdf, Erişim Tarihi: 23.03.2023). Belirtmek gerekir ki, her ne kadar Belediye Parası portalı açık verinin şeffaflık ve yolsuzlukla mücadele amacıyla nasıl kullanılabileceğine iyi bir örnek olsa da, Güney Afrika genel olarak açık veriyi yolsuzlukla mücadele için kullanmakta ve G20 prensiplerini uygulama konusunda başarısızdır.

sağlamaktadır³²¹. Bu bağlamda, açık verinin yaygınlaşmasıyla beraber kamu hizmetinin sunumu da değişikliğe uğramaktadır. Eskiden kamu hizmetinin sunumu için bu tarz uygulamaları geliştiren idarenin kendisiyken günümüzde idare bu işi yavaş yavaş özel sektöre bırakmaktadır³²². Ancak, bu durum idarenin kamu hizmetlerini geliştirmek için açık veriyi hiç kullanmadığı anlamına gelmemektedir. OECD, verinin yeniden kullanımının kamu sektöründe nasıl uygulama alanı bulacağını ve kamu sektörünü nasıl etkilediğini üç başlık altında incelemiştir.

Bunlardan ilki, “öngörücü yönetim”dir (*anticipatory governance*). Öngörücü yönetim, idarenin karar alırken geleceği göz önünde bulundurmaya yönelik sistematik çabalarını ifade etmektedir. Farklı sektör ve kurumlardan sağlanan birçok verinin analiz edilmesiyle birlikte idare, gelecekte oluşacak sorunları tespit etmek ve yaşanacak krizlerle mücadele etmek için varsayımlarda bulunabilir³²³. Örneğin, Fransa’nın *Centre-Val de Loire* bölgesi, Covid-19 aşılmasının durumu ve gelişimini tahmin etmek için Ulusal Halk Sağlığı Kurumu (*Santé Publique France*) tarafından sağlanan verileri yeniden kullanmıştır³²⁴.

İkinci olarak, idare açık veri sayesinde kamu hizmetlerinin sunumunu ve izlediği politikaları geliştirebilir. Açık veri mevcut problemlerin tespit edilmesi, problemden etkilenen grupların/kişilerin belirlenmesi ve toplumun ihtiyaçlarına cevap

³²¹ Data. Europa: *Unlocking Value from Open Data*, (<https://data.europa.eu/elearning/en/module2/#/id/co-01>, Erişim Tarihi: 23.03.2023).

³²² Ubaldi, B.: *Rebooting Public Service Delivery: How Can Open Government Data Help to Drive Innovation?* OECD Comparative Study 2016, s.5, (<https://www.oecd.org/gov/digital-government/rebooting-public-service-delivery.htm>, Erişim Tarihi: 22.03.2023).

³²³ Van Ooijen, C./ Ubaldi, B./ Welby, B.: *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance*, OECD Working Papers on Public Governance 2019, No. 33, s. 18, (<https://doi.org/10.1787/09ab162c-en>, Erişim Tarihi: 22.03.2023); Charalabidis, Y./ Zuiderwijk, A./ Alexopoulos, C./ Janssen, M./ Lampoltshammer, T./ Ferro, E.: *The World of Open Data: Concepts, Methods, Tools and Experiences*, 2018, s. 7.

³²⁴ Van Ooijen/ da Silva Carvalho/ Iordache/ Osimo, s.7.

veren hizmetler geliştirilmesi için kullanılabilir ve bu sayede de idare karar alırken kamu yararına en uygun seçeneği bulabilir³²⁵. Örneğin, *Open Data Institute* açık verinin idare tarafından karar alma aşamasında nasıl kullanılabileceğini göstermek amacıyla *London-Fire* isminde bir site geliştirmiştir. Bu site açık verileri kullanarak Londra'daki hangi itfaiye istasyonunun kapatılmasının ne gibi etkileri olabileceğine dair bilgiler sunmaktadır³²⁶.

Hassas durumdaki birey ve ailelerin tespit edilebilmesi hususunda verilebilecek bir örnekse Birleşik Krallık'taki "çocuk koruma bilgi paylaşım" projesidir. Bu proje bir çocuğun istismar veya ihmal riskini değerlendirmek için sosyal hizmetler ve Birleşik Krallık Ulusal Sağlık Hizmetleri'nin (*National Health Service*) bazı bölümleri arasında veri paylaşımını kolaylaştırmaktadır³²⁷. Her ne kadar bu örnekte açık veri kullanılsa da farklı idari kurumlardaki verilerin paylaşılmasıyla nasıl bir fayda sağlanabileceği göstermektedir³²⁸. İdarenin daha iyi kamu hizmeti sağlayabilmesi için yapması gereken şey kendi kurumları arasında veri paylaşımını kolaylaştırmak değil bu kurumların elindeki verileri açık veriye çevirerek herkesle paylaşmaktır. Bu sayede tüm devlet kurumları da basit bir şekilde bu verilere ulaşabilecektir.

³²⁵ Van Ooijen/ Ubaldi/ Welby, s. 20.

³²⁶ Open Data Institute-London Fire Stations: *Discover*, (<http://london-fire.labs.theodi.org>, Erişim Tarihi: 25.03.2023).

³²⁷ UK Parliament Post: *Sharing Public Sector Data*, Postnote No:664, s. 1-2. <https://researchbriefings.files.parliament.uk/documents/POST-PN-0664/POST-PN-0664.pdf>, Erişim Tarihi: 24.03.2023)

Son olarak, OECD'ye göre, açık verinin kullanılmasının verimliliğin artması ve kamu kaynaklarının daha iyi kullanılması yönünden faydaları bulunmaktadır. Bu özellik ekonomik değer ve verimlilik başlığı altında incelenecektir.

3. Ekonomik Değer ve Verimlilik

Açık veri, yeni hizmetlerin geliştirilmesine ve yeni iş modellerinin oluşturulmasına katkıda bulunduğu gibi kuruluşların daha bilinçli kararlar almasına ve mevcut kaynakları daha iyi kullanmasına da yardımcı olmaktadır. Çeşitli sektörlerdeki işletmeler bilgi toplamak, uygulamalar geliştirmek veya mevcut ürün ya da hizmetleri iyileştirmek için açık verileri yeniden kullanmaktadır³²⁹.

Açık verinin yeniden kullanımının ekonomik etkisi, doğrudan ve dolaylı etkiler olarak değerlendirilebilir. Doğrudan ekonomik etkiler, maliyet tasarrufu veya gelir gibi kazanç sağlayan faydalardır. Dolaylı ekonomik etkiler arasında, açık veri kullanan uygulamalar sayesinde kullanıcıların zaman tasarrufu sağlaması, ilgili pazarların büyümesi ve kamu hizmetlerinde verimlilik artışı sağlanması gibi durumlar gösterilebilir³³⁰. Ayrıca, açık verinin ekonomik etkisi makro veya mikro düzeyde de değerlendirilebilir. Açık veri, kuruluşların yenilikçi yeni iş modelleri başlatmasını sağladığından uzun vadede toplumun geneli için makroekonomik faydalar sağlamaktadır. Makroekonomik etkilere örnek olarak, bir bölgenin veya ülkenin gayri

³²⁹ Data.Europa (Benefits), (<https://data.europa.eu/en/publications/datastories/benefits-and-value-open-data>, Erişim Tarihi: 24.03.2023).

³³⁰ Berends, J./ Carrara, W./ Engbers, W./ Vollers, H.: *Reusing Open Data: A Study on Companies Transforming Open Data Into Economic and Societal Value*, Publications Office of the European Union 2020, s.18.

safl yurtiçi hasılasının büyümesi verilebilir. Mikro düzeyde ise etki, büyük şirketler ve KOBİ'ler tarafından elde edilen gelire bakılarak değerlendirilir.³³¹.

Açık verinin kamu sektörüne etkisi bakımından OECD'nin verdiği bir örnek açık verinin kamu kurumlarının daha verimli ve etkin bir şekilde çalışmasını sağlamasıdır. Açık veri kullanımı sayesinde zamandan ve maliyetten tasarruf edilebileceği için bu kaynakların başka hizmetlere aktarılma olanağı bulunmaktadır. Bunun yanında, bir idarenin halihazırda topladığı verilerin başka bir idarece tekrar toplanmasının önüne geçilerek hem mali yönden hem de zaman bakımından verimlilik sağlanmaktadır³³². *PricewaterhouseCoopers (PWC)* 2017 yılında Danimarka hakkında yayınladığı raporda Danimarka'daki kamu kurumlarının açık coğrafi veriler sayesinde 2016 yılında yaklaşık 22 milyon DKK³³³ tasarruf ettiği tahmininde bulunmuştur. *European Data Portal*'ın 2020 yılında yayınladığı bir çalışmada ise, Danimarka raporundaki verilerin tüm Avrupa Birliği için uygulanabileceği varsayımında açık verinin, Avrupa genelindeki kamu sektöründe 0,25- 14,8 milyar Euro arasında bir potansiyel maliyet tasarrufu yaratabileceği sonucuna varılmıştır³³⁴.

Açık verinin dolaylı ekonomik etkisiyle kamu kurumlarının nasıl tasarruf etmesine olanak sağladığını somut bir şekilde göstermek için verilecek en iyi ve basit örneklerden birisi otomatik çeviri hizmetleridir. Açık veri otomatik çeviri hizmetlerinin gelişmesinde büyük rol oynamaktadır. Zira, bu hizmetlerin geliştirilmesi

³³¹ Osimo, D.: *Rethinking the Impact of Open Data: Towards a European Impact Assessment for Open Data*, Publications Office of the European Union 2023, s. 26 (<https://data.europa.eu/doi/10.2830/911822>, Erişim Tarihi: 24.03.2023).

³³² Van Ooijen/ Ubaldi/ Welby, s. 27, s. 38-39.

³³³ 2016 yılı için ortalama 3.268 milyon dolardır.

³³⁴ Huyer, E.: *The Economic Impact of Open Data: Opportunities for Value Creation in Europe*, Publications Office of the European Union 2020, s.85, (<https://data.europa.eu/doi/10.2830/63132>, Erişim Tarihi: 26.03.2023); PricewaterhouseCoopers: *The Impact of the Open Geographical Data – Follow up Study*, 2017, s.3 <https://sdfe.dk/media/2917052/20170317-the-impact-of-the-open-geographical-data-management-summary-version-13-pwc-qrvkvdr.pdf>, Erişim Tarihi: 28.04.2023).

için bu programların çok büyük miktarda veriyle beslenmesi gerekmektedir. Açık verilerin ücretsiz olarak kullanıma sunulması sayesinde bu hizmeti geliştiren kurumlar büyük bir mali yükten kurtulmaktadır. Örneğin, Google çeviri, hizmetlerini geliştirmek için AB belgelerini kullanmaktadır³³⁵. Kamu kurumları da çeviri hizmetlerinin tamamını insanlara yaptırmak yerine kendi verileri sayesinde gelişen bu otomatik çeviri hizmetlerinden faydalanarak çeviri harcamalarından tasarruf edebilmektedir. Örneğin, *Huyer*'e göre, açık veri, makine çevirilerinin geliştirilmesine yardımcı olarak 24 dile çevrilmesi gereken Avrupa Veri Portalındaki çevirilerde 1,1 milyar Euro potansiyel maliyet tasarrufu sağlayabilir³³⁶.

C. Açık Verinin Kişi Haklarıyla İlişkisi

Yukarıda açıklandığı üzere açık verinin kamu yararı adına pek çok katkısı olsa da açık veri ve kişi hakları arasındaki bağlantının kurulması gerekmektedir. Zira, açık verinin hak ihlallerine yol açma tehlikesi bulunmaktadır. İdarenin topladığı ve içerisinde kişisel verileri barındıran veri setlerinin hiçbir işlem yapılmadan açık veri olarak paylaşılması mahremiyeti ve dolayısıyla özel hayatın gizliliği hakkını ihlal edebilecektir. Bunun yanı sıra, bu durum açık veri uygulamalarının gelişmesi önünde bir engel oluşturmaktadır. İdarenin kişisel verileri hukuka aykırı olarak paylaşması

³³⁵ Open Knowledge: Open Data Handbook: Why Open Data? (<https://opendatahandbook.org/guide/en/why-open-data/>, Erişim Tarihi: 24.03.2023); Regner, E.: *Parliamentary Question: Translated EU Documents Used by Google to Develop Its Language Software*, E-3436/2010, European Parliament, European Union 2010, (www.europarl.europa.eu/doceo/document/E-7-2010-3436_EN.html, Erişim Tarihi: 28.04.2023).

³³⁶ Huyer, s.72, s. 86.

vatandaşların idare ile daha az veri paylaşmak istemesine yol açacağı gibi³³⁷ halk nezdinde açık veri uygulamalarına karşı negatif bir etki yaratacaktır.

Açık verinin sağladığı faydalar ve mahremiyetin korunması birbiriyle çatışan iki unsurdur. Zira, daha az kişisel bilgi içeren veriler mahremiyeti korusa da veriden sağlanacak faydayı azaltmaktadır. Öte yandan, ayrıntılı veriler daha değerli olsa da kişilerin mahremiyetinin ihlal edilmesi kabul edilebilir değildir³³⁸. Bu bağlamda, idarenin açık veri paylaşırken kişisel verilerin korunması ile açık veriden sağlanacak fayda arasında bir denge kurması ve bunu yaparken de kişisel verileri koruyacak önlemler alması gerekmektedir. *The European Data Portal*'a göre iyi bir açık veri programı üç temel unsura dayanmalıdır: Ahlaki açıdan veri yayıncısı veri sahiplerinin mahremiyetini dikkate almalıdır, yasal olarak veri koruma yasasına saygı gösterilmelidir ve pragmatik olarak kamu güveni korunmalıdır³³⁹. Bu unsurların sağlanabilmesi için de idarenin açık verinin paylaşımı sırasında anonimleştirme gibi verilerin belirli bir kişiyle ilişkilendirilmesini engelleyecek, çeşitli kimliksizleştirme (*de-identification*) yöntemlerini kullanması gerekmektedir.

Açık verinin haklarla ilişkisi hususunda incelenmesi gereken önemli bir diğer konu ise, açık veri paylaşımının kişisel verilerin korunmasına ilişkin mevzuat kapsamında hukuka uygun olup olmadığıdır. Hem mevzuatımızda hem de *GDPR*'da belirtildiği üzere kişisel veriler belirli, açık ve meşru amaçlar için toplanır ve bu

³³⁷ Scassa, T.: *Issues in Open Data – Privacy*, iç. The State of Open Data: Histories and Horizons (ed. Tim Davies/ Stephen B. Walker/ Mor Rubinstein/ Fernando Perini), Cape Town ve Ottawa 2019, s. 341

³³⁸ Green, B./ Cunningham, G./ Ekblaw, A./ Kominers, P./ Linzer, A./ Crawford, S.P.: *Open Data Privacy*, Harvard Public Law Working Paper 2017, s.9 (<https://doi.org/10.2139/ssrn.2924751>, Erişim Tarihi: 09.05.2023).

³³⁹ Simperl, E./ Gomer, R./ O'Hara, K.: *Analytical Report 3: Open Data and Privacy*, European Data Portal 2019, s. 3, (https://data.europa.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf, Erişim Tarihi: 09.05.2023).

amaçlarla bağdaşmayacak şekilde işlenemezler³⁴⁰. Ayrıca, yukarıda da açıklandığı üzere kişisel verilerin işlenmesi kanunda öngörülen veri işleme şartlarından birinin varlığı halinde mümkündür³⁴¹. Açık verinin temelini oluşturan yeniden kullanımın bu düzenlemelerle çeliştiği aşıkardır. Zira, yeniden kullanım ile bir veri esas toplanma amacından farklı bir amaçla kullanılmaktadır. Bu bağlamda idarenin açık veri paylaşıırken bu düzenlemelere uyabilmesi için izleyebileceği iki yoldan bahsedilebilir³⁴². İlk olarak, idare açık rıza veya meşru menfaat gibi veri işleme şartlarından birine dayanabilir. Açık rıza şartı dolayısıyla idarenin kişisel verileri toplarken ilgili kişilerden yeniden kullanıma ilişkin açık rıza alması gerekmektedir. Ancak, yeniden kullanım için açık rıza alınsa dahi bu rıza sadece verinin ilk toplanma amacı için geçerli olacaktır. Verinin başka bir amaçla kullanımı için ise ilgili kişiye ulaşıp tekrar rıza alınması gerekecektir. Kanımızca, bu yöntem teorik olarak mümkün olsa da pratik açıdan uygulanması olanaklı gözükmemekte ve açık veri olarak paylaşılacak verileri kısıtlamaktadır. Böyle bir uygulama veriyi yeniden kullanacak kişilere büyük bir külfet yüklediği gibi açık veri olarak paylaşılan verilerin farklı amaçlarla kullanılıp kullanılmadığı veya veri sahiplerinden açık rıza alınıp alınmadığı gibi hususların denetlenmesi de kolay değildir. Bu noktada değinilmesi gereken bir husus ise, bir kişinin açık veri kapsamında, yani verisinin konu sınırlaması olmaksızın özgürce kullanılması için açık rıza verip veremeyeceğidir. Açık rıza metninin asgari içeriğinde veri sorumlusunun kimliği ve işleme sürecinin amacı gibi

³⁴⁰ Bkz. GDPR m.5; KVKK m.4.

³⁴¹ Bkz. GDPR m.6, KVKK m.5.

³⁴² Data.Europa: *Protecting Data and Opening Data*, 2018, (<https://data.europa.eu/en/publications/datastories/protecting-data-and-opening-data>, Erişim Tarihi: 09.05.2023).

bilgilerin³⁴³ yer alması gerektiği göz önünde bulundurulduğunda kanımızca, herkesin herhangi bir amaçla kullanabildiği açık veriye rıza göstermek mümkün değildir³⁴⁴.

Bunun yanında tartışılması gereken son husus bir kişinin verisinin açık veri olarak paylaşılması yönündeki beyanının bu verileri KVKK m.5/2-d kapsamında ilgili kişinin kendisi tarafından alenileştirilmiş veriye çevirip çevirmeyeceğidir. KVKK'nın basın duyurusunda³⁴⁵ ve çeşitli kararlarında³⁴⁶ belirttiği üzere ilgili verinin alenileştirilmiş olması, başka bir ifade ile kamuya açık hale getirilmiş olması kişisel verilerin her türlü amaç için işlenebileceği anlamına gelmemektedir. Bu veriler ancak alenileştirme amacına uygun olarak işlenebilmektedir. Bu bağlamda değerlendirilmesi gereken husus ise alenileştirme amacının sınırsız olup olamayacağıdır. Alenileştirme diğer veri işleme şartlarına kıyasla daha az üzerinde durulan ve çalışılan bir konu olduğundan, bu soruya kesin bir yanıt bulmak kolay değildir³⁴⁷. Kanımızca, her ne kadar açık verilerin kullanımında bir kısıtlama bulunmasa da ilgili kişilerin verilerinin açık veri olarak paylaşılması hususunda verdikleri bir onay sınırsız bir amaçla alenileştirme sayılmamalıdır. Kişilerin iradesi verilerinin açık veriye dönüştürülmesi yönündedir ve açık veriye dönüştürme sınırları belirli bir alenileştirme amacı olarak

³⁴³ Çekin, s. 88.

³⁴⁴ Her ne kadar birden çok amaç için de açık rıza verilebilse de sınırsız ve belirsiz bir amaçlar için rıza vermek kanımızca mümkün değildir.

³⁴⁵ Kişisel Verileri Koruma Kurumu: “Alenileştirme” Hakkında Kamuoyu Duyurusu, (www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU, Erişim Tarihi: 03.05.2023).

³⁴⁶ Bkz. Kişisel Verileri Koruma Kurulu, “İlgili kişinin internet arama motorlarında yapılan aramalardan elde edilen iş yeri e-postasının açık rızası alınmaksızın veri sorumlusu bir pazarlama şirketi tarafından ticarî elektronik ileti gönderilmesi suretiyle işlenmesi” hakkında Kişisel Verileri Koruma Kurulunun 01/09/2022 tarihli ve 2022/861 sayılı Karar Özeti (<https://kvkk.gov.tr/Icerik/7580/2022-861> Erişim Tarihi: 11.07.2023)

³⁴⁷ Açık genomik veri platformlarında alenileştirme şartına dayanılarak veri işlenip işlenemeyeceği ile ilgili çalışma için bkz: Dove, E.S./ Jiahong, C.: *What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)*, International Data Privacy Law 2021, C. XI, S. 2.

kabul edilmelidir³⁴⁸. Belirtmek gerekir ki, bu yöntemle ilgili hususlar pratik değil teorik tartışmalardır. Zira, açık veri uygulamalarında bu yöntem teorik olarak mümkün olsa da pratik zorlukları ve riskleri sebebiyle uygulamada kullanılmamaktadır.

Açık veriden daha fazla verim alabilmeyi ve açık veri programlarının kolay bir şekilde uygulanmasını sağlayacak diğer bir yöntem ise, özel hayatın gizliliğinin korunması kapsamında yapılması gerektiği gibi, verilerin anonimleştirilmesidir. Anonimleştirme neticesinde açık veri “kişisel veri” olarak tanımlanamayacağından GDPR ve ulusal veri koruma mevzuatlarına tabi olmayacaklardır³⁴⁹.

KVKK m.3'te belirtildiği üzere anonim hale getirme, “*kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini*” ifade etmektedir. Her ne kadar bu uygulama hem özel hayatın gizliliği hakkının korunmasını hem de kişisel veri koruma mevzuatlarına uyumu sağlasa da anonimleştirmenin mutlak bir koruma sağladığından söz etmek mümkün değildir. Bir veri tek başına anonim hale getirilmiş olsa bile başka veri setlerinden elde edilen yardımcı verilerle birleştğinde tekrardan kimliği belirli veya belirlenebilir gerçek kişilerle ilişkilendirilmesi yani yeniden kimliklendirilmesi (*reidentification*) tehlikesi her zaman mevcuttur³⁵⁰. Kaldı ki, yayımı sırasında yeniden

³⁴⁸ Bu noktada tartışılacak bir konu ilgili düzenlemelerde (KVKK m.5/2-d, GDPR m.9/2-e) alenileştirmenin “kişinin kendisi” tarafından gerçekleştirilecek olmasıdır. *Dove* ve *Chen*’in belirttiği üzere bu kriter iki şekilde karşılanmaktadır. Veriler, veri sahibinin kendisi tarafından açıkça alenileştirilebilir (doğrudan kendisi tarafından alenileştirme) veya veri sahibi, verilerini kamuya açık hale getirmesi için bir aracıya açık bir işaret verebilir (dolaylı olarak kendisi tarafından alenileştirme). bkz: *Dove/Chen*, s. 31-32. Bu bağlamda idare ile veri paylaşımı sırasında açık veri hususunda gösterilen bir onayın bu kriteri karşıladığını belirtmek gerekir.

³⁴⁹ *GDPR*’nin giriş bölümünün 26. paragrafında belirtildiği üzere anonim hale getirilmiş veriler *GDPR*’ın kapsamı dışındadır.

³⁵⁰ *Simperl/Gomer/ O’Hara*, s.12.; Yeniden kimliklendirmenin nasıl yapıldığıyla ilgili basit örnekler için bkz. The Office of the Information Commissioner Queensland: *Privacy and Public Data Managing Re-identification Risk*, Report No. 1 to the Queensland Legislative Assembly for 2020-21, 2020, s. 7-11, (https://www.oic.qld.gov.au/data/assets/pdf_file/0016/43045/Privacy-and-public-data-managing-re-identification-risk.pdf, Erişim Tarihi: 09.04.2023).

kimliklendirilmesi mümkün olmayan anonim bir verinin, gelişen teknoloji ve ortaya çıkacak yeni teknikler sayesinde ilerleyen zamanlarda yeniden kimliklendirilme riski bulunmaktadır. Bu sebeple, esasen hem ulusal hem de uluslararası mevzuatta düzenlenen tanımından anlaşıldığının aksine anonimleştirmenin esas amacı, yeniden kimliklendirme riskini tamamen ortadan kaldırmak değil, yeniden kimliklendirme riskini belirli bir eşiğin altına düşürmektir³⁵¹. Bu bağlamda, idarenin yeniden kimliklendirme riskini en aza indirecek şekilde anonimleştirme uygulamalarını gerçekleştirerek açık veri paylaşması gerekmektedir. Bu uygulamaların nasıl gerçekleştirilmesi gerektiğiyle ilgili hem doktrin hem de kamu kurumları çalışmalar yürütmekte ve uygun kimliksizleştirme yöntemlerinin kullanılması konusunda idareye yol göstermektedirler³⁵². Örneğin, Avusturalya'nın Queensland eyaletinin Bilgi Komiserliği Ofisi (*Office of the Information Commissioner*) "Gizlilik ve Kamu Verileri Yeniden Kimliklendirme Riskinin Yönetilmesi" başlıklı raporda özetle devlet kurumlarına şu tavsiyelerde bulunmaktadır³⁵³:

1) Yayınlanan tüm verilerin gözden geçirilerek kimliksizleştirilmiş veri içeren veri kümelerinin belirlenmesi,

³⁵¹ European Data Protection Supervisor: *10 Misunderstandings Related To Anonymisation*, s. 4, (https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf, Erişim Tarihi: 09.04.2023).

³⁵² Örn. Amerika Birleşik Devletleri Ticaret Bakanlığı'na bağlı bir kurum olan Ulusal Standartlar ve Teknoloji Enstitüsü (*The National Institute of Standards*) kimliksizleştirme kullanmak isteyen kamu kurumlarına rehberlik etmesi için "Kamu Veri Setlerinin Kimliksizleştirilmesi" raporunu yayınlamıştır. Bkz. (<https://csrc.nist.gov/publications/detail/sp/800-188/draft>, Erişim Tarihi: 09.04.2023); Ülkemizde KVKK anonim hale getirme yöntemlerini açıklayan Kişisel "Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi"ni yayınlamıştır. Bkz. (<https://www.kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20SİLİNMESİ,%20YOK%20EDİLMESİ%20VEYA%20ANONİM%20HALE%20GETİRİLMESİ%20REHBERİ.pdf>, Erişim Tarihi: 09.04.2023); Kanada'nın Ontario eyaletinin Bilgi ve Gizlilik Komisyonu (*Information and Privacy Commissioner of Ontario*) kamu kurumlarına kimliksizleştirmenin temel kavramları ve tekniklerini açıklaması için "Yapılandırılmış Veriler İçin Kimliksizleştirme Yönergesi"ni yayınlamıştır. Bkz. (<https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>, Erişim Tarihi: 09.04.2023).

³⁵³ Office of the Information Commissioner Queensland, s. 3-4.

- 2) Yayınlanan her kimliksizleştirilmiş veri kümesi için bir sorumlu atanması ve kimliksizleştirilmiş verilerin yayınlanmasına ilişkin rol ve sorumlulukların açıkça tanımlanması,
- 3) Karar mercilerine yönelik rehberlik de dahil olmak üzere kimliksizleştirilmiş veri yayınlarını yöneten politika veya prosedürlerin uygulanması ve sürdürülmesi,
- 4) Yeniden kimliklendirme riskindeki değişiklikler için kimliksizleştirilmiş verileri düzenli olarak izlenmesi ve gözden geçirilmesi.
- 5) Kimliksizleştirilmiş verileri yayınlarken yeniden kimliklendirme riskinin uygun şekilde tespit edilerek, değerlendirilerek ve ele alınarak gizliliğin yönetilmesi,

Son olarak belirtmek gerekir ki, açık veri uygulamalarının ilk ortaya çıktığı yıllarda, kişisel veriler doğrudan paylaşılmadığı için, özel hayatın gizliliği açık veri kapsamında bir sorun olarak görülmezken, zaman içerisinde hem uluslararası kuruluşlar hem de çeşitli ülkeler açık verinin yeniden kimliklendirilmesinin doğurduğu tehdidi fark edip buna göre önlemler almaya başlamışlardır. Örneğin, Birleşik Krallık, 2018 yılında yürürlüğe giren Veri Koruma Yasası'nda anonimleştirilmiş verilerin yeniden kimliklendirilmesini m. 171 uyarınca bir suç olarak düzenlemiştir³⁵⁴. 2013 yılında çıkan G8 Açık Veri Şartı da (*G8 Open Data Charter*) özel hayatın gizliliğine ilişkin bir hüküm içermezken, 2015 yılında yayınlanan Uluslararası Açık Veri Şartında açık verinin uygun anonimleştirme içermesi gerektiği düzenlenmiştir³⁵⁵.

³⁵⁴ Bkz. (<https://www.legislation.gov.uk/ukpga/2018/12/section/171/enacted>, Erişim Tarihi: 11.07.2023)

³⁵⁵ Scassa, s. 341; Uluslararası Açık Veri Şartının 1. ilkesindeki düzenleme şu şekildedir: “*Gizlilik mevzuatı ve standartlarına uygun olarak, verileri yayınlanmadan önce anonim hale getirerek hassas, kişisel olarak tanımlanabilir verilerin kaldırılmasını sağlayacağız*”.

İdare tarafından standartlara uyulmaması ve uygun anonimleştirmenin yapılmaması idarenin hizmet kusuruna vücut verecektir. Bu bağlamda, uygun anonimleştirme yapılmaması nedeniyle zarara uğrayan kişiler tam yargı davası yoluyla zararlarının tazminini idareden talep edebileceklerdir. Örneğin, Birleşik Krallık İçişleri Bakanlığı 2013 yılında mültecilerin kişisel verilerinin olduğu bir listeyi anonim şekilde paylaşması gerekirken yanlışlıkla anonim hale getirmeden paylaşmıştır. Kişisel verilerinin internet ortamında yayınlanması ve başka kişilerce indirilmesi üzerine Yüksek Mahkeme, ortaya çıkan manevi zarar sebebiyle içişleri bakanlığı aleyhine tazminata hükmetmiştir³⁵⁶. Ancak, idarenin yükümlülüklerini yerine getirmesine rağmen gelişen teknolojiler dolayısıyla yeniden kimliklendirme yapılması halinde ise hasar/risk ilkesi kapsamında yukarıdaki açıklamalarımız kanımızca bu duruma da uygulanacaktır³⁵⁷.

³⁵⁶ Global Freedom of Expression Columbia University: *TLT v. Secretary of State for the Home Department*, 2016, (<https://globalfreedomofexpression.columbia.edu/cases/tlt-v-secretary-state-home-department/>, Erişim Tarihi: 05.05.2023).

³⁵⁷ Bkz. s. 72-73.

ÜÇÜNCÜ BÖLÜM

İDARİ KOLLUK KAPSAMINDA VERİ İŞLENMESİ

I. İdari Kolluk

A. Kolluk ve Kamu Düzeni Kavramı

Geniş bir kavram olan kolluk hem bir etkinliği hem de bu etkinliği yerine getiren görevlileri ifade etmektedir³⁵⁸. Zabıta ve polis olarak da adlandırılan³⁵⁹ ve devletin güvenlik hizmetlerini sunuş aracı olan kolluk³⁶⁰, kamu düzenini sağlamaya yönelik kamu hizmeti olarak tanımlanmaktadır^{361,362}. Amacı kamu düzenini sağlamak ve korumak olan idari kolluk, *Tan*'ın ifadesiyle, “*toplumsal yaşamın gerektirdiği düzenin sağlanması için, idarenin bireylerin özgürlüklerine karışmasına, sınırlarının belirtilmesi*” olarak tanımlanmaktadır³⁶³.

Görüleceği üzere, idari kolluğun amacı kamu düzeni kavramıyla açıklanmaktadır. Belirtmek gerekir ki, kamu düzeni özel hukuk ve kamu hukukunda farklı anlamlara gelmektedir.

³⁵⁸ Atay, E. E.: İdare Hukuku, 7. Baskı, Ankara 2021, s. 624; Gözübüyük/Tan, s. 325.

³⁵⁹ Atay, s. 624; Gözler, K.: İdare Hukuku, C. II, Güncellenmiş 3. Baskı, Bursa 2019, s. 524.

³⁶⁰ Centel, N. / Zafer, H.: Ceza Muhakemesi Hukuku, Gözden Geçirilmiş 20. Baskı, İstanbul 2021, s.151.

³⁶¹ Gözler/Kaplan, s. 524.

³⁶² Belirtmek gerekir ki kolluğun bir kamu hizmeti olup olmadığı doktrinde tartışmalı bir konudur. Bkz. Akyılmaz/ Sezginer/ Kaya, s. 612, dipnot 97.

³⁶³ Gözübüyük/Tan, s. 625.

Borçlar hukuku bağlamında kamu düzeni; toplumsal huzur, güvenlik, sağlık, iş hayatı veya kamu ahlakı ile ilgili³⁶⁴ toplumun menfaatlerini koruyan hükümlerin ortaya çıkardığı hukuki düzeni ifade etmektedir³⁶⁵.

Milletlerarası özel hukuk kapsamında da yabancı bir kararın tanıma ve tenfizi için o kararın kamu düzenine açıkça aykırı olmaması gereklidir. Kamu düzenine açıkça aykırılık ise Anayasa ve hukuk sisteminin temel ilkeleri ile toplumun örf, adet ve ahlak kurallarının ihlal edilmesi halinde gündeme gelmektedir³⁶⁶. Yargıtay’a göre “*toplumun huzurlu ve uyumlu bir yaşam sürebilmesi uyulması zorunlu hukuki, ahlaki ve vicdani temel kurallarına*” açıkça aykırılık teşkil eden kararlar kamu düzenine aykırıdır³⁶⁷.

İdare hukuku perspektifinden kamu düzeni ise, bireylerin huzur ve güven içerisinde yaşamlarını sürdürebilecekleri bir ortam³⁶⁸, ya da kamusal alanda düzen ve nizamın sağlanarak kargaşanın engellenmesi ve toplumun güvenli bir şekilde yaşamını sürdürebileceği bir ortamın mevcudiyeti olarak tanımlanmaktadır³⁶⁹. İdari kolluk bu bağlamda özgürlükler ve kamu yararı arasında bir denge sağlayarak kişi hak ve özgürlüklerine sınırlamalar getirmektedir³⁷⁰. Ancak, kişi haklarına sınırlama getiren idari kolluğun temel amacını oluşturan kamu düzeni, zaman ve mekana göre değişebilen, soyut ve muğlak bir kavramdır. Bu sebeple kesin kabul gören bir tanımın yapılması mümkün değildir³⁷¹.

³⁶⁴ Tercier, P./Pichonnaz, P./ Develioğlu, M.: Borçlar Hukuku Genel Hükümler, İstanbul 2020, s. 186; Furrer, A./ Muller-Chen, M./ Çetiner, B.: Borçlar Hukuku Genel Hükümler, İstanbul 2021, s. 172.

³⁶⁵ Oğuzman, M.K./ Öz, M. T.: Borçlar Hukuku Genel Hükümler, C.I, İstanbul 2014, s.86.

³⁶⁶ Şanlı, C.: Milletlerarası Özel Hukuk, 8. Baskı, İstanbul 2020, s. 597.

³⁶⁷ Yargıtay, HGK, T. 21.06.2000, E. 2000/1051, K. 2000/1068 (Lexpera).

³⁶⁸ Gözübüyük/Tan, s. 626.

³⁶⁹ Atay, s. 627.

³⁷⁰ Gözübüyük/Tan, s. 626.

³⁷¹ Atay, s. 611.

Doktrin, mevzuat ve yargı kararları incelendiğinde kamu düzeni kavramının belirli unsurları içerdiği görülmektedir. Bu unsurları klasik ve modern anlayış olarak tasniflemek mümkündür. Klasik anlayışa göre kamu düzeni üç unsurdan oluşmaktadır:

a) Kamu güvenliği: Geniş bir kavram olan kamu güvenliği hem devletin korunması³⁷² hem de bireylerin mallarına ve kişilik haklarına yönelik her türlü tehlikenin ve tehdidin önlenmesi anlamına gelmektedir. Bu tehditlerin önlenmesi ile toplumdaki bireyler huzur içinde yaşayabilmektedir³⁷³. Danıştay’a göre “*kişilerin can ve mal güvenliğinin korunması Devletin asli görevidir*”³⁷⁴.

b) Kamu esenliği: Kamu huzuru olarak da adlandırılan³⁷⁵ esenlik, toplumsal yaşamın gerektirdiği sınırın üzerinde düzensizlik ve rahatsızlıkların yokluğu anlamına gelmektedir. Bu bağlamda, kamu esenliğinin sağlanması için toplumun olağan yaşamını olumsuz etkileyebilecek, kabul edilebilir sınırların üstündeki gürültü, toz, kirlilik gibi etkenliklerin bertaraf edilmesi gereklidir³⁷⁶.

c) Kamu sağlığı: Kamu sağlığı her bireyin sağlık hizmetlerinden münferit olarak yararlanması anlamına gelmemekte³⁷⁷, genel sağlığın korunarak toplumun bulaşıcı ve salgın hastalıklardan uzak tutulmasını ifade etmektedir³⁷⁸.

Zaman içerisinde kamu düzeni kavramının değişim göstermesiyle beraber klasik anlayıştaki bu unsurlar yetersiz kalmış ve modern anlayış bu üç unsurun yanında genel ahlak, kamusal estetik, insan onuru, bireylerin kendilerine karşı korunması³⁷⁹,

³⁷² Gözübüyük/Tan, s. 626.

³⁷³ Akyılmaz, s. 583.

³⁷⁴ Dan. 10. D, T. 26.12.2013, E. 2009/9893, K. 2013/9475 (Lexpera).

³⁷⁵ Atay, s.632.

³⁷⁶ Günday, s. 292.

³⁷⁷ Ulusoy, s.530.

³⁷⁸ Günday, s.292.

³⁷⁹ Gözler, s. 526.

ekonomik kamu düzeni ve doğal çevrenin korunmasını da kamu düzeni kavramının içine dahil etmiştir³⁸⁰.

B. Kolluk Türleri

Ülkemizde idari kolluk teşkilatı ve adli kolluk teşkilatı olarak iki farklı kolluk yapılanması bulunmamakta ve bu iki kolluk faaliyetini de aynı kamu görevlileri yerine getirmektedir. Ancak, kamu görevlilerinin ne zaman adli kolluk ne zaman idari kolluk faaliyeti yerine getirdiğinin tespiti hem uygulanacak hukuk hem de davaların görüleceği yargı yerinin belirlenmesi bakımından önem arz etmektedir. Zira, adli kolluğa ceza hukuku kuralları uygulanırken idari kolluğa idare hukuku kuralları uygulanmaktadır³⁸¹. Belirtmek gerekir ki, her ne kadar bu iki kolluk türüne farklı hukuk kuralları uygunsu da iki faaliyetin de organik olarak aynı görevliler tarafından yerine getirilmesi dolayısıyla bir faaliyetin ne zaman adli kolluk ne zaman idari kolluk alanına girdiğini tespit etmek her zaman kolay olmamaktadır³⁸².

İdari kolluk esas itibariyle, kamu düzenini korumak ve bozulmasını önlemekle görevli kolluktur. Bu bağlamda idari kolluk kamu düzenini bozabilecek tehdit ve riskleri önceden tespit ederek gerekli tedbirleri almaktadır. Bu özelliği sebebiyle idari kolluk suç öncesi kolluk veya önleyici kolluk olarak da adlandırılmaktadır³⁸³.

³⁸⁰ Gözübüyük/Tan, s. 629.

³⁸¹ Gözler, s. 527.

³⁸² Gözübüyük/Tan, s. 632.

³⁸³ Akyılmaz/Sezginer/Kaya, s. 625.

Adli kolluğun faaliyet alanı ise kamu düzeni bozulduktan sonra ortaya çıkmaktadır. Adli kolluk karşılaştığı suçu önlemek, failleri tespit etmek, delilleri toplamak, suçluları yakalamak gibi bir suç işlendikten sonra yapılması gereken görevleri yerine getirmektedir³⁸⁴. Bu bağlamda, adli kolluk bastırıcı niteliktedir³⁸⁵ ve bu özelliği sebebiyle suç kolluğu olarak da tanımlanmaktadır³⁸⁶.

Dikkat edilmesi gerekir ki, adli ve idari kolluk arasındaki farklılık adli kolluğun cezalandırıcı, idari kolluğun ise önleyici olmasından kaynaklanmamaktadır. İdari kollukta kimi durumlarda kamu düzeni bozulduktan sonra cezalandırıcı fonksiyon yerine getirerek idari yaptırımlar uygulamaktadır³⁸⁷.

İdari kolluk da kendi içerisinde genel idari kolluk ve özel idari kolluk olarak ikiye ayrılmaktadır. Genel idari kolluk ülke çapında faaliyet gösteren, kamu düzenini sağlamayı amaçlayan kolluktur. Özel idari kolluk ise sadece belirli bir faaliyet alanı için, belirli ve özel gereksinimleri karşılamak üzere yetkili olan kolluktur. Bu ayrım 3201 sayılı Emniyet Teşkilatı Kanunu m. 3'te de belirtilmekte olup, genel kolluk olarak polis ve jandarma sayılırken, özel idari kolluk, genel kolluk dışında kalıp özel kanunlar ile kurulan ve belirli görevleri olan kolluk güçleri olarak tanımlanmaktadır³⁸⁸. Genel kolluğun kapsamına polis ve jandarmanın yanında sahil güvenlik³⁸⁹ ile çarşı ve mahalle bekçileri de girmektedir³⁹⁰.

³⁸⁴ Yenisey,F./Nuhoğlu, A.: Ceza Muhakemesi Hukuku, 9. Baskı, 2021, s.170; Centel/Zafer, s. 155-156.

³⁸⁵ Akyılmaz/Sezginer/Kaya, s. 626

³⁸⁶ Akyılmaz/Sezginer/Kaya, s. 625; Gözübüyük/Tan, s. 631.

³⁸⁷ Gözübüyük/Tan, s. 632.

³⁸⁸ Gözübüyük/Tan, s. 635.

³⁸⁹ 2692 s. 2692 Sahil Güvenlik Komutanlığı Kanunu m. 2: *Bu Kanunda belirtilen görev ve hizmetleri yapmak üzere silahlı bir genel kolluk kuvveti olan Sahil Güvenlik Komutanlığı kurulmuştur.*

³⁹⁰ 7245 s. Çarşı ve Mahalle Bekçileri Kanunu m. 2: *Genel kolluk kuvvetlerine yardımcı olmak üzere, emniyet ve jandarma teşkilatları bünyesinde silahlı bir kolluk olarak çarşı ve mahalle bekçileri istihdam edilir.*

II. Kolluk Faaliyetleri Kapsamında Veri İşleme Uygulamaları

A. Genel Çerçeve

Kişisel verilerin kolluk faaliyetleri amacıyla işlenmesi günümüz toplumunda giderek daha karmaşık ve tartışmalı bir konu haline gelmiş ve bir dizi yasal ve etik kaygıyı da beraberinde getirmiştir. Genel hatlarıyla kişisel verilerin kolluk faaliyeti kapsamında aşağıdaki amaçlarla işlendiği görülmektedir:

Suçun önlenmesi ve tespiti: Kolluk kuvvetleri, kovuşturma için kanıt toplamak da dahil olmak üzere suç faaliyetlerini önlemek ve tespit etmek için kişisel verileri toplayabilir ve işleyebilir.

Ulusal güvenlik: Kolluk kuvvetleri, terörist faaliyetlerin belirlenmesi ve önlenmesi gibi ulusal güvenlik amacıyla kişisel verileri toplayabilir ve işleyebilir.

Kamu güvenliği: Kolluk kuvvetleri, potansiyel tehditleri belirlemek ve acil durumlara müdahale etmek yani kamu güvenliğini sağlamak için kişisel verileri toplayabilir ve işleyebilir.

Her ne kadar kişisel verilerin kullanımı kolluk faaliyetlerinin gerçekleştirilmesi için faydalı bir araç olsa da bu faaliyet sırasında bireylerin mahremiyetinin ve veri koruma haklarının ihlal edilmemesi ve bireylerin haklarıyla kamu düzeni arasında bir denge sağlanması gerekmektedir.

Kolluk faaliyetleri kapsamında kişisel verilerin işlenmesinin ayrıca ele alınması ve genel düzenlemelerden farklı bir rejime tabii tutulmasının önemini fark eden Avrupa Parlamentosu ve Konseyi, GDPR ile aynı zamanda 2016/680 sayılı Kolluk Direktifi'ni³⁹¹ (*Law Enforcement Directive*) (LED)³⁹² yürürlüğe koymuştur. GDPR'ın giriş kısmının 19. paragrafında belirtildiği üzere, kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dahil olmak üzere, kişisel verilerin suçların önlenmesi, soruşturulması, tespiti, kovuşturulması veya cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu tür verilerin serbest dolaşımı GDPR kapsamında değildir. Bu tür veri işleme faaliyetleri bakımından LED uygulama alanı bulmaktadır. Buna paralel olarak GDPR m.2/2-d' de bu amaçlarla yetkili makamlar tarafından işlenen kişisel verilerin GDPR kapsamında olmadığını hüküm altına almıştır. Belirtmek gerekir ki kolluk güçlerinin bu sayılan amaçlar dışında da kişisel veri

³⁹¹ İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü bu direktifinin ismini "Polis ve Ceza Yargılaması Otoriteleri İçin Veri Koruma Direktifi" olarak çevirmiştir. Bkz. İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü: *Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ya da Cezaların İnfazı Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı ile ilgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı yerine geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ Bilgi Notu*, 2019 (<https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-bilgi-notu.pdf>, Erişim Tarihi: 03.05.2023).

³⁹² Direktifin tam ismi, kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunması ve bu verilerin serbest dolaşımına dair 27 Nisan 2016 tarihli ve 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi'dir.

işlemleri mümkündür ve bu durumda genel düzenleme olan GDPR uygulama alanı bulmaktadır.

Amerika Birleşik Devletleri'ndeki yasal çerçeveye bakıldığındaysa kişisel verilerin kolluk faaliyetleri amacıyla işlenmesini özel olarak düzenleyen kapsamlı bir federal yasa olmadığı görülmektedir. ABD yargısal içtihatları incelendiğinde kişisel verilerin kolluk faaliyetleri kapsamında işlenmesi (özellikle de toplanması) karşısında bireylerin haklarının temel olarak ABD Anayasası'nın Dördüncü Değişikliğiyle korunduğu görülmektedir. Esasen kişisel veri kavramından çok önce kaleme alınmış olan ve bireyleri hükümetin makul olmayan arama ve el koymalarına karşı koruyan bu değişiklik zaman içerisinde Yüksek Mahkeme'nin içtihatlarıyla verileri kapsayacak şekilde genişletilmiştir³⁹³. Ancak belirtmek gerekir ki veri koruma bağlamında, Dördüncü Değişikliğin uygulanması, bireylerin iletişim sağlayıcıları gibi üçüncü taraflara gönüllü olarak teslim ettikleri kişisel verilerde mahremiyet beklentisine sahip olmadıklarını savunan “üçüncü taraf doktrini” nedeniyle nispeten sınırlı bir uygulama alanına sahiptir³⁹⁴. Ayrıca, idarenin Dördüncü Değişiklik ve bununla ilgili içtihatları farklı şekilde yorumlayarak bu korumayı bertaraf ettiği de görülmektedir. Son olarak ABD’de Dördüncü Değişikliğin yanında Mahremiyet Yasası (*Privacy Act*), Elektronik İletişim Gizlilik Yasası (*Electronic Communications Privacy Act*) ve Depolanmış İletişim Yasası (*Stored Communications Act*) gibi federal düzeyde çeşitli özel

³⁹³ Harper, J.: *Administering the Fourth Amendment in the Digital Age*, National Constitution Center (<https://constitutioncenter.org/news-debate/special-projects/digital-privacy/the-fourth-amendment-in-the-digital-age>, Erişim Tarihi: 18.04.2023).

³⁹⁴ Bignami, F.: *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* (PE 519.215), Committee On Civil Liberties, Justice and Home Affairs 2015, s. 5, 10.

yasalarda kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi dağınık bir şekilde düzenlenmektedir.

Türkiye’de ise, kişisel verilerin korunması açısından 95/46/EC sayılı direktif baz alınarak KVKK hazırlanmış ve direktife paralel olarak kişisel verilerin “*millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi*”³⁹⁵ tamamen KVKK kapsamı dışında bırakılmıştır. “*Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması*”³⁹⁶ hali de kısmi istisna durumu olarak sayılarak bazı muafiyetler sağlanmıştır. Benzer şekilde, Avrupa Konseyi’nin 108 sayılı Sözleşmesine taraf olan Türkiye, bu sözleşme hükümlerinin devlet kurumlarınca milli güvenlik, savunma ile soruşturma ve suç önleme amacıyla işlenen kişisel verilere uygulanmayacağını beyan etmiştir. 95/46/EC sayılı direktifin yerine geçen GDPR’da da aynı istisna bulunmaktadır. Ancak GDPR, kendisinin önemli bir tamamlayıcısı olan LED ile beraber hazırlanmış ve bu sebeple kolluk faaliyetleri kapsamında veri işlenmesi GDPR’da ayrıca düzenlenmemiştir. Ülkemizde ise KVKK hazırlanırken yürürlükte olmamasına rağmen taslak metni hazır olan LED göz ardı edilmiş ve kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi bakımından genel bir kanun çıkartılmamıştır.

Türk hukukunda kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi ABD örneğine benzer olarak genel hükümle Anayasa’da düzenlenmiş ve bazı özel düzenlemelerde yerini almıştır. 2010 yılındaki değişikle beraber Anayasa’nın özel

³⁹⁵ Bkz. KVKK m. 28/1-c.

³⁹⁶ Bkz. KVKK m. 28/2-a.

hayatın gizliliğini düzenleyen m. 20'ye “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 kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir” hükmü eklenmiştir. Esasen bu düzenleme özel olarak kolluk faaliyetlerine özgü olmasa da bir temel hak olarak bu hükmün kolluk faaliyetleri bakımından da uygulanacağı aşıkardır. Özel düzenlemelere bakıldığında ise, kolluk faaliyetleri kapsamında kişisel verilerin işlenmesinin 2559 sayılı Polis Vazife ve Salahiyet Kanunu³⁹⁷, Adli Sicil Yönetmeliği³⁹⁸, Suç Eşyası Yönetmeliği³⁹⁹ gibi birçok farklı mevzuatta karışık şekilde düzenlendiği görülmektedir⁴⁰⁰. Anayasadaki düzenleme çok genel olduğundan ve özel düzenlemelerdeki maddelerin hepsi de AB'dekine benzer şekilde belirli bir konuyu kısıtlı şekilde düzenlediğinden Türk hukukunda kolluk faaliyeti kapsamında kişisel verilerin işlenmesi bakımından temel kurallar bulunmamakta, dolayısıyla yeterli bir koruma sağlanmamaktadır. Türk hukukundaki bu eksiklik Avrupa Komisyonu raporlarına da yansımıştır. Türkiye 2019 Raporunda Avrupa Konseyi, 2016 yılında yürürlüğe giren LED'e uyumluluk açısından Türkiye'de herhangi bir yasal düzenleme yapılmadığını belirtmiştir⁴⁰¹. 2022 yılında yayınladığı son raporda da Türkiye'nin

³⁹⁷ Bkz. PVSK m. 5.

³⁹⁸ Bkz. Adli Sicil Yönetmeliği m. 13.

³⁹⁹ Bkz. Suç Eşyası Yönetmeliği m. 26.

⁴⁰⁰ Daha çok mevzuat örneği için bkz. 27 Nisan 2016 tarihli 2016/680 sayılı Avrupa Parlamentosu ve Konsey Direktifi Türkçe Tercüme ve Bilgi Notu 2019, s. 14-15 (<https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-bilgi-notu.pdf>, Erişim Tarihi: 18.04.2023).

⁴⁰¹ İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, s. 15; European Commission: Turkey 2019 Report; SWD(2019) 220 final, s. 31, (<https://neighbourhood-enlargement.ec.europa.eu/system/files/2019-05/20190529-turkey-report.pdf> Erişim Tarihi: 11.07.2023).

KVKK'yı AB müktesebatına uyumlu hale getirmesi gerektiğini ve mevzuatın, özellikle kolluk faaliyetlerine ilişkin istisnalar ve Kişisel Verileri Koruma Kurumu'nun bağımsızlığı açısından önemli ölçüde iyileştirilmesi gerektiğini dile getirmiştir⁴⁰².

Yasal düzenlemelerin ötesinde, kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi insan hakları ihlalleri, özellikle de ayrımcılık kapsamında birtakım kaygıları da beraberinde getirmektedir. Örneğin, kolluk güçleri tarafından kullanılan ve öngörücü algoritma (*Predictive Algorithms*) olarak adlandırılan yazılım, kolluğun elinde bulunan veriyi analiz ederek bir suçun işlenme olasılığını, ne zaman ve nerede işleneceğini, fail ve mağdurun kim olacağını tespit etmeye çalışan sistemlerdir⁴⁰³. Bu algoritmaların mevcut verilere ve algoritmayı veriyle besleyen kişiye bağlı olarak belirli bir zümre, etnik sınıf veya bölgeye ön yargıyla yaklaşarak ayrımcılık yapma riski mevcuttur⁴⁰⁴.

Bunun yanında yüz tanıma teknolojileri gibi sistemlerin hatalı çalışması sonucunda bireyler işlemedikleri suçlar nedeniyle tutuklanabilmektedir⁴⁰⁵. Ayrıca, bu etik kaygıların yanında, kolluk görevlilerinin kişisel verileri işlemesi önünde bazı pratik engeller de bulunmaktadır. Teknolojinin gelişmesiyle beraber işlenmesi gereken veri miktarı giderek büyümekte ve önleyici kolluk kapsamında verilerin işlenmesi giderek güçleşmektedir. Bu bağlamda, kolluk personelinin gelişen teknolojilere ayak

⁴⁰²European Commission: *Türkiye 2022 Report*, SWD(2022) 333 final, s. 34 (<https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/Türkiye%20Report%202022.pdf>, Erişim Tarihi: 11.07.2023).

⁴⁰³ Saka, E.: *Polislik Algoritmaları Bağlamında Öngörücü Algoritmalar (Predictive Algorithms) Eleştirel Bir Yaklaşım*, iç. Algoritmaların Gölgesinde Toplum ve İletişim, Alternatif Bilişim 2021, s. 68.

⁴⁰⁴ Tajuelo, G. P.: *How AI Can Be Biased Against Certain Groups of People and What We Can Do to Prevent It*, Medium 2022 (<https://medium.com/latinxinai/how-ai-can-be-biased-against-certain-groups-of-people-and-what-we-can-do-to-prevent-it-7df28bfff0a06>, Erişim Tarihi: 05.07.2023)

⁴⁰⁵ NBC News: *Facial Recognition Tool Led to Mistaken Arrest, Lawyer Says*, 2023 (www.nbcnews.com/tech/security/facial-recognition-tool-led-mistaken-arrest-lawyer-says-rcna64270, Erişim Tarihi: 05.07.2023); Hill, K.: *Wrongfully Accused by an Algorithm*, The New York Times 2020, (www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, Erişim Tarihi: 05.07.2023).

uydurması, çok çeşitli şekillerde veri toplayabilmesi ve veri depolama sistemlerini geliştirmeleri gerekmektedir. Adli kolluk görevine giren, suçluların tespiti ile yakalanması ve kolluk personelinin teknolojik gelişmelere ayak uydurması gibi konular bu çalışmanın kapsamı dışında olduğundan ayrıca incelenmeyecektir.

B. AB 2016/680 sayılı Kolluk Direktifi

1. Amaç ve Kapsam

Her ne kadar 2016/680 sayılı Direktif AB üyesi ülkeler için geçerli bir düzenleme olsa da mevzuatını AB müktesebatıyla uyumlu hale getirmek için çalışan Türkiye bakımından LED örnek alınması gereken bir düzenlemedir. Bu bağlamda, LED'in kolluk faaliyetleri kapsamında kişisel verilerin işlenmesi konusunda getirdiği düzenlemelerin ve GDPR'dan ayrıldığı noktaların incelenmesinde fayda vardır.

LED, kişisel verilerin suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması, cezai yaptırımların infazı ya da kamu güvenliğine yönelik tehditlerin önlenmesi amacıyla yetkili makamlar tarafından işlendiği durumlarda bireylerin korunmasına ilişkin kurallar getirmektedir. Bu direktif sayesinde özellikle mağdurların, tanıkların ve suç şüphelilerinin kişisel verilerinin gerektiği şekilde korunması sağlanmakta, uluslararası düzeyde verilerin korunmasına ilişkin getirdiği

standartlar sayesinde de suç ve terörle mücadelede sınır ötesi iş birliği kolaylaşmaktadır⁴⁰⁶.

Bir veri işleme faaliyetinin LED kapsamına girebilmesi için iki şartın birlikte sağlanması gerekmektedir.

İlk olarak, işleme faaliyeti Direktif m. 1’de sayılan amaçlardan biri kapsamında gerçekleştirilmelidir⁴⁰⁷. Bu bağlamda her ne kadar LED çoğunlukla cezai konularda ve özellikle adli kolluk olarak polis tarafından yürütülen faaliyetlere uygulanmayı amaçlasa da idari kolluk faaliyetleri de bu direktif kapsamına alınmıştır. Dolayısıyla, LED’in sağladığı koruma bir suç isnadına yol açabilecek, kamu güvenliğine yönelik tehditlere karşı koruma amaçlı önleyici kolluk faaliyetlerini ve bu amaçlarla gerçekleştirilen işleme faaliyetlerini de kapsamaktadır⁴⁰⁸.

İkinci olarak, bu amaçlarla gerçekleştirilen işleme faaliyetleri ancak yetkili makamlarca gerçekleştirildiği takdirde LED kapsamına girmektedir. Yetkili makamdan ne anlaşılması gerektiği de yine Direktif’de belirtilmiştir⁴⁰⁹. Buna göre yetkili makam:

a) *kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya*

⁴⁰⁶ Jourová, V.: *How Will The Data Protection Reform Help Fight International Crime?*, European Commission, Fact Sheet 2016, s. 1-2.

⁴⁰⁷ LED m. 1: “(1) *Bu Direktif, kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dâhil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla kişisel verilerin yetkili makamlar tarafından işlenmesine ilişkin olarak gerçek kişilerin korunmasına yönelik kuralları ortaya koymaktadır*”.

⁴⁰⁸ CNIL, *Law Enforcement Directive : What Are We Talking About?*, 2021 (<https://www.cnil.fr/en/law-enforcement-directive-what-are-we-talking-about>, Erişim Tarihi: 06.07.2023).

⁴⁰⁹ Bkz. LED m. 3/7.

*kovuşturulması ya da cezai yaptırımların infazı konusunda yetkili olan herhangi bir kamu makamı veya*⁴¹⁰

*(b) kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dahil olmak üzere, suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezai yaptırımların infazı amacıyla kamu otoritesini ve kamu yetkilerini kullanmak üzere Üye Devlet hukuku tarafından görevlendirilen diğer herhangi bir kurum veya kuruluşu ifade etmektedir.*⁴¹¹

2. LED ile GDPR'ın Farkları

GDPR ile LED arasında her ne kadar benzerlikler bulunsun da⁴¹² bu iki direktifin getirdiği düzenlemeler önemli noktalarda birbirlerinden ayrılmaktadır. Bu farklılıklar kısaca şu şekilde sıralanabilir⁴¹³:

- LED, veri işleme faaliyetinin şeffaf olmasını gerektiren hükümler içermemektedir.
- LED, kolluk görevlilerinin mümkün olduğu ölçüde verileri kategorize etme yükümlülüğünü içermektedir. Örneğin, suç işlediklerine veya işlemek üzere

⁴¹⁰ Örn. Birleşik Krallık yetkili makamları Veri Koruma Kanunu'nun 7 sayılı listesinde belirtmiştir. (<https://www.legislation.gov.uk/ukpga/2018/12/schedule/7/enacted>, Erişim Tarihi: 20.04.2023).

⁴¹¹ Örn. Birleşik Krallık bakımından, ticaret standartları suçlarını kovuşturan yerel makamlar veya çevre suçlarını kovuştururken Çevre Ajansı bu kapsama girmektedir. Bkz. ICO: *Scope and Key Definitions*, (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/scope-and-key-definitions/#2>, Erişim Tarihi: 20.04.2023).

⁴¹² Yetkili makamın yükümlülükleri bakımından benzerlikler için bkz. (<https://www.cnil.fr/en/law-e/nforcement-directive-what-are-we-talking-about>, Erişim Tarihi: 20.04.2023).

⁴¹³ UK The Home Office: *Impact Assessment, Data Protection Bill: Implementing the European Union Law Enforcement Directive*, HO0295, 2019, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711221/Law_Enforcement_Directive_Impact_Assessment.pdf, Erişim Tarihi: 20.04.2023).

olduklarına inanmak için ciddi gerekçeler bulunanlar ile bir suçtan hüküm giymiş olanların ayrılması gerekmektedir⁴¹⁴. Ayrıca, kolluk kuvvetleri mümkün olduğunca gerçeklere dayanan kişisel verilerin, kişisel değerlendirmelere dayanan kişisel verilerden ayırt edilmesini sağlamalıdır⁴¹⁵.

- LED kapsamında veri sahiplerine sunulması gereken bilgi yükümlülüğü GDPR'a oranla daha zayıftır⁴¹⁶.
- LED kapsamında devletler, belirli koşullar altında veri sahiplerinin haklarını (silme dahil) tamamen veya kısmen kısıtlamaya yönelik hükümleri ulusal kanunlarına koyabilmektedir⁴¹⁷.
- LED, bir tüzük olarak yayımlanmış olan GDPR'den daha az AB gözetimi içermektedir.
- GDPR'daki işleme faaliyetinin hukuka uygun olabilmesi için birçok şart sayılmaktadır. Buna karşın LED uyarınca veri işleme faaliyetinin hukuka uygunluğu, işleme faaliyetinin mevzuatta düzenlenen bir görevin yerine getirilmesine bağlanmıştır⁴¹⁸. Direktifin gerçekleştirmeye çalıştığı amaçlar düşünüldüğünde veri sahiplerinden rıza alınmasını beklemek makul değildir⁴¹⁹.

⁴¹⁴ Bkz. LED m. 6.

⁴¹⁵ Bkz. LED m. 7.

⁴¹⁶ Bkz. LED m. 13

⁴¹⁷ Bkz. LED m. 13, m. 15, m. 16.

⁴¹⁸ Bkz. LED m. 8.

⁴¹⁹ Kędzior, M.: *GDPR and Beyond: a Year of Changes in the Data Protection Landscape of the European Union*, ERA Forum 2019, s. 508 (<https://doi.org/10.1007/s12027-019-00549-x>, Erişim Tarihi: 25.05.2023).

- LED, direktife uygun hareket edildiğinin kanıtlanması bakımından GDPR'ye göre daha ağır yükümlülükler getirmektedir. Örneğin, LED kapsamında yetkili makamların log kaydı⁴²⁰ tutma yükümlülüğü bulunmaktadır⁴²¹.

C. Öngörücü Kolluk Faaliyetleri

1. Tanım

Günümüzde veri miktarının artması ve bu verileri işleyebilen teknolojilerin gelişmesinin doğurduğu yeniliklerin bir yansıması da önleyici kolluğun bir uzantısı olan öngörücü kolluk faaliyetlerinde görmekteyiz. Öngörücü polislik olarak da adlandırılan bu faaliyet en temelinde, farklı kaynaklardan veri almak, analiz etmek ve gelecekteki suçları tahmin etmek, önlemek ve bunlara daha etkili bir şekilde müdahale etmek için sonuçların kullanılmasını ifade etmektedir. Öngörücü kolluk, kolluk personelinin ne olduğuna yoğunlaşmak yerine ne olacağına odaklanmaya ve böylelikle suçun önlenmesi için mevcut kaynakları daha verimli bir şekilde kullanmaya sevk etmektedir⁴²². Doktrinde öngörücü kolluğun kesin kabul görmüş ortak bir tanımı

⁴²⁰ Günlük dosyası olarak da adlandırılabilir log kayıtları bilgisayar biliminde; uygulamalardan, işletim sistemlerinden veya cihazlardan gelen olayları, işlemleri, mesajları ve diğer verileri depolayan metinsel bir veri dosyasıdır. Kullanıcılar tarafından gerçekleştirilen eylemlere dayalı olarak bilgi sağlarlar ve bilgi teknolojisi ortamlarının izlenmesinde önemli bir rol oynarlar. Bkz. Wigmore, I.: *Definition log (log file)*, (<https://www.techtarget.com/whatis/definition/log-log-file>, Erişim Tarihi: 25.05.2023).

⁴²¹ Bkz. LED m. 25.

⁴²² Pearsall, B.: *Predictive Policing: The Future of Law Enforcement?*, NIJ Journal 2010, S. 266, s.16-17.

bulunmasa da temel özellikleri konusunda benzer görüşler ileri sürülmektedir. *Meijer* ve *Wessels* doktrindeki farklı tanımlardaki ortak özelliklerden yola çıkarak öngörücü kolluğu şu şekilde tanımlamaktadır: “Öngörücü kolluk, polis müdahalesi, önleme stratejileri ve taktiklerinin geliştirilmesine yardımcı olmak için suç işleme olasılığı yüksek olan bireylerin veya coğrafi alanların tanımlanması ve istatistiksel tahmini adına önceki suçlarla ilgili verilerin toplanması ve analizidir”⁴²³.

Öngörücü kolluk bu bağlamda profillemeye adı verilen bir yöntem kullanmaktadır. Profillemeye esasen sadece öngörücü kolluk kapsamında kullanılan bir yöntem olmayıp hedefli reklamcılık veya sağlık taramaları gibi geniş bir kullanım alanına sahiptir⁴²⁴. Genel tabiriyle profil oluşturma, tahmine dayalı bilgiler oluşturarak karar alma süreçlerinde kullanmak üzere kişisel veya kişisel olmayan verileri otomatik olarak işlemek için kullanılan bir tekniktir⁴²⁵. GDPR ve LED’de de profil oluşturma “bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, 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 tanımlanmaktadır⁴²⁶.

Belirtmek gerekir ki, profillemeye ve öngörücü kolluk bilgi teknolojilerine başvurmadan da gerçekleştirilebilen bir faaliyetlerdir. Ancak bu faaliyetlerden beklenen

⁴²³ Meijer, A./Martijn, W.: *Predictive Policing: Review of Benefits and Drawbacks*, *International Journal of Public Administration*, C. XLII, S. 12, 2019, s.1033.

⁴²⁴ Kaltheuner, F./Elettra, B.: *Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-making in the GDPR*, *Journal of Information Rights, Policy, and Practice* 2017, C. II, S. 2, s. 4.

⁴²⁵ Ferraris, V./ Bosco, F./ Cafiero, G./ D'Angelo, E./ Suloyeva, Y.: *Working Paper: Defining Profiling*, 2013, s. 33, <http://dx.doi.org/10.2139/ssrn.2366564>.

⁴²⁶ GDPR m. 4/4.; LED m. 3/4.

faydanın gerçekten sağlanabilmesi için insan gücüyle incelenmesi pratik olarak imkânsız, çok büyük miktarda verinin analiz edilmesi gereklidir. Bu sebeple teknolojinin gelişmesiyle beraber profil oluşturma faaliyeti büyük miktarda veriyi işlemek için bilgisayar teknolojilerini kullanmaya başlamıştır. Algoritmik profillemeye olarak adlandırılan bu yöntem, verilerdeki korelasyonlara ve kalıplara dayalı olarak kişilerin profilini çıkarmak için farklı teknikler kullanmaktadır⁴²⁷.

Önleyici kolluk faaliyetlerinde kullanılan algoritmaları iki geniş kategoriye ayırmak mümkündür. Bu algoritmalar:

Suç tahmin etme algoritmaları (coğrafi algoritmalar): Bu tip algoritmalar suçların nerede ve ne zaman gerçekleşme olasılığının daha yüksek olduğunu tahmin etmek için yerler, olaylar ve geçmiş suç oranları arasındaki bağlantılardan yararlanır. Örneğin, belirli hava koşulları veya büyük spor etkinlikleri ile suç verileri arasında bağlantı kurar. Bu algoritmalar suç işleme oranı yüksek olan sıcak nokta (*hot spot*) diye adlandırılan alanları belirler ve polis bu noktalarda devriyeler planlar. Bu tip algoritmalarından biri olan ve ABD'de yaygın olarak kullanılan olan PredPol bölgeleri 500'e 500 metrelik bloklara ayırmakta ve tahminlerini gün boyunca güncellemektedir.

Suçluları ve mağdurları tespit etme algoritmaları: Bu tip sistemler, yaş, cinsiyet, medeni durum, ekonomik sınıf, madde bağımlılığı geçmişi ve sabıka kaydı gibi verilerden yararlanarak kimlerin gelecekte suç faaliyetlerine karışma ihtimalinin yüksek olduğunu tahmin etmektedir. Öngörücü profil oluşturma olarak da tanımlanabilecek bu kişi bazlı araçlar, suç işlenmeden önce müdahale etmek için polis tarafından kullanılmasının yanında tutuklanan bir kişinin yeniden suç işleme

⁴²⁷ European Union Agency for Fundamental Rights (FRA): *Preventing Unlawful Profiling Today and In The Future: A Guide*, Luxembourg 2018, s. 19.

olasılığının olup olmadığını belirlemek için mahkemeler tarafından da kullanılabilmektedir⁴²⁸.

Oluşabilecek kavram karmaşasını gidermek adına belirtmek gerekir ki önleyici kolluk ve öngörücü kolluk birbirlerinden farklı kavramlardır. Daha geniş bir kavram olan ve öngörücü kolluğu da kapsayan önleyici kolluk faaliyeti de bir suçun veya tehlikenin oluşmadan önce engellenmesini amaçlamaktadır. Ancak öngörücü kolluktan farklı olarak bir veriye dayanma zorunluluğu bulunmamakta ve kamusal alanların video kameralarla izlenmesi gibi hiçbir suç tahmininde bulunmadan sadece caydırma amaçlı gerçekleştirilen faaliyetleri de kapsamaktadır. Bu bağlamda, öngörücü kolluğu istatistiksel veriler kullanarak önleyici kolluk faaliyeti yerine getirmek olarak tanımlamak mümkündür⁴²⁹. Bunun yanında, öngörücü kolluk algoritmalarının, yani yapay zekanın verdiği kararların idari işlemler açısından nasıl tasnif edilmesi gerektiği sorusunun da düşünülmesi gerekmektedir. Öngörücü kolluk algoritmaları bakımından, sistem doğrudan bir karar almayıp sadece kolluk personeline belirli olasılıklar sunmakta, nihai kararı bu olasılıkları değerlendirerek yetkili kişiler vermektedir. Bu bağlamda algoritmanın verdiği kararlar icrai nitelikte olmadığından dolayı kanımızca idarenin karar niteliğinde olmayan işlemlerinden kabul edilmelidir.

⁴²⁸Heaven, W.D.: *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled*, MIT Technology Review 2020 (www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice, Erişim Tarihi: 07.07.2023); Perry, W.L./McInnis, B./Price, C.C./Smith, S./Hollywood, J.S.: *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation eBooks 2013, s. 8-9.

Perry et al. mağdurların tespitini ayrı bir kategori olarak saymış ve dördüncü bir kategori olarak da işlenmiş bir suçun failinin tespiti için geçmiş suç kaydı verilerinin kullanılmasını da öngörücü kolluk kapsamında kabul etmiştir ancak bu konu adli kolluk kapsamına girdiğinden çalışma kapsamı dışında kalmaktadır.

⁴²⁹ Moses, L.B./Chan, J: *Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability*, *Policing & Society*, C. XXVIII, S. 7, 2018, s. 808.

2. Öngörücü Kolluğun Faydaları ve Riskleri

Öngörücü kolluğun olası suçları ve tehlikeleri daha gerçekleşmeden engellediği için kamu düzenini sağladığı ve koruduğu açıktır. Ayrıca, olası suçlar önceden tahmin edildiğinden mevcut kaynaklar daha verimli bir şekilde kullanılabilir. ABD'de birçok polis teşkilatı, yeniden suç işleme olasılığını hesaplamak veya belirli bir suçun gerçekleşme olasılığını öngörmek amacıyla algoritmalar kullanmaktadır. Örneğin, Santa Cruz polis teşkilatı 2011 yılından bu yana PredPol algoritması gibi suç tahmin araçlarını olası yerleri, suçları ve suç zaman dilimlerini öngörmek için kullanmaktadır⁴³⁰. Öngörücü kolluğun faydalarına başarılı bir başka örnek olarak 2003 yılında ABD'nin Richmond kentinde gerçekleştirilen uygulama da gösterilebilir. Richmond kentinde her yılbaşı yaşanan havaya ateş açılması olaylarını engellemek için polis güçleri geçmiş yıllardaki vakaları inceleyerek o yıl gerçekleşecek olayların zamanını, yerini ve niteliğini tahmin etmiş ve yılbaşı gecesi suçu önlemek ve daha hızlı müdahale etmek için bu noktalara memurlar yerleştirmiştir. Bunun sonucunda rastgele ateş etme olaylarında %47'lik bir azalma ve ele geçirilen silahlarda %246'lık bir artış olduğu gibi teşkilat personel masraflarından 15,000 dolar tasarruf etmiştir⁴³¹.

⁴³⁰ Gültekin Várkonyi, G.: *Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes*, iç. Digital Criminal Justice: A Studybook Selected Topics for Learners and Researchers (ed.:Krisztina Karsai, Adem Sözüer, Liane Wörner) Social Science Research Network, İstanbul 2022, s.2.

⁴³¹ Pearsall, s.17.

Ancak, her ne kadar öngörücü kolluğun kamu düzeninin sağlanması açısından büyük faydaları olsa da bazı risk ve endişeleri de beraberinde getirmektedir.

Her şeyden önce öngörücü kolluk, en temelinde bir veri analizi olduğundan sisteme sunulan girdilere bağlı olarak belirli gruplara veya bölgelere karşı önyargıyla yaklaşma ve bunları hedef alma riskini barındırmaktadır. *Gültekin Várkonyi*'nin belirttiği üzere, sistemi eğiten veri miktarı büyüdükçe küçük grupların temsil gücü azalmakta, bazı veriler sistem için daha az fark edilir hale gelmekte ve bu durum sınıf dengesizliğine yol açmaktadır. Eğer sistem belirli bir grupla ilgili çok fazla eğitilirse, o gruba mensup bir kişinin masum olmasına rağmen potansiyel bir suçlu olarak değerlendirilme olasılığı başka bir kişiye göre daha yüksek olacaktır⁴³². *Lum ve Isaac* tarafından yapılan bir çalışmada, önyargısız olduğu iddia edilen PredPol algoritmasının *Oakland*, Kaliforniya'daki geçmiş uyuşturucu suçu verileri üzerinde eğitildiğinde siyah mahalleleri beyaz mahallelerin yaklaşık iki katı oranında hedef aldığı tespit edilmiş, gelir gruplarına göre analiz edildiğinde ise düşük gelirli mahalleler, yüksek gelirli mahallelere kıyasla orantısız bir şekilde daha yüksek oranlarda hedef alınmıştır⁴³³. Algoritmaların yaptığı bu ayrımcılığın doğurduğu en büyük sorun sistemin ayrımcı sonuçlarının daha çok ayrımcı veri yaratmasıdır. Algoritmaların sağladığı ayrımcı öngörü neticesinde polisler belirli bir bölgeye daha çok yoğunlaşmakta ve bunun sonucu olarak da o bölgede daha fazla suç tespit etmektedir. Sonuç olarak, geri beslenme döngüsü olarak tanımlanan bu durum

⁴³² Gültekin Várkonyi, s. 4-5.

⁴³³ Lum, K. / Isaac, W.: *To Predict and Serve?*, Significance 2016, C. XIII, S. 5, s. 18.

algoritma açısından kaçınılmaz bir kartopu etkisi yaratmakta ve sistemdeki ayrımcılık güçlenmektedir⁴³⁴.

Öngörücü kolluk faaliyetleri kapsamında ikinci problemse şeffaflık ve hesap verilebilirlik noktasında ortaya çıkmaktadır. Fikri mülkiyet hukuku ve genellikle kullanılan algoritmaların karmaşıklığı nedeniyle, kolluk personeli bir algoritmanın ne yaptığını ve neden yaptığını tam olarak anlamak için gereken bilgiye sahip değildir. Hatta, kolluk personeline bu konuda uzman bireyler bulunsa dahi karmaşık bir yapıya sahip olan bu sistemlerin tam olarak nasıl karar verdiğini anlamak kolay değildir. Kara kutu⁴³⁵ olarak adlandırılan bu problem, algoritmanın tahminlerindeki hataların ya da önyargıların tespit edilmesini zorlaştırmakta, öngörücü kolluk sistemlerinin etki mekanizmalarının ve etkinliğinin objektif bir şekilde değerlendirilememesine neden olmaktadır. Günümüzde kara kutu probleminin önüne geçebilmek ve algoritma tarafından verilen kararların insanlar tarafından anlaşılabilmesi adına bazı çalışmalar yürütülmektedir⁴³⁶.

⁴³⁴ Gültekin Várkonyi, s. 5; FRA: *Bias in Algorithms: Artificial Intelligence and Discrimination*, 2022, s. 29-30 (<http://fra.europa.eu/en/publication/2022/bias-algorithm>, Erişim Tarihi: 07.07.2023).

⁴³⁵ Kara kutu yapay zeka, girdileri ve işlemleri kullanıcı veya başka bir ilgili taraf tarafından görülemeyen herhangi bir yapay zeka sistemidir. Kara kutu, genel anlamda, içine girilemeyen bir sistemdir. Kara kutu YZ modelleri, nasıl ulaşıldıklarına dair herhangi bir açıklama yapmadan sonuçlara veya kararlara varır. Kara kutu modellerinde, yapay nöronlardan oluşan derin ağlar, verileri ve karar verme süreçlerini on binlerce nöron arasında dağıtarak, anlaşılması insan beynininki kadar zor olabilecek bir karmaşıklığa neden olur. Kısacası, kara kutu YZ'nin iç mekanizmaları ve katkıda bulunan faktörler bilinmemektedir. Bkz. Yasar, K: *Definition Black Box AI*, (<https://www.techtarget.com/whatis/definition/black-box-AI>, Erişim Tarihi: 23.05.2023).

⁴³⁶ FRA (Bias in Algorithms), s. 36; Gültekin Várkonyi, s.11; Aksoy, H.C.: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, *Kişisel Verileri Koruma Dergisi* 2022, C. IV, S. 2. s. 73.

Yukarıda anlatılan tüm bu sorunların önüne geçebilmek adına Avrupa Birliği Temel Haklar Ajansı (FRA) AB kurumlarına ve AB ülkelerine şu çağrıda bulunmuştur⁴³⁷:

- Önyargı testi gerçekleştirilmesi: Özellikle otomatik karar verme süreçlerinde, kullanım öncesinde ve sırasında yanlılığın test edilmesi sistemdeki önyargıyı azaltacaktır.
- Özel nitelikli verilere ilişkin rehberlik sağlanması: Potansiyel ayrımcılığı değerlendirmek için etnik köken, cinsiyet gibi verilere ihtiyaç duyulabilir. Bu tür veri toplamaya ne zaman izin verildiğine dair rehberlik sağlanması, veri işleme fiilinin gerekli olması ve etkili güvencelere sahip olması gerekmektedir.
- Etnik ve toplumsal cinsiyet önyargılarının değerlendirilmesi: Konuşma, algılama ve tahmin modellerinde etnik ve toplumsal cinsiyet önyargıları güçlüdür. Bunların vaka bazında değerlendirilmesi gerekir. Bu tür değerlendirmelerin kanıta dayalı olması ve denetim organları ile kamuoyuna sunulması gerekmektedir.
- Tüm ayrımcılık temellerinin göz önünde bulundurulması: Önyargılar çok çeşitlidir, dolayısıyla, cinsiyet, din veya etnik köken gibi yasaklanmış tüm ayrımcılık temellerinin değerlendirilmesi gerekir. Bunun yanında, algoritmalarda ayrımcılıkla mücadele etmek için AB'nin hukuki düzenlemelere ihtiyacı vardır.

⁴³⁷ FRA: *Test Algorithms for Bias to Avoid Discrimination*, 2022 (<http://fra.europa.eu/en/news/2022/test-algorithms-bias-avoid-discrimination>, Erişim Tarihi: 20.04.2023).

- Kanıta dayalı gözetim için erişimin artırılması: Yapay zeka sistemlerinin arkasında ne olduğu büyük ölçüde bilinmeyebilir. Etkili gözetim, algoritmalarındaki önyargı riskini belirlemek ve bununla mücadele etmek için verilere ve veri altyapılarına daha iyi erişim gerektirir.

Benzer şekilde *Gerards* ve *Xenidis* Avrupa Komisyonu için hazırladıkları raporda algoritmik ayrımcılığa karşı çözüm yollarının yasal çözümler, bilgiye dayalı çözümler ve teknolojiye dayalı çözümler olarak üçe ayırıp bu üç yöntemin birbiriyle entegre şekilde kullanılmasını gerektiğini ileri sürerek yedi aşamalı bir yaklaşım önermişlerdir⁴³⁸.

Öngörücü kolluk uygulamaları yeni yaygınlaşan bir alan olduğundan bu konudaki yargı kararları bir hayli kısıtlıdır. Yakın tarihli önemli bir karar Alman Federal Anayasa Mahkemesi (*Bundesverfassungsgericht*) tarafından verilmiştir. Almanya'nın Hessen eyaletinde öngörücü kolluk faaliyetleri için 2017 yılından itibaren *Gotham* gözetim yazılımı kullanılmaya başlanmıştır. İdare tarafından tutulan kişisel verilerin mevcut bir suçun soruşturması veya kovuşturması yerine gelecekteki bir suçu engellemek için işlenip işlenemeyeceğini değerlendiren Alman Federal Anayasa Mahkemesi; orantılılık ilkesine ve verilerin toplanma amacı dışında kullanılmasına dayanarak, bu sisteme izin veren kanuni dayanakların "veri analizi veya yorumu için kullanılacak verilerin türü ve miktarı konusunda neredeyse hiçbir kısıtlama getirmediğine", "çok geniş kapsamlı otomatik veri analizi ve

⁴³⁸ Gerards, J./ Xenidis, R.: *Algorithmic discrimination in Europe : challenges and opportunities for gender equality and non-discrimination law*, 2021, s. 151. (<https://data.europa.eu/doi/10.2838/544956>, Erişim Tarihi: 09.08.2023)

yorumlama yöntemlerinin kullanılmasını" yasaklamadığına değinerek öngörücü kolluk faaliyetlerine izin veren düzenlemeleri Anayasa'ya aykırı bulmuştur⁴³⁹.

3. Öngörücü Kolluk Bağlamında Kolluk Direktifi ve Yapay Zeka Yasası

AB'de kolluk faaliyetleri kapsamında kişisel verilerin işlenmesini düzenleyen LED, öngörücü kolluk faaliyetlerini açık bir şekilde düzenlemese de belirli maddelerin bu konuda uygulama alanı bulması mümkündür. Zira direktif profil oluşturma ve otomatik karar vermeyle ilgili düzenlemelere sahiptir.

LED m. 11, AB veya üye devlet yasaları tarafından yetkilendirilmedikçe ve en azından insan müdahalesi elde etme hakkı gibi güvenceler sağlanmadıkça veri sahibini yasal olarak olumsuz etkileyecek sadece otomatik işlemeye dayalı karar verme mekanizmalarını yasaklamaktadır. Bunun yanında m. 27 yeni teknolojilerin kullanılması halinde yetkililere etki değerlendirmesi yapma yükümlülüğü getirmektedir.

Burada, değinilmesi gereken iki önemli husus bulunmaktadır. İlk olarak, LED'in coğrafi algoritmalar kapsamında uygulama alanı bulamaması söz konusu olabilecektir çünkü kişi bazlı algoritmaların aksine coğrafi algoritmalar genellikle kişisel verileri değil toplu istatistikleri kullanmaktadır. Daha önemli ikinci bir durum ise uygulamada m.11'in öngörücü kolluk bağlamında uygulanma olanağının

⁴³⁹ Bundesverfassungsgericht: *Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional*, Press Release No. 18/2023, (<https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html>), Erişim Tarihi: 06.07.2023).

neredeşye hi olmamasıdır. İlgili düzenleme “yalnızca otomatik işleme” faaliyetleri kapsamında uygulanmakta olup, maddenin uygulanması için karar alma sürecinde hiçbir insan faktörü bulunmamalıdır. Ancak öngörücü kolluk kapsamında pratikte böyle bir durumla karşılaşmak en azından günümüz için olası değildir. Zira, algoritmalar belirli sonuçlar elde etse de nihai karar (örneğin, polis personelinin hangi alanlarda yoğunlaştırılacağı) insanlar tarafından verilmektedir. Buna rağmen, nihai kararın verilmesinde memurun takdirinin hi olmadığı kanıtlanabilirse m. 11 uygulama alanı bulacaktır.⁴⁴⁰

Henüz teklif aşamasında olan ve veri kalitesi, şeffaflık, insan gözetimi ve hesap verebilirlik ile ilgili kuralları güçlendirmeye odaklanan⁴⁴¹ Yapay Zekâ Yasası (*AI Act*)’da öngörücü kolluk faaliyetlerine uygulanabilecek düzenlemeler içermektedir. Piyasaya sürüldükten veya hizmete alındıktan sonra öğrenmeye devam eden yüksek riskli yapay zekâ sistemlerini ele alan m. 15/3 uyarınca “*Piyasaya sürüldükten veya hizmete alındıktan sonra öğrenmeye devam eden yüksek riskli YZ sistemleri, gelecekteki operasyonlar için bir girdi olarak kullanılan çıktılar ('geri bildirim döngüleri') nedeniyle olası önyargılı çıktılarının uygun azaltma önlemleriyle gerektiği gibi ele alınmasını sağlayacak şekilde geliştirilmelidir.*”

⁴⁴⁰ Lynskey, O.: *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection From Predictive Policing*, International Journal of Law in Context 2019, C. XV, S. 2, s. 173-174; FRA (Bias in Algorithms), s. 33.

⁴⁴¹ World Economic Forum: The EU’s Artificial Intelligence Act Explained, 2023, (www.weforum.org/agenda/2023/03/the-european-union-s-ai-act-explained, Erişim tarihi: 22.04.2023).

III. İdarenin Özel Sektördeki Kişisel Verilere Erişimi

A. Genel Olarak

Önceki bölümlerde açıklandığı üzere kişisel verilerin işlenmesinin kamu sektörü açısından büyük faydaları bulunmaktadır ve bu faydaların farkına varan devletlerin kişisel verilere erişim talebi giderek artmaktadır. *Cate, Dempsey* ve *Rubinstein'a* göre 21. yüzyılda devletlerin verilere erişim talebinin artması temel olarak üç nedenden kaynaklanmaktadır: Bunlardan ilki; New York, Londra, Madrid gibi şehirlerde yaşanan terör saldırılarının gösterdiği üzere, ulusal güvenliğe yönelik yeni ve ciddi tehlikelerin ortaya çıkması ve nükleer/kimyasal silahlar ile siber güvenlik açıklarına karşı artan endişedir. İkincisi, bireylerin yaşamlarının her yönü hakkında (ilişkileri, hareketleri, mali durumları vs.) rutin olarak üretilen, toplanan ve depolanan dijital verilerin hacmindeki patlama ve bu tür verileri toplamak, depolamak ve veri madenciliği yapmak için kullanılan teknolojilerin gücünde sürekli bir artış olmasıdır. Son neden ise, bu verilerin çoğunun genellikle özel sektördeki servis sağlayıcıları tarafından, hizmeti sağlamak için gerekli bir işlem olarak veya verilerin pazarlama, araştırma veya diğer amaçlar bakımından bağımsız bir değere sahip olmasından dolayı toplanması ve saklanmasıdır. E-posta ve diğer elektronik iletişim araçlarının kullanımı, çevrimiçi veri depolama, kredi ve banka kartı ödemeleri, banka havaleleri, sosyal ağ, uzaktan izleme, fotoğraf ve video paylaşım hizmetleri, tarama ve arama hizmetleri, çevrimiçi alışveriş ve diğer binlerce hizmet çok büyük miktarlarda verinin özel

sektörün elinde tutulması ile sonuçlanmaktadır. Hükümetler bu özel şirketleri hazır, verimli ve uygun maliyetli bir veri kaynağı olarak görmektedir⁴⁴².

Bu bölümde değinilecek esas konu, idarenin özel sektörün elindeki kişisel verilere erişim yollarının neler olduğudur. Her ne kadar günümüz dijital dünyasında devletler, bireyler hakkında önemli miktarda veriyi ellerinde bulundursa da özel sektörün sahip olduğu veri miktarına kıyasla devletin sahip olduğu veri miktarı az kalmaktadır. Bu sebeple, idare kendi topladığı kişisel veriler yanında özel sektörden de veri toplama yoluna gitmektedir. Belirtmek gerekir ki idarenin özel sektördeki kişisel verilere erişimi ve bu verilerin kullanılması esasen sadece kolluk faaliyetleri kapsamında kullanım alanına sahip olmayıp, kamu hizmetlerinin geliştirilmesi için de kullanılabilir. Ancak, uygulamada idare özel sektördeki kişisel verilere çoğunlukla kolluk amacıyla erişmektedir. Bu bağlamda, özel sektörün sahip olduğu kişisel veriler salgınlara karşı genel sağlığın korunması, finansal piyasaların düzenlenmesi, ulusal güvenlik ve kolluk faaliyetlerinin yerine getirilmesi gibi kamu düzeni ile örtüşen çeşitli alanlarda kullanılabilir⁴⁴³.

Wetzling, Sarkesian ve Dietrich'e göre idare, özel sektör tarafından tutulan verilere iki ana yoldan erişebilmektedir; ya özel sektörü yasal yollarla veya baskı yoluyla veri paylaşmaya zorlayabilir ya da özel sektör, veri setlerini (*data set*) satarak veya gönüllü olarak bunları idarelere sunarak, idarenin verilere erişimini sağlayabilir⁴⁴⁴. Kimi yazarlar ise, özel sektörün verileri satması durumunu göz ardı

⁴⁴² Cate, F. H./ Dempsey, J. X./ Rubinstein, I. S.: Systematic Government Access To Private-Sector Data, International Data Privacy Law 2012, C.II, S.4, s. 195.

⁴⁴³ Swire, P./ Propp K./ Christakis, T.: *Towards OECD Principles for Government Access to Data*, Lawfareblog 2021, (<https://www.lawfareblog.com/towards-oecd-principles-government-access-data>, Erişim Tarihi:15.11.2022).

⁴⁴⁴ Wetzling, T./Sarkesian,L./Dietrich,C.: *Solving the Transatlantic Data Dilemma : Surveillance Reforms to Break the International Gridlock*, 2021, s. 32.

ederek devletin özel sektördeki kişisel verilere erişim yollarını mecburi paylaşım ve doğrudan erişim olarak ikiye ayırmaktadır⁴⁴⁵. Bu çalışmada idarenin özel sektördeki verilere erişim yolları özel sektörün istem dışı olarak verileri paylaşması ve özel sektörün gönüllü olarak verileri paylaşması olarak iki ana başlıkta incelenecektir.

B. Özel Sektörün Kişisel Verileri İstem Dışı Paylaşması

1. Mecburi Paylaşım

Mecburi paylaşım kanuni bir zorunluluk olarak karşımıza çıkmaktadır. Kanunlarda öngörülen bazı durumlarda özel sektörün ellerindeki veriyi kamu otoriteleri ile paylaşma zorunluluğu bulunmaktadır. Bu tip veri erişimlerinin meşruiyeti GDPR’da işleme faaliyetinin hukuka uygunluğu başlıklı m. 6’dan kaynaklanmaktadır. Benzer düzenlemeler ulusal veri koruma kanunlarında da yer almaktadır. Ülkemizde KVKK m. 5 uyarınca kişisel veriler kanunlarda açıkça öngörülmesi veya veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması durumlarında, ilgili kişinin açık rızası olmaksızın işlenebilmektedir. Her ne kadar kişisel verilerin aktarılması KVKK m. 8’de ayrıca düzenlenmiş olsa da⁴⁴⁶

(<https://www.newamerica.org/oti/reports/solving-the-transatlantic-data-dilemma/> , Erişim Tarihi: 15.11.2022).

⁴⁴⁵ Swire/Propp/Christakis, (<https://www.lawfareblog.com/towards-oecd-principles-government-access-data>, Erişim Tarihi: 15.11.2022).

⁴⁴⁶ KVKK m. 8: “(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

(2) Kişisel veriler;

a) 5 inci maddenin ikinci fıkrasında,

b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında,

kişisel verilerin işlenmesi terimi verinin aktarılmasını da içerdiğinden ilgili düzenleme malumun ilanından öteye geçememektedir⁴⁴⁷. Ayrıca, bu genel düzenlemelerin yanında, mecburi paylaşım farklı özel kanunlarda da karşımıza çıkmaktadır. Özellikle elektronik iletişim sektörüyle ilgili mevzuatta bu durum gözlenmektedir. Zira, ulusal güvenliğin korunması ve suçla mücadele için elektronik iletişim sektöründeki kişisel verilerin saklanması ve bunlara erişim, ulusal güvenlik kurumları arasında yaygın bir kullanıma sahiptir⁴⁴⁸.

Mecburi paylaşım kapsamında idarenin kişisel verilere ulaşmasına örnek olarak, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'da düzenlenen; her türlü gerçek ve tüzel kişi ile tüzel kişiliği bulunmayan kuruluşların Malî Suçları Araştırma Kurulu'nca (MASAK) talep edilen her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları paylaşma yükümlülüğü gösterilebilir⁴⁴⁹.

belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

(3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

⁴⁴⁷ Çekin, s. 121.

⁴⁴⁸ Espinoza, J./Brunsden, J./Venkataramakrishnan, S.: *EU's Top Court Blocks States From Gathering User Data for Surveillance*, Financial Times 2020, (<https://www.ft.com/content/71cc07fb-58ff-404d-868c-5dd0e8a97e20>), Erişim Tarihi: 15.11.2022).

⁴⁴⁹ 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun m. 7: "(1) Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar; Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla yükümlüdür.

(2) Yukarıdaki fıkraya göre talepte bulunulanlar savunma hakkına ilişkin hükümler saklı kalmak kaydıyla, özel kanunlarda yazılı hükümleri ileri sürerek bilgi ve belge vermekten kaçınamazlar."

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik m. 31: "(1) Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar; Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlar da dâhil olmak üzere her türlü ortamdaki kayıtlarını, bu kayıtlara erişimi sağlamak veya okunabilir hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak, istenilen usul, şekil ve sürede gecikmeksizin vermek ve gerekli kolaylığı sağlamak zorundadır.

(2) Kendisinden talepte bulunulanlar, savunma hakkına ilişkin hükümler saklı kalmak kaydıyla, özel kanunlarda yazılı hükümleri ileri sürerek bilgi ve belge vermekten kaçınamazlar.

(3) Yükümlüler yerinde yapılacak denetimler kapsamında defter ve belgeleri denetime hazır bulundurmak; tüm bilgi işlem sistemini, denetimin amaçlarına uygun olarak denetim elemanlarına açmak ve verilerin güvenliğini sağlamak zorundadır.

Benzer bir düzenleme 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı (MİT) Kanunu'nda da bulunmaktadır⁴⁵⁰. Türkiye ve başka ülkelerden mecburi paylaşım ile ilgili farklı örnekler de vermek mümkündür⁴⁵¹. MASAK ve MİT ile ilgili düzenlemelerin ülkemiz açısından önemi, bu kuruluşların veri işleme faaliyetlerinin KVKK m. 28 uyarınca tam istisna hallerinden sayılmasıdır⁴⁵².

Her ne kadar mevzuatta ilgili kurumların her türlü belge ve bilgiyi özel sektörden alabileceği düzenlense ve bu kurumların faaliyetleri KVKK kapsamı dışında bırakılsa da bu durum MASAK ve MİT'in hiçbir sınır olmaksızın özel sektördeki kişisel verilere ulaşabileceği anlamına gelmemektedir⁴⁵³. Avrupa içtihat hukuku uyarınca mecburi paylaşımın birtakım sınırları bulunmaktadır. ABAD'ın içtihatlarına baktığımızda mecburi paylaşımın yalnızca "kesinlikle gerekli olanın" (*strictly necessary*) sınırı aşılmadığı takdirde mümkün olduğunu görmekteyiz.

(4) Bilgi ve belgeler acil haller dışında yazılı olarak istenir. Yazıyla istenilen bilgi ve belgeler için yedi günden az olmamak üzere uygun bir süre verilir. Sözlü olarak bilgi ve belge talep edilmesi halinde bu talep yazı ile teyit edilir."

⁴⁵⁰ 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu m. 6:

"(1) Millî İstihbarat Teşkilatı bu Kanun kapsamındaki görevlerini yerine getirirken aşağıdaki yetkileri kullanır:

...

b) Kamu kurum ve kuruluşları, kamu kurumu niteliğindeki meslek kuruluşları, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanunu kapsamındaki kurum ve kuruluşlar ile diğer tüzel kişiler ve tüzel kişiliği bulunmayan kuruluşlardan bilgi, belge, veri ve kayıtları alabilir, bunlara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim alt yapısından yararlanabilir ve bunlarla irtibat kurabilir. Bu kapsamda talepte bulunulanlar, kendi mevzuatlarındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar."

⁴⁵¹ Örneğin Amerika Birleşik Devletleri Kanunu'nun 18. başlığının 1. kısmının 2258A maddesi uyarınca elektronik haberleşme servis sağlayıcıları çocuk istismarı durumunda istismara karışan kişinin verileri de dahil olmak üzere birtakım bilgileri Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi'ne bildirmekle yükümlüdür. Bkz. (<https://www.law.cornell.edu/uscode/text/18/2258A>, Erişim Tarihi: 02.04.2023).

⁴⁵² Buna paralel olarak Türkiye 108 sayılı sözleşme hükümlerinin devlet kurumlarınca milli güvenlik, savunma ile soruşturma ve suç önleme amacıyla işlenen kişisel verilere uygulanmayacağını beyan etmiştir.

⁴⁵³ Bkz. s. 41-42

ABAD 2006/24 sayılı Veri Saklama Direktifi'ni⁴⁵⁴ iptal ettiđi *Digital Rights Ireland* ve Diđerleri kararında, ilgili direktifte düzenlenen, verilerin yetkili ulusal makamlara olası aktarımları amacıyla saklanması faaliyetinin ciddi suçlara karşı mücadele ve asayişin sağlanması gibi kamu düzenini sağlamaya yönelik amaçları gerçekleştirmeye olanak sağladığını kabul etmiştir. Bunun yanında Direktif ile zorunlu kılınan veri saklama ve paylaşma faaliyetinin, özel hayata saygı ve kişisel verilerin korunması haklarının özünü olumsuz etkileyecek nitelikte olmadığını belirtmiştir. Ancak, Direktif idarenin özel sektörün elindeki kişisel verilere erişimini kesinlikle gerekli olan ile sınırlandırmakta başarısız olmuştur çünkü;

1) Direktif, elektronik iletişim hizmetlerini kullanan herkesi kapsayacak şekilde kaleme alınmıştır. Bu nedenle, davranışlarının ciddi bir suçla dolaylı veya uzak olsa bile bir bağlantısı olabileceğine dair hiçbir kanıt bulunmayan kişilerin verileri bile Direktif kapsamında işlenebilecektir. Ayrıca Direktif, saklanması öngörülen veriler ile kamu güvenliğine yönelik tehdit arasında herhangi bir ilişki kurulmasını gerektirmemektedir.

2) Direktif özel hayatın gizliliđi ve kişisel verilerin korunması haklarına müdahaleyi haklı kılacak kadar ciddi olduđu düşünölebilecek suçların önlenmesi, tespiti veya cezai kovuşturulması amacıyla yetkili ulusal makamların verilere erişiminin ve bunların müteakip kullanımının sınırlarını belirleyecek herhangi bir objektif kriter ortaya koymamıştır. Bunun yanı sıra, Direktifin kamu otoritelerinin tutulan verilere erişimini düzenleyen m.4 hükmünde, erişim ve müteakip kullanımın ciddi suçların önlenmesi

⁴⁵⁴ Veri Saklama Direktifi'nin temel amacı, halka açık elektronik iletişim hizmetleri veya kamu iletişim ađları sağlayıcıları tarafından üretilen veya işlenen belirli verilerin saklanmasına ilişkin Üye Devletlerin hükümlerini uyumlu hale getirmektir.

ve kovuşturmanın yürütülmesi ile sınırlı olması gerektiğini de açık bir şekilde belirtmemektedir.

3) Kamu otoritelerinin verilere erişimi ve bunları kullanması, mahkeme veya bağımsız idari organın ön incelemesine tabi tutulmamıştır. Nitekim bu tür bir ön incelemenin amacı verilere erişimin kesinlikle gerekli olan ile sınırlı olmasını sağlamaktır. Bu sebeplerle ABAD ilgili direktifi iptal etmiştir⁴⁵⁵.

Daha yakın tarihli kararlara baktığımızda da ABAD'ın bu içtihadını sürdürdüğü görülmektedir. Örneğin, *Privacy International* kararında ABAD, önceki içtihatlarıyla uyumlu önemli çıkarımlar yapmıştır. Dava konusu olayda Birleşik Krallık istihbarat servisinin iletişim verilerini servis sağlayıcılarından toplu bir şekilde almasına olanak sağlayan ulusal mevzuatın Avrupa Birliği Temel Haklar Şartı ile uyumlu olup olmadığı incelenmiştir. Kararda açıklandığı üzere, izlenen amaçla en azından dolaylı bir bağlantısı olup olmadığına bakılmaksızın, tutulan tüm verilere genel erişim izninin “kesinlikle gerekli olanla” sınırlı olduğu kabul edilmemektedir. Ayrıca, bir makamın kişisel verilere erişimiyle ilgili olarak, mevzuat, makamların verilere erişiminin söz konusu mevzuatın izlediği amaçla tutarlı olmasını şart koşmakla yetinemez, aynı zamanda erişimi ve müteakip kullanımı düzenleyen maddi ve usuli koşulları da belirlemelidir⁴⁵⁶.

⁴⁵⁵ Kararda bunlar dışında başka gerekçelerde belirtilmektedir ancak çalışmanın konusu bakımından diğer gerekçeler bu çalışmada değerlendirilmemiştir; Bkz. ABAD, C-293/12, 08.04.2014: *Digital Rights Ireland Ltd and Others v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0293>, Erişim Tarihi: 20.03.2023).

⁴⁵⁶ Bkz. ABAD, C-623/17, 06.10.2020: *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0623>, Erişim Tarihi: 20.03.2023).

Bu konudaki önemli bir diğer karar ise Avrupa İnsan Hakları Mahkemesi'nin (AİHM) verdiği *Big Brother Watch* v. Birleşik Krallık kararıdır. Başvuru, ABD Ulusal Güvenlik Ajansı Merkezi İstihbarat Teşkilatı (CIA) ve Ulusal Güvenlik Dairesi (NSA) eski çalışanı *Edward Snowden*'in ABD ve Birleşik Krallık arasındaki gözetleme ve istihbarat paylaşım programlarını ifşa etmesinin ardından yapılmış ve davada 3 farklı gözetleme biçimi ele alınmıştır: (1) iletişimin toplu olarak dinlenmesi, (2) yabancı hükümetlerden ve istihbarat kurumlarından iletişimin dinlenmesiyle ilgili materyallerinin alınması, (3) iletişim hizmeti sağlayıcılarından iletişim verilerinin elde edilmesi. AİHM birinci ve üçüncü gözetleme biçimlerinin Avrupa İnsan Hakları Sözleşmesi (AİHS) m. 8'de düzenlenen özel hayata saygı hakkını ihlal ettiğine, ikinci gözetleme biçiminin ise bu hakkı ihlal etmediğine karar vermiştir. Ayrıca AİHM, AİHS m. 10'da düzenlenen ifade özgürlüğü bakımından yaptığı değerlendirmede, birinci gözetim biçimi için ihlal kararı verirken üçüncü gözetim biçiminin bir ihlal oluşturmadığına hükmetmiştir.

AİHM gerekçesinde, devletlerin modern toplumda karşılaştıkları tehditlerin çokluğu nedeniyle, toplu dinleme rejimlerinin kendi başına AİHS'yi ihlal etmediğini, hükümetlerin, ulusal güvenliği korumak için ne tür bir gözetleme türünün gerekli olduğuna karar verirken geniş bir takdir marjına sahip olduğunu belirtmiş, ancak bu tarz bir rejimin “uçtan uca güvencelere” tabi olması gerektiğini değerlendirmiştir. Bunun anlamı: ulusal düzeyde, alınan tedbirlerin gerekliliği ve orantılılığı konusunda sürecin her aşamasında bir değerlendirme yapılması gerekmesi; toplu dinleme operasyonunun amacı ve kapsamı tanımlanırken, bağımsız bir otoritenin iznine tabi olması gerekmesi; operasyonun denetime ve bağımsız *ex post facto* incelemeye tabi olmasının gerekmesidir. Birleşik Krallık'ta uygulanan toplu dinleme rejimini göz

önünde bulunduran AİHM, şu eksiklikleri tespit etmiştir: Toplu dinleme yetkisi, yürütmeden bağımsız bir organ tarafından değil, Dışişleri Bakanı tarafından verilmiştir; incelemeye tabi tutulacak iletişim türlerini tanımlayan arama terimleri kategorileri, arama izni başvurusuna dahil edilmemiştir; bir kişiyle bağlantılı arama terimleri (yani e-posta adresi gibi belirli tanımlayıcılar) önceden kurum içi yetkilendirmeye tabi tutulmamıştır. Ayrıca AİHM kararında, yetkililerin iletişim servis sağlayıcıları tarafından tutulan verilere erişmesine izin veren herhangi bir düzenlemenin, erişimi “ciddi suçlarla” mücadele amacıyla sınırlandırması gerektiği ve erişimin bir mahkeme veya bağımsız idari organ tarafından gerçekleştirilen bir ön incelemeye tabi olmasını gerektirdiğini belirtmiştir⁴⁵⁷.

Ülkemizde ise AYM’nin 2014 tarihli bir kararında, internet trafik bilgilerinin Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmelerden alınıp, hâkim tarafından karar verilmesi hâlinde bu verilerin ilgili mercilere verilmesini düzenleyen yasa hükmünü iptal ettiği kararındaki gerekçelerden bazıları şöyledir:

“(…) Kuralda, temin edilecek bilgiyle ilgili olarak herhangi bir konu ve amaç sınırlaması bulunmadığı gibi bilginin kapsamı, ne şekilde kullanılacağı, tutulacağı süre, temin edilme gerekçesi gibi hususlarla ilgili olarak da herhangi bir belirlilik bulunmamaktadır.

(…) verilerin işlenebileceği hâllerin kanunda açıkça yer alması zorunluluğu bulunmasına karşın, kuralda herhangi bir belirleme ve sınırlama yapılmaksızın doğrudan kişisel veri niteliğindeki trafik bilgisinin temin edilmesine ve

⁴⁵⁷ AİHM, *Big Brother Watch and Others v. Birleşik Krallık* [GC], nos. 58170/13 and 2 others, 25.05.2021.

işlenmesine olanak sağlanmasının bu yönüyle Anayasa'nın 20. maddesine aykırı olduğu açıktır.

(...) bu bilgilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olması temel hak ve özgürlüklerin doğrudan ihlaline sebebiyet vermektedir.

Anayasa'nın 13. ve 20. maddelerinde yer alan güvencelere rağmen dava konusu kural ile kişiler, bilgi toplama, saklama, işleme ve değiştirme yetkisi olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın amaç, gerekçe, kapsam ve sınırlarına yasal düzenlemede yer verilmemiştir⁴⁵⁸. ”

Benzer şekilde AYM, MİT'in özel sektördeki verilere erişmesine olanak sağlayan 2937 sayılı Kanun'un 6/1-b bendinin iptal istemini reddederken ilgili kanunda açıkça düzenlendiği üzere, elde edilen bilgilerin kanundaki amaçlar dışında kullanılamayacağı gibi bu verilerin amacı dışında kullanılmasını önleyecek yasal güvencelere de kanunda yer verildiğine hükmetmiştir. Çünkü kanun verilerin ele geçirilme amacına uygun kullanılmasını denetlemek için sıralı kurum amirleri ve Devlet Denetleme Kurulu'nu yetkilendirmiştir. Fakat karara karşı oy yazan üyeler, kanunda, verilerin işlenmesine ilişkin yeterli düzenleme bulunmadığı için bir belirsizlik olduğu, “MİT'e bu şekilde milli güvenlik amacıyla geniş bir yetki verilecekse, yapılan görevle doğrudan bağlantılı, talebin amacıyla sınırlı ve zorunlu hallerde bu yetkinin kullanılabilmesinin de öngörülmesi, bu sınırların korunmasını sağlayacak ve amaç dışı kullanımına engel olacak tedbirlerin alınması gerektiğini” belirtmiştir⁴⁵⁹. Kanımızca ilgili kanunda veya

⁴⁵⁸ AYM, T. 02.10.2014, E.2014/149, K.2014/151, RG. 01.01.2015, S. 2922.

⁴⁵⁹ AYM, T. 30.12.2015, E.2014/122, K.2015/123, RG. 01.03.2016, S. 29640.

ikincil mevzuatta kişisel verilerin istenme usulü ve saklama süresi hakkında bir düzenleme bulunmaması bir eksikliktir.

Yukarıda verilen içtihat hukuku çerçevesinde 5549 sayılı Kanun'da MASAK'a özel sektördeki her türlü bilgi ve belgeye erişme imkânı veren m.7 hükmünü değerlendirecek olursak, kanımızca ilgili maddenin hukuka aykırı olduğunun belirtilmesi gerekir. İlgili kanunda MASAK'ın hangi amaçla verilere erişeceği açıkça düzenlenmediği gibi verilerin toplanması ve bunların kullanılmasının "kesinlikle gerekli olan" ile sınırlanmasını sağlayacak herhangi bir düzenleme de bulunmamaktadır. AYM güvenlik soruşturmaları ile ilgili düzenlemeleri iptal ettiği yakın tarihli kararlarında da şu gerekçelere dayanmaktadır:

“Kuralda güvenlik soruşturması ve arşiv araştırması yapmakla görevli olanların bu kapsamda kişisel veri niteliğindeki bilgilere ulaşması öngörülmüşken Kanun'da bu bilgilerin ne şekilde kullanılacağına, hangi mercilerin soruşturma ve araştırmayı yapacağına, bu bilgilerin ne suretle ve ne kadar süre ile saklanacağına, ilgililerin söz konusu bilgilere itiraz etme imkânının olup olmadığına, bilgilerin bir müddet sonra silinip silinmeyeceğine, silinecekse bu sırada izlenecek usulün ne olduğuna, yetkinin kötüye kullanımını önlemeye yönelik nasıl bir denetim yapılacağına ilişkin herhangi bir düzenleme yapılmamıştır. Diğer bir ifadeyle güvenlik soruşturması ve arşiv araştırmasının yapılmasına ve elde edilecek verilerin kullanılmasına ilişkin keyfiliğe izin vermeyecek şekilde belirli ve öngörülebilir kanuni güvenceler belirlenmeksizin, kuralla güvenlik soruşturması ve arşiv araştırması yapmakla görevli olanların bu soruşturma ve araştırma

kapsamında kişisel veri niteliğindeki bilgileri almakla yetkili oldukları belirtilmiştir.

“Güvenlik soruşturması ve arşiv araştırması sonucunda kişisel veri niteliğindeki bilgilerin alınmasına, kullanılmasına, işlenmesine yönelik güvenceler ve temel ilkeler kanunla belirlenmeksizin bunların alınmasına ve kullanılmasına izin verilmesi Anayasa’nın 13. ve 20. maddeleriyle bağdaşmamaktadır”⁴⁶⁰.

2. Doğrudan Erişim

Doğrudan erişim⁴⁶¹, devletin özel sektörün elinde bulunan verileri kuruluşun bir çalışanın veya temsilcisinin aracılığı veya etkileşimi olmaksızın doğrudan elde etmek için bizzat çaba sarf ettiği durumları ifade etmektedir. Hatta çoğu durumda özel sektördeki aktörlerin, devletlerin verilerine erişmeye çalıştığından bile haberi olmamaktadır. Bu duruma örnek olarak sinyal istihbaratı ve dinlemeler, gizli casusluk operasyonları veya bilgisayar korsanlığı aktiviteleri gösterilebilir⁴⁶². Bu bağlamda, doğrudan erişim şu noktalarda mecburi paylaşımdan ayrılmaktadır: İlk olarak, doğrudan erişim standartlaştırılmış yasal erişim yöntemlerinin ötesinde çok çeşitli araçlar kullanılarak gerçekleştirilme eğilimindedir. İkincisi, çoğu durumda doğrudan

⁴⁶⁰ AYM, T. 19.2.2020, E. 2018/163-K. 2020/13, RG. 28.04.2020, S. 31112; Benzer nitelikteki kararlar için bkz. AYM, T. 24.07.2019, E.2018/73, K.2019/65, RG.29.11.2019, S. 30963; AYM, T. 19.02.2020, E.2018/91, K. 2020/10, RG; T. 30/4/2020, S. 31114.

⁴⁶¹ Bu noktada doğrudan erişim ve “sistematik devlet erişimi” terimleri arasındaki ayrımın yapılması gerekir. Bazı akademik çalışmalarda görülen “sistematik devlet erişimi” terimi doğrudan erişimden daha geniş bir kavramdır. Buna göre sistematik devlet erişimi şu iki erişim türünü kapsamaktadır; i) her türlü doğrudan erişim ii) doğrudan veya özel şirketin aracılığıyla olması fark etmeksizin büyük hacimli verilere erişim. Bkz. Rubinstein, I. S./Nojeim, G. T./Lee, R. D.: *Systematic Government Access to Personal Data: A Comparative Analysis*, International Data Privacy Law 2014, C. IV, S.2, s. 96.

⁴⁶² Swire/Propp/Christakis, (<https://www.lawfareblog.com/towards-oecd-principles-government-access-data> Erişim Tarihi: 15.04.2023).

erişim kamuya açık şekilde düzenlenmez ve raporlanmaz. Bunun ötesinde, yasalarda düzenlendikleri durumlarda bile, nasıl ve ne zaman uygulandıklarına ilişkin ayrıntılar genellikle gizlidir⁴⁶³. Doğrudan erişime örnek olarak Hindistan'ın 2013 yılında hayata geçirdiği Merkezi İzleme Sistemi (CMS) gösterilebilir. CMS'den önce kolluk , şüpheli teröristler veya suçluların iletişimini dinlemek için telekomünikasyon servis sağlayıcılarına başvurmak zorundaydı ancak CMS ile hükümet, araçları devre dışı bırakarak e-posta, sohbet, sesli arama ve mesajlaşmalara doğrudan gerçek zamanlı erişim imkânı kazanmıştır⁴⁶⁴.

OECD bünyesindeki İşveren ve Sanayi Danışma Komitesi'nin (BIAC) belirttiği üzere, doğrudan devlet erişiminin ekonomik etkisi, mecburi paylaşım kıyasla daha az anlaşılmış durumdadır. Yine de doğrudan erişim uygulamalarının kamu standartlarına veya hesap verebilirliğe bağlı olmayabileceği algısı, sınır ötesi veri akışlarına güven eksikliğinin artmasına sebep olabilir. Bu sebeple, iş dünyası uzun süredir doğrudan erişim ile ilgili, insan haklarını koruyacak ve siber suçlar konusunda uluslararası iş birliği sağlayacak şekilde açık normlar belirlenmesini istemektedir⁴⁶⁵.

Yukarıda belirtildiği gibi doğrudan erişim genellikle kamuya duyurulmadan gerçekleştirildiği için bu konuda çok fazla örnek, dolayısıyla yargı kararı da

⁴⁶³ Global Network Initiative: *Defining Direct Access: GNI calls for greater transparency and dialogue around mandatory, unmediated government access to data*, 2021, (https://globalnetworkinitiative.org/defining-direct-access-2/#_ftn2, Erişim Tarihi 15.01.2023).

⁴⁶⁴ Internet Freedom Foundation: *Watch the Watchmen Series Part 2 : The Centralised Monitoring System*, 2020, (<https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/>, Erişim Tarihi 15.01.2023).

⁴⁶⁵ BIAC: *The OECD Process to Develop Common Principles for Trusted Government Access to Data: BIAC Supports Continuation and Successful Completion of the Process with Timely Outcomes: Draft 2.0 for Discussion Only*, 2021, (<https://25159535.fs1.hubspotusercontent-eu1.net/hubfs/25159535/website/documents/pdf/Digital%20Economy/The%20OECD%20Process%20to%20Develop%20Common%20Principles%20for%20Trusted%20Government%20Access%20to%20Data%20BIAC%20Supports%20Continuation%20and%20Successful%20Completion%20of%20the%20Process%20with%20Timely%20Outcomes.pdf>, Erişim Tarihi: 15.01.2023).

bulunmamaktadır. Ancak doğrudan erişimle ilgili önemli bir olay 2009 yılında AİHM'nin önüne gelmiştir. *Roman Zakharov v. Rusya* davasında başvuru *Zakharov* Rusya'nın kullandığı Operasyonel Soruşturma Faaliyetleri Sistemi'nin (SORM)⁴⁶⁶ önceden bir mahkeme izni alınmaksızın, güvenlik kurumları tarafından, tüm telefon iletişiminin sınırsız bir şekilde dinlenmesine olanak sağladığını ve bu durumun Sözleşme'de düzenlenen özel hayata saygı hakkını ihlal ettiğini ileri sürmüştür. Ayrıca, 13. maddeye (etkili başvuru hakkı) dayanarak, söz konusu mevzuata itiraz etmek için ulusal düzeyde etkili bir hukuk yolu bulunmadığından şikayetçi olmuştur. AİHM 4 Aralık 2015 tarihli kararıyla özel hayata saygı hakkının ihlal edildiğine karar vermiştir.

AİHM, iletişimin dinlenmesinin ulusal güvenliğin ve kamu güvenliğinin korunması, suçun önlenmesi ve ülkenin ekonomik refahının korunması gibi meşru amaçlar taşıdığını kabul etmekle beraber, gizli bir kitlesel izleme sisteminin, demokrasiyi savunma kisvesi altında onu zayıflatmak ve hatta yok etmek için kullanılabileceği riski göz önüne alındığında, kötüye kullanıma karşı yeterli ve etkili güvenceler sağlandığı konusunda AİHM'nin tatmin olması gerektiğini belirtmiştir. Bu bağlamda inceleme yapan AİHM, iletişimin dinlenmesini düzenleyen Rus mevzuatının keyfilik ve suistimal gibi kötüye kullanma durumlarına karşı yeterli güvenceleri sağlamadığına hükmetmiştir. Özellikle de şu konularda yasal çerçevede eksiklikler tespit edilmiştir: Rusya'daki kamu makamlarının hangi durumlarda gizli izleme tedbirlerine başvurma yetkisine sahip olduğu; bu tür tedbirlerin süresi ve özellikle hangi durumlarda sona erdirilmesi gerektiği; iletişimin dinlenmesine izin verme ve dinlenen verilerin saklanması ile imha edilmesine ilişkin usuller; iletişimin

⁴⁶⁶ Rusya'da faaliyet gösteren telefon ve internet şirketleri yasalar gereği hükümete erişim imkânı sağlayan cihazları ağlarına kurmak zorundadır.

dinlenmesinin denetlenmesi. Ayrıca, iletişimin dinlenmesine itiraz etmek için mevcut olan hukuk yollarının sadece dinleme yapıldığına dair kanıt sunabilen kişilere açık olması ve herhangi bir bildirim sisteminin olmaması yanında dinleme ile ilgili bilgilere erişim imkanının bulunmaması nedeniyle bu tür bir kanıtın elde edilmesinin imkânsız olması nedeniyle etkili çözüm yolları da bulunmamaktadır.

AİHM, Rusya'daki gibi, gizli servislerin ve polisin, iletişim hizmeti sağlayıcısına veya başka herhangi bir kişiye dinleme izni sunmasına gerek kalmadan, her bir vatandaşın iletişimini doğrudan dinlemesine olanak tanıyan bir sistemin, özellikle suistimale açık olduğunu bu nedenle doğrudan erişim sağlayan böyle bir sistemde keyfiliğe ve suistimale karşı güvencelere duyulan ihtiyacın özellikle fazla olduğunu belirtmiştir⁴⁶⁷.

C. Özel Sektörün Kişisel Verileri Gönüllü Paylaşması

1. Genel Olarak Gönüllü Paylaşım

İdare özel sektördeki verilere erişmek için her zaman zorlayıcı yöntemler kullanmamakta bazı durumlarda özel sektör gönüllü olarak elindeki verileri idare ile paylaşmaktadır. Bu tür paylaşımlar genellikle vatanseverlik, devlet kurumlarıyla iyi ilişkiler kurma arzusu, ulusal yasaların bu tür taleplere uymayı gerektirmediğinin anlaşılmaması, iş birliği yapmazlarsa misillemeye uğrama korkusu ve sahip oldukları

⁴⁶⁷ AİHM, *Roman Zakharov v. Rusya* [GC], no. 47143/06, 2015.

verileri devlete satarak gelir elde etme arzusu neticesinde ortaya çıkmaktadır. Verilerin toplu bir şekilde idare ile paylaşılmasındaki motive edici bir faktör ise verimliliktir çünkü toplu paylaşım idareden gelecek çok sayıda bireysel erişim talebinin sebep olacağı yükü azaltacaktır⁴⁶⁸.

Örneğin, *Facebook* ve *RIM/BlackBerry*, kamuya açık bir telekomünikasyon sistemi sağlamaları sebebiyle Birleşik Krallık'ın Soruşturma Yetkilerinin Düzenlenmesi Kanunu'na (RIPA) tabi olmasalar da kamu makamlarının RIPA prosedürleri kapsamında gerçekleştirdiği belirli abone verilerine yönelik taleplerine uymaktadırlar⁴⁶⁹.

Bu uygulama çoğunlukla özel sektördeki verilerin satın alınması şeklinde karşımıza çıkmaktadır. Ancak her ne kadar satın alma haricindeki verileri gönüllü paylaşma uygulamaları en azından kamu tarafından yeterince bilinmese de herhangi bir parasal anlaşma olmaksızın gönüllü paylaşım yapılabileceği olasılığı da göz önünde bulundurulmalıdır. Ayrıca belirtilmesi gerekir ki bu tip uygulamalar çoğunlukla halka duyurulmadan gerçekleştirilmektedir ve basın sızıntıları yoluyla ortaya çıkmaktadır.

⁴⁶⁸ Rubinstein/ Nojeim/ Lee, s. 105; Schneier, B.: *Do You Want the Government Buying Your Data From Corporations?*, 2013, (<https://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/>, Erişim Tarihi: 15.01.2023).

⁴⁶⁹ Brown, I.: *Government Access to Private-Sector Data in the United Kingdom*, International Data Privacy Law 2012, C. II, S.4, s. 237.

2. Gönüllü Paylaşım Yolu Olarak Satış

Hükümetlerin verileri satın almasına yönelik uygulamalar genellikle ABD’de karşımıza çıkmaktadır ya da en azından ABD kapsamında satın alma uygulamaları hakkındaki bilgiler basına yansımaktadır. Verilerin özel sektörden satın alınması faaliyetinin ABD’de giderek yaygınlaşmasının nedeni ise Amerikalıların bilgilerini toplayan, paketleyen ve satmaya istekli olan kuruluşların çoğalmasındır. Bu kuruluşların varlığıyla beraber, hükümetin artık telekomünikasyon servis sağlayıcılarından konum verilerinin üretilmesini talep etmesine gerek kalmamıştır. Zira, coğrafi konum verileri gibi birçok kişisel veriyi toplayan sayısız cep telefonu uygulaması mevcuttur. Şirketler topladıkları bu verileri veri simsarlarına, onlar da devlet kurumlarına satmaktadır⁴⁷⁰.

Kamu otoritelerinin mecburi paylaşım yöntemini kullanmak yerine bu verileri satın almasının ardında yatan sebep ise bu yöntem ile kişisel verilerin korunması hakkındaki güvencelerin çevresinden dolanabilmeleridir. ABD kolluk kuvvetleri ve istihbarat yetkilileri, mahkeme emri olmaksızın veri simsarlarıyla sözleşme yaparak, önemli ölçüde daha az kamu şeffaflığı ve adli gözetim ile verileri işleyebilmektedir⁴⁷¹.

Kişisel verilerin Amerikan kamu otoriteleri tarafından satın alınmasıyla ilgili yakın tarihli çok sayıda örnek bulmak mümkündür. Örneğin ABD Göçmenlik ve Gümrük Muhafaza (ICE) 2020 yılında milyonlarca kişinin kişisel verilerini içeren *LexisNexis Risk Solutions* veri tabanına erişimi satın alarak çok büyük miktarda veriye

⁴⁷⁰ Goitein, E.: *The Government Can't Seize Your Digital Data, Except by Buying It*, Washington Post 2021, (<https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/>, Erişim Tarihi: 15.01.2023).

⁴⁷¹ Chin, C.: *Digital Dragnets: Examining the Government's Access to Your Personal*, 2022, s.2 <https://www.csis.org/analysis/digital-dragnets-examining-governments-access-your-personal-data>, Erişim Tarihi: 15.01.2023).

erişim sağlamış ve sadece 2021’in ilk 7 ayında 1.2 milyon kez bu veri tabanında arama yapmıştır⁴⁷². ICE ve ABD Gümrük ve Sınır Koruma Biriminin göçmen hareketlerini izlemek için veri simsarlarından büyük miktarda konum verisi aldığı da bilinen bir durumdur⁴⁷³. Bu konudaki başka bir çarpıcı örnek de ABD ordusunun popüler Namaz uygulaması ve müslüman flört uygulamaları aracılığıyla elde edilen hassas verileri satın almasıdır⁴⁷⁴.

Satın alma uygulamalarının artması ve bunların basına çok fazla yansımaları üzerine, son yıllarda ABD’de bu konu hakkındaki çalışmalar da artmaya başlamış ve Yüksek Mahkeme’nin 22 Haziran 2018 tarihli *Carpenter* v. Amerika Birleşik Devletleri kararıyla kolluk kuvvetlerinin özel sektördeki konum verilerine erişimi konusunda önemli gelişmeler yaşanmıştır. Bu karardan önce Yüksek Mahkeme telekomünikasyon servis sağlayıcılarındaki kişisel verilerle ilgili *Smith v. Maryland* davasında belirlediği “üçüncü taraf doktrini” uygulamaktaydı. Bu doktrine göre telefon şirketleri gibi üçüncü taraflara gönüllü olarak verilen bilgilerle ilgili olarak bir kişinin makul bir mahremiyet beklentisi bulunmamakta ve bu nedenle hükümet yetkililerinin bu bilgilere erişmek için bir arama izni almalarına gerek bulunmamaktadır. Ancak *Carpenter* kararıyla Yüksek Mahkeme, kamu otoritelerinin, cep telefonlarının fiziksel konumlarını içeren geçmiş baz istasyonu konum kayıtlarına mahkemeden alınan bir arama emri olmaksızın erişmesinin, Birleşik Devletler

⁴⁷² Biddle, S.: *ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months*, The Intercept 2022, (<https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/>), Erişim Tarihi: 15.01.2023).

⁴⁷³ Tau, B./ Hackman, M.: *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WSJ 2020, (<https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>), Erişim Tarihi: 15.01.2023).

⁴⁷⁴ Cox, J.: *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE 2020, (<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>), Erişim Tarihi: 15.01.2023).

Anayasasının Dördüncü Değişikliğini ihlal ettiğine karar vermiştir. Bunun nedeni baz istasyonu konum verileri sayesinde kişiler hakkında çok geniş kapsamlı bilgiler elde edilebilmesi ve kişi üzerinde neredeyse mükemmel bir gözetim gerçekleştirilmesidir⁴⁷⁵.

Ancak, her ne kadar *Carpenter* davası önemli bir gelişme olsa da kısıtlı bir dille kaleme alındığından kişisel verilerle ilgili sorunlara tam bir çözüm getirememiştir. Kamu otoriteleri *Carpenter* kararının sadece belirli bir tip konum verisine erişim için geçerli olduğunu ve bunun ötesinde kararın, baz istasyonu konum verilerinin bir veri simsarından alınması için mahkeme kararı gerektiği şeklinde yorumlanamayacağını savunmaktadır⁴⁷⁶.

ABD’de veri satışının engellenmesine yönelik bir başka önemli gelişme ise “Dördüncü Değişiklik Satılık Değildir Yasası’nın (*The Fourth Amendment is Not for Sale Act*)” yürürlüğe koyulmaya çalışılmasıdır. Bu yasa veri simsallarının kişisel verileri herhangi bir mahkeme denetimi olmaksızın kolluk kuvvetlerine ve istihbarat kurumlarına satmasına olanak tanıyan yasal boşlukları kapatmayı amaçlamaktadır⁴⁷⁷.

Chin, ABD Senatosu Yargı Komitesi huzurunda yaptığı açıklamada *Carpenter* kararının uygulama alanının belirsiz olduğuna değindikten sonra, Kongre’nin özel hayatın gizliliği için daha güçlü korumalar geliştirebilmesi adına bazı öneriler

⁴⁷⁵ U.S. Supreme Court, *Carpenter v. United States*, 585 U.S. (2018). <https://supreme.justia.com/cases/federal/us/585/16-402/#tab-opinion-3919270>

⁴⁷⁶ Savage, C.: *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants*, *Memo Says*. The New York Times 2021, (<https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html>, Erişim Tarihi: 15.01.2023).

⁴⁷⁷ U.S. Senator Ron Wyden of Oregon’s Press Release: *Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not for Sale Act*, 2021, (www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-#:~:text=The%20Fourth%20Amendment%20is%20Not%20for%20Sale%20Act%20closes%20the,other%20businesses%20that%20have%20direct, Erişim Tarihi: 15.01.2023).

sunmuştur. Öncelikle devletin özel şirketler tarafından tutulan verilere erişimine ilişkin kuralların netleştirilmesi gerekmektedir. Bu durum kısa vadede veri simsarları ve dijital platformlar tarafından yapılan gönüllü erişimlerin mevcut anayasal ve yasal kısıtlamalara tabi olduğunun teyit edilmesiyle sağlanabilecektir. Ancak uzun vadede, dijital veri toplamanın giderek daha sofistike hale gelmesi, geleneksel anayasal ve yasal çerçevelerin de daha kapsamlı bir şekilde yeniden incelenmesini gerektirmektedir. İkinci olarak federal kolluk kuvvetleri ve istihbarat kurumları veri toplama uygulamaları konusunda şeffaflığı artırmalıdır. Bu durumun sağlanması için kolluk kuvvetleri ve istihbarat kurumlarına özel sektör aracılığıyla izledikleri tüm bireyleri doğrudan bilgilendirmeleri yükümlülüğü getirilebilir. Son olarak ise, federal ticari gizlilik mevzuatı veri simsarlarına yönelik hükümler içermelidir. Bu bağlamda Kongre, hükümet erişimine yönelik güvenceler getirmenin yanı sıra, özel şirketler ve veri simsarları tarafından gereksiz veri toplanmasını da doğrudan engellemelidir⁴⁷⁸.

Avrupa Birliği'nde ise GDPR, AIHS, Avrupa Birliği Temel Haklar Şartı ve 108 sayılı Sözleşmedeki ilgili hükümler sayesinde, veri simsarlarının toplayabileceği ve ifşa edebileceği veriler kısıtlanmıştır. GDPR m. 5, kişisel verilerin işlenmesi ve toplanması ile ilgili genel ilkeler belirlemektedir. Bu ilkeler: hukuka uygunluk, hakkaniyet ve şeffaflık, amaçla sınırlı olma, veri minimizasyonu, doğruluk, sınırlı süre saklama, bütünlük ve gizlilik. Bunun yanında, GDPR m. 6'da işleme faaliyetinin hangi durumlarda hukuka uygun olacağı da düzenlenmiştir. Ancak, her ne kadar bu ilkeler verilerin simsarlar tarafından alınıp satılması önünde büyük bir koruma sağlasa da mutlak bir koruma oluşturmamaktadır. GDPR, veri araçlarının m. 6 kapsamında yasal bir dayanakları olması halinde kişisel verileri kolluk kuvvetleriyle

⁴⁷⁸ Chin, s. 4-7.

paylaşmalarına izin vermektedir. Örneğin, m. 6/1-d uyarınca kişisel verilerin paylaşılması bir kişinin hayatını korumak için gerekliyse, veri simsarları ellerindeki veriyi paylaşabilecektir. Bu bağlamda Avrupa Birliği vatandaşları ABD'deki vatandaşlara kıyasla çok daha fazla veri koruma hakkına sahip olsa da AB kolluk kuvvetleri, işleme için yasal bir dayanak oluşturabildikleri takdirde veri simsarlarından kişisel verileri elde edebilmektedir⁴⁷⁹.

Yakın zamanda Avrupa Birliği'nde bu konuyla ilgili yaşanan önemli bir gelişme ise Veri Yönetimi Yasası olarak adlandırılan 2022/868 sayılı Tüzüğün (DGA) kabul edilmesidir. DGA m. 10-15 “veri aracılık hizmeti” başlığı altında, veri simsarlığını bir iş modeli olarak düzenlemekte ve belirli birtakım kurallarla sınırlandırmaktadır. Örneğin, yeni düzenlemeyle beraber veri aracılık hizmeti sağlayıcılığı yapabilmek için ülkelerin belirleyeceği yetkili makama bildirim yapma yükümlülüğü getirilmiştir. Bu düzenlemenin amacı ise veri simsarlığını daha yasal bir düzleme oturtmak, birtakım kurallar belirleyerek veri aracılık hizmeti sağlayanlar üzerindeki denetimi arttırmak, şeffaflık ve tarafsızlığı sağlamak ve bu sektörde kişisel verilerin korunmasını sağlamaktır. İlgili tüzük 24 Eylül 2023 tarihinde yürürlüğe girecektir.

⁴⁷⁹ Wetzling/Sarkesian/Dietrich, s. 38-42.

C. Özel Sektördeki Kişisel Verilere Erişimin Uluslararası Ekonomiye Etkisi ve Genel İlkeler

Sınır ötesi veri akışları dünya ekonomisinin merkezide yer almaktadır; zira şirketler tarım, sağlık, imalat ve bankacılık gibi çok çeşitli sektörlerde müşterileri ve ortaklarıyla günlük işlerini yürütmek, işlerinde ve operasyonlarında yenilik yapmak ve daha etkin bir şekilde rekabet etmek için bu tür akışlara güvenmektedirler. Özel sektör tarafından tutulan kişisel verilere sınırsız ve orantısız devlet erişimi kişi haklarının korunması bağlamında çok önemli bir sorun teşkil etmesinin yanında verilerin güvenle serbest akışının sağlanmasının önünde de potansiyel bir engel oluşturmaktadır⁴⁸⁰. Bu durumun medyaya yansımış en büyük örneklerinden biri *Huawei* gibi Çin yasalarına tabi olan Çinli şirketlerin, ellerindeki verileri Pekin'in güvenlik servislerine teslim etmeye zorlanabileceklerinden şüphe edilmesi dolayısıyla Amerika Birleşik Devletleri'nde yasaklanmalarıdır⁴⁸¹. Bu bağlamda, idarenin özel sektörün elindeki verilere erişiminin olumsuz sonuçlarını ortadan kaldırabilmek adına uluslararası kuruluşlar bu konuda çalışmalar yapıp belirli birtakım standartlar oluşturmaya çabalamaktadır.

Milletlerarası Ticaret Odası'nın (ICC) belirttiği üzere, ulusal güvenlik ve yukarıda sayılan diğer nedenlerden dolayı idarenin özel sektördeki kişisel verilere

⁴⁸⁰ OECD: *Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy*, (<https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm>, Erişim Tarihi: 15.01.2023); International Chamber of Commerce: *ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector*, 2022, s. 1-2 (<https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector/>, Erişim Tarihi: 15.01.2023).

⁴⁸¹ Page, C.: *US Government Bans Huawei, ZTE and Hikvision tech over 'unacceptable' spying fears*. Techcrunch 2022, (<https://techcrunch.com/2022/11/28/fcc-huawei-zte-hikvision-hytera-dahua-ban/>, Erişim Tarihi: 15.01.2023).

eriřim isteęi anlařılabilir olsa da bu durum bir takım temel problemleri de beraberinde getirmektedir:

1) Ulusal bağlamda, devletin kamu yararı adına özel kuruluşları mecburi paylaşım zorlama yetkisine hangi amaçlarla ve ne ölçüde sahip olduęu irdelenmelidir.

2) Uluslararası düzeyde, her bir devletin erişimini düzenleyen yasalara yaklaşımındaki farklılıklar, bunların uygulanması ve koruma önlemlerindeki tutarsızlıklar, veriler sınırları aştığında önemli zorluklar ortaya çıkarmaktadır.

3) İdarelerin verilere erişim talepleri, şirketler açısından önemli sorunlar ortaya çıkarmaktadır. Şirketler, ulusal mevzuatlar tam olarak açık olmasa bile, bir talebin yasal olup olmadığına ve sınır ötesi bir talebin faaliyet gösterdikleri farklı yargı bölgeleri arasında bir hukuk çatışması yaratıp yaratmadığına karar vermek zorundadır. Düzenlemelerin eksikliği ve muğlaklığı karşısında şirketlerin ne kadar veriyi açıklamak zorunda olduklarına karar vermesi gerekmektedir. Ayrıca şirketler, bu taleplere verdikleri yanıtlarla ilgili hangi bilgileri müşterilerine ve kamuoyuna açıklayabilecekleri ikilemiyle de karşı karşıyadır⁴⁸².

Bu sorunların çözümüne ilişkin uluslararası kuruluşlar birtakım ilkeler ileri sürse de yasal olarak bağlayıcılığı bulunan uluslararası ilkeler henüz bulunmamaktadır. Bu konuda yakın zamanda yaşanan önemli bir gelişme, 14.12.2022 tarihinde OECD üye devletlerinin “Özel Sektör Kuruluşları Tarafından Tutulan Kişisel Verilere Devlet Eriřimi Deklarasyonu”nu kabul etmesidir. İlgili deklarasyon ulusal güvenlik ve kolluk faaliyetleri kapsamında kişisel verilere erişim uygulamalarında insan haklarının korunması için bazı temel ilkeler belirlemektedir. Her ne kadar

⁴⁸² ICC, s. 11.

“Deklarasyon” ,yasal olarak bağlayıcı olmasa da bu konuda ortak politikalar belirlenmesi konusunda atılan önemli bir adımdır. Deklarasyonda belirlenen yedi temel ilke genel hatlarıyla aşağıdaki gibidir⁴⁸³:

1) Yasal dayanak: İdarenin özel sektördeki kişisel verilere erişimi yasal bir çerçeve ile düzenlenir. Yasal çerçeve, bireylerin kötüye kullanım ve suistimal riskine karşı yeterli güvencelere sahip olması için idarenin erişimine ilişkin amaçları, koşulları, sınırlamaları ve güvenceleri belirler.

2) Meşru Amaç: İdarenin özel sektördeki kişisel verilere erişimi belirli ve meşru amaçları desteklemek için gerçekleştirilmelidir. Hükümetler yalnızca bu amaçlar doğrultusunda ve hukukun üstünlüğüne uygun olarak erişim talep ederler. İdarenin verilere erişimi, meşru amaçlara göre aşırı olmayan bir şekilde, gereklilik, orantılılık, ölçülülük kriterlerine uygun olarak ve kötüye kullanım ile suistimale karşı koruma sağlanmak suretiyle yerine getirilmelidir. Bunun yanında idare, muhalefeti bastırmak amacıyla kişisel verilere erişim talep etmez.

3) Onay Gereksinimi: İdarenin verilere erişimi için ön onay gerekliliği, erişimin geçerli standartlar, kurallar ve süreçlere uygun olarak yürütülmesini sağlamak için ulusal mevzuat kapsamında belirlenir. Bu gereklilikler, idarenin erişiminin bir sonucu olarak mahremiyete ve diğer insan hak ve özgürlüklerine yapılacak müdahalenin derecesi ile

⁴⁸³ OECD’nin bu konudaki önceki çalışmalarında bu ilkeler temel hatlarıyla belirlenmiş ve bu ilkeler üzerinde çalışmayı sürdürüp ek koruma mekanizmaları hazırlayan çalışma grubu, 24 Haziran 2021 tarihli kamuya açık olmayan bir OECD Sekreterliği iç belgesinde özellikle mecburi paylaşıma uygulanabilen daha ayrıntılı yedi ilke belirlemiştir. Bkz. Swire/Propp/Christakis, (<https://www.lawfareblog.com/towards-oecd-principles-government-access-data>, Erişim Tarihi:15.11.2022). Ancak Direktif’ten görülebileceği üzere özellikle mecburi paylaşım ile ilgili bu ayrıntılı düzenlemeler tam olarak kabul görmemiştir. Bkz. (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>, Erişim Tarihi: 15.11.2022).

orantılı olup onay isteme ve verme kriterlerini, izlenecek prosedürü ve onayı verecek kuruluşu belirtir.

4) Kişisel verilerin işlenmesi: Devlet erişimi yoluyla elde edilen kişisel veriler yalnızca yetkili personel tarafından işlenebilir ve kullanılabilir. İdare tarafından elde edilen veriler, mahremiyet, güvenlik ve bütünlüğü koruyacak şekilde doğru ve güncel olarak yalnızca yasalarda izin verilen süre boyunca saklanır ve saklama yetkisi yoksa silinir.

5) Şeffaflık: Vatandaşların, idarenin kişisel verilere erişiminin kendi mahremiyetleri ve diğer insan hakları üzerindeki potansiyel etkisini değerlendirebilmeleri için idarenin erişimine ilişkin yasal çerçeve açık ve kamuoyu tarafından kolayca erişilebilir olmalıdır. Ancak ulusal güvenlik veya kolluk faaliyetlerine zarar verecek bilgilerin ifşa edilmesi ile kişilerin ve kamunun bilgilendirilme menfaatinin çatıştığı durumlarda, bu iki çatışan menfaat arasında dengeyi sağlayan mekanizmalar bulunmalıdır.

6) Gözetim: Devlet erişiminin yasal çerçeveye uygunluğunu sağlamak üzere etkili ve tarafsız gözetim mekanizmaları mevcuttur. Bu gözetim, iç uyum ofisleri, mahkemeler, parlamento veya yasama komiteleri ve bağımsız idari otoriteler gibi organlar aracılığıyla sağlanmaktadır. Gözetim organlarının, görevlerini yerine getirirken müdahalelere karşı korunmaları ve görevlerini etkin bir şekilde yerine getirmeleri için mali, beşerî ve teknik kaynaklar sağlanır. Bu organlar, elde ettikleri bulgularını belgelendirir, raporlar hazırlar ve tavsiyelerde bulunurlar ve bu kaynaklar mümkün olduğunca kamuya açık olmalıdır.

7) Hukuki Çözüm Yolları: Ulusal mevzuat, ihlallerin tespit edilmesi ve giderilmesi için etkili çözüm yolları sunar. Bu çözüm yolları mahkemeler gibi bağımsız kurumların veya diğer tarafsız kuruluşların eliyle gerçekleştirilmelidir. Bu çözüm

mekanizmalarının işleyişinde ulusal güvenlik ve kolluk faaliyetlerinin gizliliğinin korunması ihtiyacı dikkate alınır. Bu bağlamda, bireylerin verilerine erişilip erişilmediği veya bir ihlalin gerçekleşip gerçekleşmediği konusunda bilgilendirilmelerine ilişkin hususlarda sınırlamalar getirilebilir. Çözüm yolları, somut olayın şartları göz önünde tutularak, erişimin sonlandırılması, uygunsuz şekilde erişilen veya tutulan verilerin silinmesi, verilerin bütünlüğünün yeniden sağlanması ve hukuka aykırı işlemenin durdurulmasını içerir. Ayrıca, koşullara bağlı olarak, bireyin uğradığı zararların tazmin edilmesi de gerekebilir⁴⁸⁴.

Bu ilkelerin tamamı idarenin özel sektördeki kişisel verilere erişiminin hukuki ve makul bir çerçevede gerçekleşmesi açısından çok önemlidir. Ancak kanımızca, kişi hakları ve kamu düzeni arasında dengenin sağlanabilmesi için en önemli şart idarenin

⁴⁸⁴ OECD üye devleti tarafından kabul gören bu ilkelere ek olarak aşağıdaki şu ilkeler de dikkate alınabilir: “1) *Adil ve Eşit muamele*: Devlet erişimine ilişkin yasal sistemin işleyişi keyfi olmamalı, yeknesak standartlar ve yöntemlerle yürütülmelidir. Erişime tabi özel sektör aktörlerinin seçiminde adil olmayan, keyfi veya ayrımcı muameleler ortadan kaldırılmalıdır. Devletin talepleri ırk, etnik köken, kültür, din, cinsiyet veya cinsel yönelim gibi herhangi bir temelde önyargı veya ayrımcılığa dayanmamalıdır.

2) *Ekonomik Rasyonellik*: Devlet talepleri, verilerine erişilen özel şirkete aşırı maliyet ve yük getirmekten kaçınılmalıdır.

3) *Sorumluluğun Sınırlandırılması*: Şirketlerin yasal olarak kişisel verileri paylaşma yükümlülüğü olsa bile, kullanıcılar kişisel verileri ifşa ettiği için şirketlerin sorumluluğuna gitmeye çalışabilir. Benzer şekilde, şirketler işledikleri ancak kendilerinin oluşturmadığı kullanıcı verilerinin içeriğinden sorumlu tutulabilir. Bu gibi durumlarda verileri sunan kurumlara sorumluluk muaftiyeti tanınmalıdır. Ancak vergilendirme için uygun mali bilgilerin sağlanması gibi devlet erişiminin amaçlarına sorumluluk olmadan ulaşılamaması hallerinde bu ilke geçerli değildir.

4) *Kanunlar İhtilafının Çözülmesi*: Devletin başka bir yargı alanında özel bir şirket tarafından tutulan verilere erişim talepleri, işletmeler için içinden çıkılması zor hukuk çatışmaları yaratabilir. Bir yargı alanındaki mevzuata uyulmasının başka bir yargı alanındaki mevzuatın ihlali ile sonuçlanmamasını sağlamak için bu tür çatışmaların ve tutarsızlıkların hükümetler arasında gündeme getirilebileceği ve çözülebileceği bir mekanizma geliştirilmelidir. Bu tür bir mekanizma özel sektörün veri sağlama yükümlülüğü ve sır saklama yükümlülüğü arasında bir çatışmada kalmasını engelleyecektir. Ayrıca devletler kendi ulusal mevzuatlarındaki uyumsuzlukları da gidermelidir.” Bkz. Center for International Economic Collaboration: *Forming Rules for Government Access: Toward Optimizing the International Flow of Personal and Non-Personal Data*, 2022, (<https://www.cfiec.jp/en/pdf/gov/gov-2022-11-complete-en.pdf>, Erişim Tarihi:15.01.2023).

şeffaflığının sağlanmasıdır. Zira, yeterince şeffaf olmayan idarenin elindeki gücü aşırı kullanma riski bulunmaktadır. *Snowden* olaylarına kadar idarenin özel sektördeki kişisel verilere aşırı bir erişiminin olması ve ancak kamunun, idarenin gerçekleştirdiği faaliyetleri öğrenmesi sonrasında veri koruma hukuku bakımından çok önemli gelişmeler yaşanması da bu savı destekler niteliktedir⁴⁸⁵. Şeffaflığın hangi dereceye kadar sağlanması gerektiğine kesin bir cevap vermek mümkün olmasa da idarenin yürüttüğü bu faaliyetlerden halkın asgari düzeyde haberdar olması gerekmektedir. Örneğin, sadece bir yıl içerisinde özel sektöre milli güvenlik gibi sebeplerle kişisel veri paylaşım talebiyle kaç kere başvurulduğu ve kaç kişinin verisine erişildiğinin istatistiği bile, idare üzerinde hukuka uygun veri işlenmesi için bir baskı oluşmasına katkı sağlayacaktır. Ülkemizde bu konuda resmi bir istatistik bulunmadığı gibi *Vodafone*'un belirttiği üzere bu istatistikler özel sektörün kendisi tarafından da paylaşılamamaktadır. Almanya gibi bazı ülkelerde ise bu istatistik idarenin kendisi tarafından sağlanmaktadır⁴⁸⁶.

⁴⁸⁵ Snowden sızıntısının AB veri koruma düzenlemeleri üzerindeki etkisi için bkz. Coyne, H.: *The Untold Story of Edward Snowden's Impact on the GDPR*, The Cyber Defense Review 2019, C. IV, S. 2.

⁴⁸⁶ Bkz. Vodafone: *Government assistance demands reporting*, (<https://www.vodafone.com/about-vodafone/reporting-centre/government-assistance-demands-reporting>, Erişim Tarihi: 09.07.2023); Almanya'nın raporları için bkz. (https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152 Erişim Tarihi: 09.07.2023).

SONUÇ

Bilgi toplumunun dinamik gelişimi ve daha kaliteli hizmet ve ürünlere yönelik artan talep, dijital ekonominin hayatın çeşitli alanlarında yaygın bir şekilde gelişmesine yol açmış ve buna bağlı olarak üretilen veri miktarı da giderek artmıştır. Veri hacminin ve dijital teknolojilerin hızla gelişmesi, sadece özel sektörde değil, kamu sektöründe de önemli değişimlere yol açmıştır. Zira, idarenin doğru kararlar alabilmesi ve kamu yararına hareket edebilmesi için, veri analizi yardımıyla doğru bilgiye doğru zamanda ulaşabilmesi ve bu bilgiyi doğru şekilde kullanabilmesi gerekmektedir.

İdare; trafik verilerinin işlenmesi, sosyal yardımların yönetilmesi, verginin toplanması, ulusal sağlık ve eğitim sistemlerinin izlenmesi gibi günlük faaliyetlerinde bir dizi eylem ve işlem yoluyla büyük miktarda veri üretmekte ve toplamaktadır. Bu tür bilgiler, yetkililerin öncelikli alanları belirlemelerine, daha hızlı ve daha bilinçli kararlar almalarına ve gerekli değişiklikleri hayata geçirmelerine olanak tanımaktadır.

Ancak, idarenin veri işleme uygulamaları çoğunlukla kişisel verileri de içereceğinden bu veri işleme faaliyetlerinin temel hak ve özgürlükleri ihlal edebilmesi riski bulunmaktadır. Bu bağlamda, idarenin veri işleme faaliyetlerinin nasıl gerçekleştiği ve bunlardan kaynaklanabilecek problemlerin iyi incelenmesi gerekmektedir. Bu incelemeyi yapabilmek adına idari faaliyetler kapsamında veri işleme uygulamalarını, kamu hizmeti ve idari kolluk kapsamında verilerin işlenmesi olmak üzere iki ana başlık altında incelemenin sistematik olarak faydalı olacağını düşünmekteyiz.

Kamu hizmeti kapsamında idarenin en bilinen veri işleme uygulaması, kamu hizmetlerinin BİT’ler vasıtasıyla dijital ortamda sunulması olarak tanımlanabilecek e-devlet uygulamasıdır. E-devlet her ne kadar kamu hizmetinin sunumunda büyük faydalar sağlasa da kişisel verilerin korunması bakımından taşıdığı riskler de bulunmaktadır. Verilerin ekonomik değere sahip olması dolayısıyla, e-devlet üzerinde tutulan veriler her zaman siber saldırı riski altındadır. Hatta, e-devlete dışarıdan bir siber saldırı gerçekleştirilmese bile uygulamadaki hatalar ve dikkatsizlikler nedeniyle kişisel verilerin e-devlet üzerinden sızması da pratikte karşılaşılabilen bir durumdur. Bu sebeple, idarenin veri güvenliğini sağlamak için KVKK’da da belirtildiği üzere, gerekli tüm teknik ve idari tedbirleri alma yükümlülüğü bulunmaktadır. Ayrıca, kişisel verilerin korunmasının temel ilkelerinden olan amaca bağlılık ilkesi uyarınca e-devletteki kişisel verilerin idare tarafından toplanma amacı dışında kullanılmaması, veriler başka bir veri işleme faaliyeti kapsamında kullanılacaksa da KVKK’daki hukuka uygunluk nedenlerinden birine dayanılması gerekmektedir. Bu bağlamda, kişisel verilerin kamu görevlileri tarafından hukuka aykırı olarak kullanılması, veri güvenliğine ilişkin yükümlülüklerin ihlali kabul edilmektedir.

Ayrıca, e-devlet kapsamında üzerine çok düşülmeyen bir konu da kamu sitelerinde çerezler vasıtasıyla kişisel verilerin işlenmesidir. Birçok devlet internet sitesi, farkında olarak veya olmadan çerezler vasıtasıyla kişisel verileri işlese de bu durumu siteyi kullanan kişilere bildirmemekte, yani aydınlatma yükümlülüğünü yerine getirmemektedir.

Kamu hizmeti kapsamında çok önemli bir diğer uygulama ise idarenin elindeki kamu sektörü bilgisini açık veri olarak paylaşması ve bu verilerin yeniden kullanılabilmesiyle veriden değer elde edilmesidir. Açık veri ve dolayısıyla verinin

yeniden kullanımının idarenin şeffaflığının sağlanması, kamu hizmetlerinin iyileştirilmesi ve ekonomik değer elde edilmesi gibi faydaları bulunmaktadır. Buna karşın açık veri ve mahremiyet birbiriyle çatışan kavramlardır. Zira, veri setleri barındırdıkları kişisel bilgiler oranında değer kazanmaktadır. Bu bağlamda idarenin, kişisel verilerin korunmasıyla ilgili genel çerçeve içerisinde, veri gizliliği ile açık veriden sağlanacak fayda arasında bir denge kurması gerekmektedir. Bunu gerçekleştirebilmek için idarenin açık veri olarak paylaşmak istediği verileri anonimleştirilmesi gerekmektedir. Zira anonimleştirme hem kişilerin mahremiyetini güvenceye alacak hem de veri işleme faaliyetini KVKK kapsamı dışına çıkartarak hukuka uygun hale getirecektir. Ancak, anonimleştirme mutlak bir koruma sağlamamaktadır çünkü, anonim verilerin birtakım yöntemlerle tekrar kimliği belirli veya belirlenebilir bir kişiyle ilişkilendirilmesi mümkündür. Bu sebeple, idarenin ulusal ve uluslararası kuruluşların belirlediği birtakım standartlar çerçevesinde anonimleştirme gerçekleştirerek, yeniden kimliklendirme riskini en aza indirmesi gerekmektedir.

İdarenin yukarıda belirtilen veri güvenliği veya uygun anonimleştirme gibi yükümlülüklerini yerine getirmemesinin hizmetin hiç işlememesi veya kötü işlemesi sebebiyle hizmet kusurunu doğuracağı açıktır. Ancak, tartışılması gereken esas konu, idarenin tüm yükümlülüklerini gereği gibi yerine getirmesine rağmen teknolojik gelişmeler neticesinde verilerin hukuka aykırı olarak işlenmesi durumunda ne olacaktır. Zira teknoloji katlanan bir hızda gelişmekte ve bu sayede günümüz şartlarında yeniden kimliklendirilmesi mümkün olmayan bir verinin yeniden kimliklendirilmesi veya yeni siber saldırı yollarının geliştirilmesi her zaman ihtimal dahilindedir. Bu bağlamda iki olası durumdan bahsedilebilecektir. İlk olasılık, idarenin

teknolojik gelişmeleri yakalayamamasının bir hizmet kusuru olarak değerlendirilmesidir. İkinci olasılık ise idarenin gelişen teknolojilere bağlı olarak yürüttüğü hizmetlerin bünyesinde risk barındırdığının kabul edilmesi ile hasar/risk ilkesi kapsamında idarenin sorumluluğuna gitmektedir. Kanımızca her durumda, idarenin elinde tuttuğu verilerin hukuka aykırı olarak işlenmesinden dolayı sorumluluğu doğacaktır. Zira teknolojik gelişmeler sayesinde dijital ortamda büyük miktarda veriyi kolay bir şekilde işleyebilme olanağına kavuşan, yani teknolojinin nimetlerinden faydalanan idarenin, bu teknolojilerin risklerine de katlanması gerekmektedir.

Kolluk kapsamında verilerin işlenmesi ise ayrıca ele alınması gereken bir husustur. Zira kolluk, tanımı gereği, kamu düzeninin sağlanması için idarenin bireylerin özgürlüklerine karışması, sınırlar belirlemesi olduğundan, bu kapsamda gerçekleşen veri işleme faaliyetlerinin kişi hak ve özgürlüklerini ihlal etme tehlikesi çok yüksektir.

Hem ulusal hem uluslararası düzenlemeler incelendiğinde, milli güvenlik veya suçların önlenmesi gibi amaçlarla gerçekleştirilen veri işleme faaliyetlerinin, kişisel verilerle ilgili genel düzenlemelere tabi olmadığı görülmektedir. GDPR’da da böyle bir istisna hali düzenlenmiş olsa da kolluk kapsamında kişisel veri işlenmesinin öneminin farkında olan AB yasa koyucusu, GDPR ile aynı anda, kolluk faaliyetleri kapsamında işlenen kişisel verilerin korunması açısından genel bir düzenleme olan Kolluk Direktifini yürürlüğe koymuştur. Ülkemizde ise kolluk faaliyetleri KVKK’da istisna hallerinden sayılsa da, bu veri işleme faaliyetlerine uygulanacak genel bir düzenlemenin bulunmaması büyük bir eksikliktir. Ancak, bu durum kolluk kapsamında veri işleyen idarenin hiçbir sınırlamaya tabi olmadığı anlamına da

gelmemektedir. Zira, KVKK'nın sağladığı korumadan yararlanılamasa bile kişisel verilerin korunması Anayasamızda bir temel hak olarak düzenlenmektedir. Bu bağlamda, bu hakka yapılacak her türlü sınırlama Anayasamızın 13. maddesi kapsamındaki kısıtlamalara tabi olacaktır.

Kolluk amacıyla yeni teknolojilerin kullanılmaya başlamasıyla da hem kişisel verilerin korunmasına duyulan ihtiyaç hem de kişisel olmasa bile veri işlemeye hakim olan bir takım sınırlama ve ilkelere duyulan ihtiyaç giderek artmaktadır. Yeni veri işleme teknolojilerinin idari kolluk açısından getirdiği en önemli gelişmelerden birisi öngörücü kolluğun pratik olarak uygulama alanı bulmaya başlamasıdır. Veri analizi yardımıyla önleyici kolluk faaliyeti yerine getirmek olarak tanımlanabilecek öngörücü kolluk; gelecekteki suçu ve suçluları önceden tahmin ederek, kamu düzenine yönelik tehditleri daha doğmadan bertaraf etmeyi amaçlamaktadır. Ancak, kamu düzeninin sağlanması açısından yadsınamaz faydaları olan bu faaliyet, çok büyük risk ve endişeleri de beraberinde getirmektedir. İlk olarak, öngörücü kolluk algoritmaları bir veri analizi olduğundan, sistemin eğitildiği verilere bağlı olarak, belirli bir grup veya bölgeye karşı ayrımcılık yapma riski bulunmaktadır. Algoritmanın ayrımcı kararlar almasının doğuracağı en büyük sorun ise sistemin kendisini geri bildirim döngüsüne sokacak olmasıdır. Algoritmanın önyargılı kararları neticesinde, kolluk organları belirli bir grup üzerinde daha çok yoğunlaşacağından, ortaya daha çok önyargılı veri çıkacak ve algoritmanın sağladığı önyargılı kararlar üzerinden daha çok ayrımcı veri üretilerek sistemdeki ayrımcılık güçlenecektir. İkinci problem ise öngörücü kolluk uygulamalarının yeterince şeffaf olmamasından kaynaklanmaktadır. Yapay zeka kullanan bu algoritmaların, hangi kararları nasıl aldığının çözülebilmesi mümkün olmadığından, idarenin faaliyetlerinin objektif bir şekilde değerlendirilebilmesinin de

önü kapanmaktadır. Bu kapsamda, öngörücü kolluk faaliyeti yerine getirirken idarenin ayrıca bir dikkat ve özen göstermesi gerekmektedir.

Bunun yanında, idare her ne kadar kolluk amacıyla kullanabilecek çok miktarda veriye sahip olsa da özel sektördeki veri hacmiyle kıyaslandığında bu miktar az kalmaktadır. Bu sebeple, idarenin özel sektördeki kişisel verilere erişim talebi giderek artmaktadır. İdarenin özel sektördeki kişisel verilere erişim yolları genel hatlarıyla özel sektörün kişisel verileri istem dışı paylaşması ve özel sektörün kişisel verileri gönüllü paylaşması olarak ikiye ayrılmaktadır. İstem dışı paylaşımında idare, özel sektörü verileri paylaşmaya zorlayabileceği gibi, özel sektör aktörlerine hiç başvurmadan doğrudan da verilere erişebilmektedir. Gönüllü paylaşım ise çeşitli sebeplerle ortaya çıkabilmesine rağmen uygulamada en sık karşılaşılan yöntemi verilerin kar elde etmek için idareye satılmasıdır.

Yakın bir tarihe kadar idarenin bu uygulamaları kamuya gizli bir şekilde gerçekleştiğinden, bu konuda henüz uluslararası standartlar belirlenmemiş olsa da, kişisel verilerin korunması özel hayatın gizliliği kapsamında bir temel hak olduğundan dolayı idarenin bu verileri özel sektörden elde etmesinin sınırları ölçülülük ilkesi kapsamında yargı içtihatlarıyla belirlenmektedir. Ayrıca, uluslararası kuruluşlar verilerin serbest dolaşımının sağlanması için bu konuda temel ilke ve prensipler geliştirmeye çalışmaktadır. Kanaatimizce özel sektördeki kişisel verilere erişim noktasında kişisel verilerin en çok korunmasını sağlayacak yöntem idarenin şeffaflığının artırılmasıdır. Zira idarenin uygulamaları halk tarafından öğrenildiği takdirde idare elindeki gücü aşırı bir şekilde kullanarak hukuka aykırı veri işlemekten kaçınacaktır. İdarenin özel sektördeki verilere erişim yöntemlerinin kısıtlanması ve bu konuda çalışmalara başlanması ancak bu uygulamaların sızıntılar yoluyla

kamuoyuna duyurulmasından sonra gerekleşmesi de bu düşüncemizi desteklemektedir.



KAYNAKÇA

Ackoff, R. L: *On Learning and the Systems That Facilitate It*, Reflections 1999, C. I, S. 1, s. 14–24.

Agbozo, E.: *Personal Data and Privacy Barriers to E-Government Adoption, Implementation and Development in Sub-Saharan Africa*, Electronic Governance and Open Society: Challenges in Eurasia (Ed. Voigt, P./ von dem Bussche, A.), 5th International Conference 2018, s. 82-91 (https://doi.org/10.1007/978-3-030-13283-5_7 Erişim Tarihi: 17.06.2023).

Aksoy, H. C./ Halıcıoğlu, M.: *AB ve Türk Hukuklarında Çerezler*, Kişisel Verileri Koruma Dergisi 2021, C. 3, S. 1, s. 61-88.

Aksoy, H. C.: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi 2022, C. IV, S. 2, s. 69-87 (Algoritmik Karar).

Aksoy, H. C: *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması*, Ankara 2010 (Kişilik Hakkı Yönünden Kişisel Verilerin Korunması).

Akyılmaz, B. /Sezginer, M. /Kaya, C.: *Türk İdare Hukuku*, 16. Baskı, Ankara 2023.

Al-Jamal, M./ Abu-Shanab, E.: *Privacy Policy of E-Government Websites and the Effect on Users' Privacy*, International Conference on Information Technology 2015, s. 338-344.

Altındağ, H.: *Kişisel Verilerin Korunması Bağlamında İdarenin Sorumluluğu*, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi 2019, C. XVIII, S. 2, s. 387-401.

An Coimisiun Um Chosaint Sonrai: *Guidance Note: Legal Bases for Processing Personal Data*, 2019, (<https://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data>, Eriřim Tarihi: 17.06.2023) (Guidance Note: Legal Bases for Processing Personal Data).

An Coimisiun Um Chosaint Sonrai: *Principles of Data Protection*, (<https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>, Eriřim Tarihi: 20.06.2023) (Principles of Data Protection).

Article 29 Data Protection Working Party: *Opinion 03/2013 on Purpose Limitation*, 2013, s. 35, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, Eriřim Tarihi: 11.07.2023) (Purpose Limitation).

Article 29 Data Protection Working Party: *Opinion 4/2007 on The Concept Of Personal Data*, 01248/07/EN WP 136 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, Eriřim Tarihi: 15.06.2023) (The Concept Of Personal Data).

Ařıkoęlu, ř. İ.: Avrupa Birlięi ve Trk Hukukunda Kiřisel Verilerin Korunması ve Byk Veri, İstanbul 2018.

Atay, E. E.: İdare Hukuku, 7. Baskı, Ankara 2021.

Ayzger ngn, .: Kiřisel Verilerin Korunması Hukuku, 2. Baskı, Ankara 2019.

Başar, C.: Trk İdare Hukuku ve Avrupa Birlięi Hukuku Iřıęında Kiřisel Verilerin Korunması, İstanbul 2020.

Berends, J./ Carrara, W./ Engbers, W./ Vollers, H.: *Reusing Open Data: A Study on Companies Transforming Open Data Into Economic and Societal Value*, Publications Office of the European Union 2020, s. 1-106.

BIAC: *The OECD Process to Develop Common Principles for Trusted Government Access to Data: BIAC Supports Continuation and Successful Completion of the Process with Timely Outcomes: Draft 2.0 for Discussion Only*, 2021, (<https://25159535.fs1.hubspotusercontent-eu1.net/hubfs/25159535/website/documents/pdf/Digital%20Economy/The%20OECD%20Process%20to%20Develop%20Common%20Principles%20for%20Trusted%20Government%20Access%20to%20Data%20BIAC%20Supports%20Continuation%20and%20Successful%20Completion%20of%20the%20Process%20with%20Timely%20Outcomes.pdf>, Erişim Tarihi: 15.01.2023).

Biddle, S.: *ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months*, The Intercept 2022, (<https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/>, Erişim Tarihi: 15.01.2023).

Bignami, F.: *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens* (PE 519.215), Committee On Civil Liberties, Justice and Home Affairs 2015.

Bond, R.: *The EU E-Privacy Directive and Consent to Cookies*, Business Lawyer 2012, C. 68, S. 1, s. 215-224.

Brown, I.: *Government Access to Private-Sector Data in the United Kingdom*, International Data Privacy Law 2012, C.II, S.4, s. 230-238.

Bundesverfassungsgericht: *Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional*, Press Release No. 18/2023, (<https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html>, Eriřim Tarihi: 06.07.2023).

Cahn, A/ Alfeld, S./ Barford, P. R./ Muthukrishnan, S.: *An Empirical Study of Web Cookies*, Proceedings of the 25th International Conference on World Wide Web 2016, s. 891 – 901.

Cate, F. H./Dempsey, J. X./Rubinstein, I. S.: *Systematic Government Access To Private- Sector Data, International Data*, Privacy Law 2012, C.II, S.4, s. 195–199.

Cavanillas, J. M./ Curry, E./ Wahlster, W.: *The Big Data Value Opportunity*, i. New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe (ed. Cavanillas, Jos Mara/ Curry, Edward/ Wahlster, Wolfgang), New York 2016, s. 3-11.

CDC: *About CDC’s Flu Forecasting Efforts, Centres For Disease Control And Prevention*, (<https://www.cdc.gov/flu/weekly/flusight/how-flu-forecasting.htm>, Eriřim Tarihi: 04.06.2023).

Centel, N. / Zafer, H.: *Ceza Muhakemesi Hukuku*, Gzden Geirilmiş 20. Baskı, İstanbul 2021.

Center for International Economic Colloboration: *Forming Rules for Government Access: Toward Optimizing the International Flow of Personal and Non-*

Personal Data, 2022, (<https://www.cfiec.jp/en/pdf/gov/gov-2022-11-complete-en.pdf>, Eriřim Tarihi: 15.01.2023).

Charalabidis, Y./ Zuiderwijk, A./ Alexopoulos, C./ Janssen, M./ Lampoltshammer, T./ Ferro, E.: *The World of Open Data: Concepts, Methods, Tools and Experiences*, 2018.

Chin, C.: *Digital Dragnets: Examining the Government's Access to Your Personal*, 2022. (<https://www.csis.org/analysis/digital-dragnets-examining-governments-access-your-personal-data>, Eriřim Tarihi: 15.01.2023).

Chin, K.: *Biggest Data Breaches in Europe [Updated 2023]*, (www.upguard.com/blog/biggest-data-breaches-europe, Eriřim Tarihi: 02.05.2023).

Cimpanu, C.: *Dutch Government Loses Hard Drives With Data of 6.9 Million Registered Donors*, ZDNET 2020, (www.zdnet.com/article/dutch-government-loses-hard-drives-with-data-of-6-9-million-registered-donors, Eriřim Tarihi: 02.05.2023).

Civelek, M.E.: *Elektronik Devletin Geliřim Evreleri*, Opus Uluslararası Toplum Arařtırmaları Dergisi, 2019, C. 13, S. 19, s. 2533-2548.

Cookie Script: *Cookie Law Explained*, 2022, (<https://cookie-script.com/blog/cookie-law>, Eriřim Tarihi: 11.07.2023).

Cox, J.: *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE 2020, (<https://www.vice.com/en/article/jgqmq5x/us-military-location-data-xmode-locate-x>, Eriřim Tarihi: 15.01.2023).

Coyne, H.: *The Untold Story of Edward Snowden's Impact on the GDPR*, The Cyber Defense Review 2019, C. IV, S. 2. s. 65-79.

Cumhuriyet Gazetesi: *Hukukçulardan Murat Kurum'un SMS Yollamasına İlişkin Açıklama*, 2023, (www.cumhuriyet.com.tr/turkiye/hukukculardan-murat-kurumun-sms-yollamasina-iliskin-aciklama-2077190, Erişim Tarihi: 03.05.2023).

Curry, E.: *The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches*, iç. New Horizons for a Data-Driven Economy (ed. Cavanillas, José María/ Curry, Edward/ Wahlster, Wolfgang), New York, 2016, s. 29-38.

Custers, B./ Ursic, H.: *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection*, International Data Privacy Law 2016, C. VI, S.1, s. 1-18.

Çarıkçı, O.: *Türkiyede E-Devlet Uygulamaları Üzerine Bir Araştırma*", Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 2010, C. 12, S. 12, s. 95–122.

Çekin, M. S./Berktaş, A.S./ Akıncı, M. F.: *Veri Hukuku*, İstanbul 2023.

Çekin, M. S.: *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, 3. Baskı, İstanbul 2020.

Darbishire, H.: *Proactive Transparency: The Future of the Right to Information?*, World Bank Group, Governance Working Paper Series: 56598, 2010.

Data Protection Bill 2018: Second stage. Seanad E' ireann debate, 08,02,2018, C. 255 S. 14, <https://www.oireachtas.ie/en/debates/debate/seanad/2018-02-08/9/> (Eriřim Tarihi: 02.07.2023).

Data.Europa: *Protecting Data and Opening Data*, 2018, (<https://data.europa.eu/en/publications/datastories/protecting-data-and-opening-data>, Eriřim Tarihi: 09.05.2023) (Opening Data).

Data.Europa: *The Benefits and Value of Open Data*, 2020, (<https://data.europa.eu/en/publications/datastories/benefits-and-value-open-data>, Eriřim Tarihi: 24.03.2023) (Benefits).

Data.Europa: *Unlocking Value from Open Data*, (<https://data.europa.eu/elearning/en/module2/#!/id/co-01>, Eriřim Tarihi: 23.03.2023) (Unlocking Value).

Data.Europa: *What Is Open Data*, (<https://data.europa.eu/en/trening/what-open-data>, Eriřim Tarihi: 09.03.2023) (What Is Open Data).

Desouza, K. C./ Jacob, B.: *Big Data in the Public Sector: Lessons for Practitioners and Scholars*, Administration & Society, C. XLIX, S. 7, s. 1043–1064.

Devlet Planlama Teřkilatı Yönetim Bilgi Merkezi Dairesi KamuNet Teknik Kurulu Başkanlığı: *e-Devlet'e Geçiř Sürecinde KamuNet Çalışmaları*, 2002 (http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/e-Devlete_Gecis_Surecinde_KAMU-NET_Calismalari.pdf, Eriřim Tarihi: 17.06.2023).

Doğan, K./ Arslantekin, S.: *Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum*, Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi (DTCF) 2016, C. 56, S. 1, s. 15-36.

Dove, E.S./ Jiahong,C.: *What Does It Mean for a Data Subject to Make Their Personal Data ‘Manifestly Public’? An Analysis of GDPR Article 9(2)(e)*, International Data Privacy Law 2021, C. XI, S. 2, s. 107–124.

Döner, A.: Şeffaf Devlette Bilgi Edinme Hakkı, İstanbul 2010.

Dülger, M. V.: *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 2016, C. III, S. 2, s. 101-167.

EDPB: Guidelines 05/2020 On Consent Under Regulation 2016/679, Version 1.1, 2020, s. 20-22
(https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, Erişim Tarihi: 22.06.2023).

Ersay Kekevi, Ç.: *Genel Kavramlar*, iç.Kişisel Verilerin Korunmasına Akademik Bakış - KVKK Akademi Derleme Çalışması (ed. Aksoy, Pınar Çağlayan/ Aksoy, Hüseyin Can), Ankara 2023, s. 103-134.

Espinoza, J./Brunsden, J./Venkataramakrishnan, S.: *EU’s Top Court Blocks States From Gathering User Data for Surveillance*, Financial Times 2020, (<https://www.ft.com/content/71cc07fb-58ff-404d-868c-5dd0e8a97e20>, Erişim Tarihi: 15.11.2022).

European Commission: Communication to the Commission-Data, Information and Knowledge Management at the European Commission, 2016, C (2016) 6626 Final ([https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2016\)6626&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2016)6626&lang=en), Erişim Tarihi: 22.06.2023).

European Commission: *Turkey 2019 Report*, SWD(2019) 220 final, (<https://neighbourhood-enlargement.ec.europa.eu/system/files/2019-05/20190529-turkey-report.pdf> Erişim Tarihi: 11.07.2023) (2021).

European Commission: *Türkiye 2022 Report*, SWD(2022) 333 final, (<https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/Türkiye%20Report%202022.pdf>, Erişim Tarihi: 11.07.2023) (2022).

European Data Protection Supervisor: *10 Misunderstandings Related To Anonymisation*, (https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf, Erişim Tarihi: 09.04.2023).

FRA: *Bias in Algorithms: Artificial Intelligence and Discrimination*, 2022, (<http://fra.europa.eu/en/publication/2022/bias-algorithm>, Erişim Tarihi: 07.07.2023) (Bias in Algorithms).

FRA: *Preventing Unlawful Profiling Today and In The Future: A Guide*, Luxembourg 2018 (Preventing Unlawful Profiling).

FRA: *Test Algorithms for Bias to Avoid Discrimination*, 2022 (<http://fra.europa.eu/en/news/2022/test-algorithms-bias-avoid-discrimination>, Erişim Tarihi: 20.04.2023) (Test Algorithms for Bias).

Ferraris,V./ Bosco, F./ Caffero, G./ D'Angelo, E./ Suloyeva, Y.: *Working Paper: Defining Profiling*, 2013.

Finck, M./Biega, A.: *Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems*, *Technology and Regulation* 2021, s. 44–61.

Fredriksson, C./ Mubarak, F./ Tuohimaa, M./ Zhan, M.: *Big Data in the Public Sector: A Systematic Literature Review*, *Scandinavian Journal of Public Administration* 2017, C. 21, S. 3, s. 39–61.

Frennert, S.: *Hitting A Moving Target: Digital Transformation And Welfare Technology in Swedish Municipal Eldercare. Disability and Rehabilitation, Assistive Technology* 2019, C. XVI, S. 1, s. 103–111.

Furrer, A./ Muller-Chen, M./ Çetiner, B.: *Borçlar Hukuku Genel Hükümler*, İstanbul 2021.

Germany Federal Ministry for Digital and Transport: *Open Data*, 2022, (<https://bmdv.bund.de/SharedDocs/EN/Articles/DG/open-data.html>, Erişim Tarihi: 05.07.2023).

Global Freedom of Expression Columbia University: *TLT v. Secretary of State for the Home Department*, 2016, (<https://globalfreedomofexpression.columbia.edu/cases/tlt-v-secretary-state-home-department/>, Erişim Tarihi: 05.05.2023).

Global Network Initiative: *Defining Direct Access: GNI calls for greater transparency and dialogue around mandatory, unmediated government access*

to data, 2021, (https://globalnetworkinitiative.org/defining-direct-access-2/#_ftn2, Eriřim Tarihi 15.01.2023).

Goitein, E.: *The Government Can't Seize Your Digital Data, Except by Buying It*, Washington Post 2021, (<https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/>, Eriřim Tarihi: 15.01.2023).

Gotze, M./ Matic, S./ Iordanou, C./ Smaragdakis, G./ Laoutaris, L.: *Measuring Web Cookies in Governmental Websites*, WebSci '22: 14th ACM Web Science Conference 2022.

Gözler, K. /Kaplan, G.: *İdare Hukuku Dersleri*, Güncellenmiř 22. Baskı, Bursa 2020.

Gözler, K.: *İdare Hukuku, C. II*, Güncellenmiř 3. Baskı, Bursa 2019.

Gözübüyük, A. ř./ Tan, T.: *İdare Hukuku Cilt I Genel Esaslar*, Güncelleřtirilmiř 13. Baskı, Ankara 2019.

Green, B./ Cunningham, G./ Ekblaw, A./ Kominers, P./ Linzer, A./ Crawford, S.P.: *Open Data Privacy*, Harward Public Law Working Paper 2017, s.1-111. (<https://doi.org/10.2139/ssrn.2924751>, Eriřim Tarihi: 09.05.2023).

Grönlund, Å./ Horan, T.A.: *Introducing e-Gov: History, Definitions, and Issues*, Communications of the Association for Information Systems, Association for Information Systems 2004, C. 15, S. 39, s. 713-729.

Gültekin Várkonyi, G.: *Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes*, iç. Digital Criminal Justice: A Studybook Selected Topics for Learners and

Researchers (ed.:Krisztina Karsai, Adem Sözüer, Liane Wörner) Social Science Research Network, İstanbul 2022, s.39-59.

Günday, M.: İdare Hukuku, 11. Baskı, Ankara 2017.

Gündem, F.: *Açık Yönetişim Verisi (Open Government Data) Uygulamaları ve İzmir’de Yerel Fiyatlar*, İzmir Büyükşehir Belediyesi Açık Veri Portalı 2022, (<https://acikveri.bizizmir.com/tr/showcase/acik-yonetisim-verisi-open-government-data-uygulamalari-ve-izmir-de-yerel-fiyatlar>, Erişim Tarihi: 09.03.2023).

Gürpınar, D.: *Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 2017, Prof. Dr. Şeref Ertaş’a Armağan, C. 19, Özel Sayı, s. 679-694.

Hagemann, R./ Huddleston, J./ Thierer, A. D.: *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, Colorado Technology Law Journal 2018, C. XVII, S. 1, s. 38-130.

Harper, J.: *Administering the Fourth Amendment in the Digital Age*, National Constitution Center (<https://constitutioncenter.org/news-debate/special-projects/digital-privacy/the-fourth-amendment-in-the-digital-age>, Erişim Tarihi: 18.04.2023).

Heaven, W.D.: *Predictive Policing Algorithms Are Racist. They Need to Be Dismantled*, MIT Technology Review 2020 (www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice, Erişim Tarihi: 07.07.2023).

Hill, K.: *Wrongfully Accused by an Algorithm*, The New York Times 2020, (www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, Erişim Tarihi: 05.07.2023).

Hinton Jones, N.: *Evidence-based investing: What it is and Why It's Awesome*, 2022, (<https://www.timeline.co/blog/evidence-based-investing-what-it-is-and-why-it-awesome#:~:text=What%20is%20evidence-based%20investing,long-term%20observation%20of%20markets>, Erişim Tarihi: 17.06.2023).

Huyer, E.: *The Economic Impact of Open Data: Opportunities for Value Creation in Europe*. Publications Office of the European Union 2020, (<https://data.europa.eu/doi/10.2830/63132>, Erişim Tarihi: 26.03.2023).

IBM Security: *Cost of a Data Breach Report 2021*, 2021, (www.ibm.com/downloads/cas/OJDVQGRY, Erişim Tarihi: 17.06.2023) (2021).

IBM Security: *Cost of a Data Breach Report 2022*, 2022, (www.ibm.com/downloads/cas/3R8N1DZJi, Erişim Tarihi: 17.06.2023) (2022).

ICO: *A Guide to the Data Protection Principles*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>, Erişim Tarihi: 20.06.2023).

ICO: *Big Data and Data Protection*, 2014, (<https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220> Erişim Tarihi: 04.06.2023).

ICO: *What Are the Rules on Cookies and Similar Technologies?*, (<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules4>, Eriřim Tarihi: 08.05.2023).

ICO: *What Is Valid Consent?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/>, Eriřim Tarihi: 22.06.2023).

ICO: *What is Special Category Data?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/>, Eriřim Tarihi: 15.06.2023).

ICO: *When is Consent Appropriate?*, (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/when-is-consent-appropriate/>, Eriřim Tarihi: 28.06.2023).

International Chamber of Commerce: *ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector*, 2022, (<https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector/>, Eriřim Tarihi: 15.01.2023).

Internet Freedom Foundation: *Watch the Watchmen Series Part 2 : The Centralised Monitoring System*. 2020, (<https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system/>, Eriřim Tarihi 15.01.2023).

Iřıkçı, Y.M.: *E-Devlet Uygulamalarının Hukuk Devletine Etkisi: Yeni Kamu İřletmecilięi Paradigması Üzerinden Bir Deęerlendirme*, Süleyman Demirel

Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2017, C. 22, S. Kayfor15 Özel Sayısı, s. 1893-1913.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü: *Suçların Önlenmesi, Soruşturulması, Ortaya Çıkarılması veya Kovuşturulması ya da Cezaların İnfazı Amacıyla Yetkili Makamlarca Kişisel Verilerin İşlenmesine İlişkin Olarak Gerçek Kişilerin Korunması ve Bu Verilerin Serbest Dolaşımı ile İlgili, 2008/977/Aİİ sayılı Konsey Çerçeve Kararı Yerine Geçen 27 Nisan 2016 tarihli (AB) 2016/680 SAYILI AVRUPA PARLAMENTOSU ve KONSEY DİREKTİFİ Bilgi Notu*, 2019 (<https://itlaw.bilgi.edu.tr/media/2019/7/29/law-enforcement-directive-bilgi-notu.pdf>, Erişim Tarihi: 03.05.2023).

Jacobi, A./ Lund, M./ Kool, L./ Munnichs, G./ Weber, A.: *Security of eGovernment Systems: Final Report*, European Parliament 2013.

Kaltheuner, F. /Elettra, B.: *Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-making in the GDPR*, Journal of Information Rights, Policy, and Practice 2017, C. II, S. 2, s. 1-17.

Kędzior, M.: *GDPR and Beyond: a Year of Changes in the Data Protection Landscape of the European Union*, ERA Forum 2019, s. 505-509. (<https://doi.org/10.1007/s12027-019-00549-x>, Erişim Tarihi: 25.05.2023).

Kerle, I.: *What Is Public Data?* (<https://enigma.com/blog/post/what-is-public-data>, Erişim Tarihi: 09.03.2023).

Ketizmen, M./ Çağlar Ü.: *E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması*, XII. Türkiye’de İnternet Konferansı 2007, (<http://inet-tr.org.tr/inetconf12/bildiri/2.pdf>, Erişim Tarihi: 17.06.2023).

Kıraç, S./ Bayrakçı E.: *E-Devlet Uygulamaları Bağlamında Türkiye’de E-Belediyeçilik Anlayışı*, Balıkesir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2020, C. 1, S. 2, s. 106–128.

Kim, G. U./ Trimi, S./ Chung, J.: *Big-Data Applications in The Government Sector*, Communications of the ACM 2014, C. LVII, S. 3, s. 78-85.

Kişisel Verileri Koruma Kurumu: *Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu*,
(<https://www.kvkk.gov.tr/Icerik/6765/AYDINLATMA-YUKUMLULUGUNUN-YERINE-GETIRILMESI-HAKKINDA-KAMUOYU-DUYURUSU>, Erişim Tarihi: 11.05.2023) (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Hakkında Kamuoyu Duyurusu).

Kişisel Verileri Koruma Kurumu: *“Alenileştirme” Hakkında Kamuoyu Duyurusu*,
(www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU, Erişim Tarihi: 03.05.2023).

Kişisel Verileri Koruma Kurumu: *6698 Sayılı Kanun’da Yer Alan Temel Kavramlar*,
(<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/8110dc3c-2856-4e54-9129-5e2e375469af.pdf>, Erişim Tarihi: 28.06.2023) (6698 Sayılı Kanun’da Yer Alan Temel Kavramlar).

Kişisel Verileri Koruma Kurumu: *Çerez Uygulamaları Hakkında Rehber*, 2022,
(<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf>, Erişim Tarihi: 17.06.2023).

Kişisel Verileri Koruma Kurumu: *İlgili Kişinin Hak Arama Yöntemleri*,
(<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/353d85d5-87df->

[4c91-b08e-b4f0991a80f4.pdf](#), Eriřim Tarihi: 28.06.2023) (İlgili Kiřinin Hak Arama Yöntemleri).

Kiřisel Verileri Koruma Kurumu: Kamuoyu Duyurusu (Belediyeler), 05.11.2021, (<https://www.kvkk.gov.tr/Icerik/7073/BELEDIYELERE-ILISKIN-KAMUOYU-DUYURUSU>, Eriřim Tarihi: 01.07.2023) (Kamuoyu Duyurusu)

Kiřisel Verileri Koruma Kurumu: Kiřisel Veri Güvenlięi Rehberi (Teknik ve İdari Tedbirler), 2021, (https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf, Eriřim Tarihi: 11.07.2023) (Kiřisel Veri Güvenlięi Rehberi).

Kiřisel Verileri Koruma Kurumu: *Kiřisel Verilerin İřlenme řartları*, (<https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/9feefe58-9b0f-49c9-a0c7-2b2eb8c012bb.pdf>, Eriřim Tarihi: 17.06.2023) (Kiřisel Verilerin İřlenme řartları).

Kiřisel Verileri Koruma Kurumu: *Kiřisel Verilerin İřlenmesine İliřkin Temel İlkeler*, (<https://kvkk.gov.tr/SharedFolderServer/CMSFiles/32ff74f6-9798-405a-b3d2-b42d28423fde.pdf>, Eriřim Tarihi: 20.06.2023) (Kiřisel Verilerin İřlenmesine İliřkin Temel İlkeler).

Kiřisel Verileri Koruma Kurumu: *Kiřisel Verilerin Korunmasına İliřkin Bařvuru ve řikâyet Hakkı*, (<https://kvkk.gov.tr/yayinlar/KIřISEL%20VERİLERİN%20KORUNMASIN A%20İLİřKİN%20BAřVURU%20VE%20řİKÂYET%20HAKKI.pdf>, Eriřim Tarihi: 20.06.2023) (Kiřisel Verilerin Korunmasına İliřkin Bařvuru ve řikâyet Hakkı).

Kişisel Verileri Koruma Kurumu: *Veri Sorumlusu ve Veri İşleyen*,
(<https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>, Erişim
Tarihi: 20.06.2023) (Veri Sorumlusu ve Veri İşleyen).

Koch, R.: *Cookies, the GDPR, and the ePrivacy Directive*, GDPR.eu 2019,
(<https://gdpr.eu/cookies/>, Erişim Tarihi: 06.05.2023).

Küzeci E./ Kılıç, Ş.: *698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi
Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer
Aktörler*, Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi 2019, C. XVI,
S.63, s. 947 – 992.

Küzeci, E.: *Kişisel Verilerin Korunması*, 4. Baskı, Ankara 2021.

Layne, K. / Jungwoo L.: *Developing Fully Functional E-government: A Four Stage
Model*, Government Information Quarterly 2001, C. 18, S. 2, s. 122–136.

Leistner, M./ Antonie, L.: *IPR and The Use Of Open Data And Data Sharing
Initiatives by Public and Private Actors (Study commissioned by the European
Parliament's Policy Department for Citizens' Rights and Constitutional Affairs
at the request of the Committee on Legal Affairs)*, 2022, s. 39,
([https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2022\)73
2266](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266) , Erişim Tarihi: 07.07.2023).

Liew, A.: *DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and Their
Interrelationships*, Business Management Dynamics 2013, C. II, S. 10, s. 49-
62.

Lum,K. / Isaac,W.: *To Predict and Serve?*, Significance 2016, C. XIII, S. 5, s. 16-19.

Lynskey, O.: *Criminal Justice Profiling and EU Data Protection Law: Precarious Protection From Predictive Policing*, International Journal of Law in Context 2019, C. XV, S. 2, s. 162–176.

Maraş, G.: *Kamu Yönetimlerinde E-Devlet ve E-Demokrasi İlişkisi*, Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2011, C. 37, s. 121–144.

Meijer, A./Martijn, W.: *Predictive Policing: Review of Benefits and Drawbacks*, International Journal of Public Administration, C. XLII, S. 12, 2019, s.1031-1039.

Moses, L.B./Chan, J: *Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability*, Policing & Society, C. XXVIII, S. 7, 2018, s.808.

NBC News: *Facial Recognition Tool Led to Mistaken Arrest, Lawyer Says*, 2023 (www.nbcnews.com/tech/security/facial-recognition-tool-led-mistaken-arrest-lawyer-says-rcna64270, Erişim Tarihi: 05.07.2023)

Nguyen, S. J.: *What Are Internet Cookies and How Are They Used?*, All About Cookies, 2023, (<https://allaboutcookies.org/what-is-a-cookie>, Erişim Tarihi: 06.05.2023).

OECD: *Background Paper: Implementing E-Government In OECD Countries: Experiences And Challenges*, 2008, s. 2, (<https://www.oecd.org/mena/governance/36853121.pdf>, Erişim Tarihi: 04.06.2023) (Background Paper).

OECD: *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, OECD Publishing Paris 2021, s. 139, (<https://doi.org/10.1787/ce08832f-en> , Eriřim Tarihi: 17.06.2023) (Co-operation).

OECD: *G20 / OECD Compendium of Good Practices on the Use of Open Data For Anti-Corruption*, <https://www.oecd.org/corruption/g20-oecd-compendium-open-data-anti-corruption.htm>, Eriřim Tarihi: 22.03.2023) (Anti-Corruption).

OECD: *Government Access to Personal Data Held by the Private Sector: Statement by the OECD Committee on Digital Economy Policy*, (<https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm>, Eriřim Tarihi: 15.01.2023) (Personal Data).

OECD: *Government at a Glance 2011*, 2011, s.142 (https://www.oecd-ilibrary.org/governance/government-at-a-glance-2011_gov_glance-2011-en Eriřim Tarihi: 11.07.2023) (Glance 2011).

OECD: *Government at a Glance 2019*, (<https://doi.org/10.1787/8ccf5c38-en>, Eriřim Tarihi: 17.06.2023) (Glance).

OECD: *Proactive Disclosure of Information, in Government at a Glance*, Paris 2011 (Proactive).

OECD: *Recommendation of the Council on Digital Government Strategies*, 2014, (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406>, Eriřim Tarihi: 17.06.2023) (Digital Government Strategies).

OECD: *Recommendation of the Council on Digital Security Risk Management*, 2022, (<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479>,

Erişim Tarihi: 02.05.2023) (Digital Security).

OECD: *The OECD Digital Government Policy Framework: Six dimensions of a Digital Government*, OECD Public Governance Policy Papers No. 02, 2020 (<https://www.oecd.org/governance/the-oecd-digital-government-policy-framework-f64fed2a-en.htm>, Erişim Tarihi: 17.06.2023) (Policy Framework).

Oğuz, S.: *Kişisel Verilerin Korunması Hukukunun Genel İlkeleri*, Bilgi Ekonomisi ve Yönetimi Dergisi 2018, C. XIII, S. 2, s. 121–138.

Oğuzman, M.K./ Öz, M. T.: *Borçlar Hukuku Genel Hükümler*, C.I, İstanbul 2012.

Open Data Charter: *Open up Guide: Using Open Data to Combat Corruption: Version 2.0*, 2018. (<https://drive.google.com/file/d/1efBzdh2A4pIOvTGuAaIMzaVm05oBjMzc/view>, Erişim Tarihi: 06.04.2023).

Open Knowledge: *Open Data Handbook: Why Open Data?* (<https://opendatahandbook.org/guide/en/why-open-data/>, Erişim Tarihi: 24.03.2023).

Opendatasoft: *Public Data*, 2023, (www.opendatasoft.com/en/glossary/public-data, Erişim Tarihi: 09.03.2023).

OECD: *Assessing Government Initiatives on Public Sector Information: A Review of the OECD Council Recommendation*, OECD Digital Economy Papers 2015, No. 248, (<https://doi.org/10.1787/5js04dr9l47j-en>, Erişim Tarihi: 20.06.2023)

(Assessing Government Initiatives on Public Sector Information: A Review of the OECD Council Recommendation).

OECD: *Data-Driven Innovation: Big Data for Growth and Well-Being*, Paris 2015, (<https://doi.org/10.1787/9789264229358-en>, Erişim Tarihi: 20.06.2023) (Data-Driven Innovation: Big Data for Growth and Well-Being).

OECD: *Fostering Innovation in the Public Sector*, Paris 2017, (<https://doi.org/10.1787/9789264270879-9-en>, Erişim Tarihi: 20.06.2023) (Fostering Innovation in the Public Sector).

Osimo, D.: *Rethinking the Impact of Open Data: Towards a European Impact Assessment for Open Data*. Publications Office of the European Union 2023, s. 26 (<https://data.europa.eu/doi/10.2830/911822>, Erişim Tarihi: 24.03.2023).

Page, C.: *US Government Bans Huawei, ZTE and Hikvision tech over 'unacceptable' spying fears*. Techcrunch 2022, (<https://techcrunch.com/2022/11/28/fcc-huawei-zte-hikvision-hytera-dahua-ban/>, Erişim Tarihi: 15.01.2023).

Pearsall, B.: *Predictive Policing: The Future of Law Enforcement?*, NIJ Journal 2010, S. 266, s. 16-19.

Perry, W.L./McInnis, B./ Price, C.C./ Smith, S./Hollywood, J.S.: *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation eBooks 2013.

Peters, M.: *Germany Finally Has an Open Data Law*, Open Government Partnership 2017, (<https://www.opengovpartnership.org/stories/germany-finally-has-an-open-data-law/>, Erişim Tarihi: 04.07.2023).

PricewaterhouseCoopers: *The Impact of the Open Geographical Data – Follow up Study*, 2017, (<https://sdfe.dk/media/2917052/20170317-the-impact-of-the-open-geographical-data-management-summary-version-13-pwc-qrvkvdr.pdf>, Erişim Tarihi: 28.04.2023).

Queensland Government: Queensland Government Open Data Policy Statement, (https://www.data.qld.gov.au/_resources/documents/qld-data-policy-statement.pdf, Erişim Tarihi: 06.04.2023).

Reddick, C. G.: *A Two-stage Model of E-government Growth: Theories and Empirical Evidence for U.S. Cities*, Government Information Quarterly 2004, C. 21, S. 1, s.51–64.

Regner, E.: *Parliamentary Question: Translated EU Documents Used by Google to Develop Its Language Software*, E-3436/2010, European Parliament, European Union 2010, (www.europarl.europa.eu/doceo/document/E-7-2010-3436_EN.html, Erişim Tarihi: 28.04.2023).

Rubinstein, I. S./Nojeim, G. T./Lee, R. D.: *Systematic Government Access to Personal Data: A Comparative Analysis*, International Data Privacy Law 2014, C. IV, S.2, s. 96–119.

Sahu, M: *Big Data in the Public Sector: Applications and Benefits*. Analyticssteps, 2021, (<https://www.analyticssteps.com/blogs/big-data-public-sector-applications-and-benefits> Erişim Tarihi: 15.01.2023).

Saka, E.: *Polislik Algoritmaları Bağlamında Öngörücü Algoritmalar (Predictive Algorithms) Eleştirel Bir Yaklaşım*, iç. Algoritmaların Gölgesinde Toplum ve İletişim, Alternatif Bilişim 2021, s. 67-80.

Savage, C.: *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says.* The New York Times 2021, (<https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html>, Eriřim Tarihi: 15.01.2023).

Saygı, S.: *6698 Sayılı Kanun'un Sistematiğinde Yargısal Başvuru Yolları*", Kiřisel Verileri Koruma Dergisi 2002, C. II, S. 2, s. 30-60.

Scassa, T.: *Issues in Open Data – Privacy*, iç. The State of Open Data: Histories and Horizons (ed. Tim Davies/ Stephen B.Walker/ Mor Rubinstein/ Fernando Perini), Cape Town ve Ottawa 2019, s. 339- 350.

Schneier, B.: *Do You Want the Government Buying Your Data From Corporations?*, 2013, (<https://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/>, Eriřim Tarihi: 15.01.2023).

Schroers, J.: *Are Public Keys Personal Data?*, CITIP Blog, 2018, (www.law.kuleuven.be/citip/blog/are-public-keys-personal-data, Eriřim Tarihi: 28.04.2023).

Shastri, A./ Deshpande, M.: *A Review of Big Data and Its Applications in Healthcare and Public Sector*, iç. Big Data Analytics in Healthcare, Studies in Big Data (ed. Kulkarni, Anand J./ Siarry, Patrick/ Singh, Pramod Kumar/Abraham, Ajith/ Zhang , Mengjie/ Zomaya, Albert/ Baki, Fazle), C. 66, Cham 2020, s. 55-66.

Cookieyes: *ePrivacy Regulation: What Is It & How Does It Affect Cookies*, 2022, (www.cookieyes.com/blog/eprivacy-regulation, Eriřim Tarihi: 08.05.20203).

Simperl, E./ Gomer, R./ O'Hara, K.: *Analytical Report 3: Open Data and Privacy,*
European Data Portal 2019,

(https://data.europa.eu/sites/default/files/open_data_and_privacy_v1_final_clean.pdf, Eriřim Tarihi: 09.05.2023).

State Secretariat for International Finance: *Switzerland Suspends AEOI With Bulgaria,*
(www.sif.admin.ch/sif/en/home/documentation/specialist-information/archive/suspension-aeoi-bulgaria.html Eriřim Tarihi: 02.05.2023).

Swire, P./Propp K./Christakis, T.: *Towards OECD Principles for Government Access to Data,* Lawfareblog 2021, (<https://www.lawfareblog.com/towards-oecd-principles-government-access-data>, Eriřim Tarihi: 15.11.2022).

řanlı, C.: *Milletlerarası Özel Hukuk*, 8. Baskı, İstanbul 2020.

Tajuelo, G. P.: *How AI Can Be Biased Against Certain Groups of People and What We Can Do to Prevent It,* Medium 2022 (<https://medium.com/latinxinai/how-ai-can-be-biased-against-certain-groups-of-people-and-what-we-can-do-to-prevent-it-7df28bff0a06>, Eriřim Tarihi: 05.07.2023).

Tansuğ, Ç.: *Türkiye'de İdari Faaliyetlerde Büyük Veri Uygulamaları*, iç. Geliřen Teknolojiler ve Hukuk III (Ed. Aksoy Retornaz, Eylem/ Güçlütürk, Osman Gazi), İstanbul 2021, s. 221-255.

Tau, B./ Hackman, M.: *Federal Agencies Use Cellphone Location Data for Immigration Enforcement,* WSJ 2020, (<https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600>, Eriřim Tarihi: 15.01.2023).

Taylor, P.: *Amount of data Created, Consumed, and Stored 2010-2020, with Forecasts to 2025* (Veri Kümesi), Statista (<https://www.statista.com/statistics/871513/worldwide-data-created/>, Erişim Tarihi: 17.06.2023).

Tercier, P./Pichonnaz, P./ Develioğlu, M.: *Borçlar Hukuku Genel Hükümler*, İstanbul 2020.

The Group of Twenty: *G20 Anti-Corruption Open Data Principles*, (<http://www.g20.utoronto.ca/2015/G20-Anti-Corruption-Open-Data-Principles.pdf>, Erişim Tarihi: 22.03.2023).

The National Cyber Security Centre: *General Data Protection Regulation (GDPR)*, (www.ncsc.gov.uk/information/gdpr#:~:text=What%20does%20the%20GDPR%20mean,to%20take%20%27appropriate%27%20action, Erişim Tarihi: 02.05.2023).

The Office of the Information Commissioner Queensland: *Privacy and Public Data Managing Re-identification Risk*, Report No. 1 to the Queensland Legislative Assembly for 2020-21, 2020, (https://www.oic.qld.gov.au/_data/assets/pdf_file/0016/43045/Privacy-and-public-data-managing-re-identification-risk.pdf, Erişim Tarihi: 09.04.2023).

The World Bank: *Starting an Open Data Initiative*, (<http://opendatatoolkit.worldbank.org/en/starting.html>, Erişim Tarihi: 17.03.2023).

Transparency International: *Open Data: Promise, but Not Enough Progress From G20 Countries*, 2019, (<https://www.transparency.org/en/news/open-data->

[promise-but-not-enough-progress-from-g20-countries](#), Eriřim Tarihi: 22.03.2023).

Turan, M.: Karşılařtırılmalı Hukukta Kiřisel Verilerin Korunması, 4. Baskı, Ankara 2017.

Türkiye Bilgi ve İletişim Teknolojileri Dairesi Başkanlığı: *E-Dönüşüm*, 20.01.2015, (www.bilgitoplumu.gov.tr/bilgi-toplumu/e-donusum-projesi, Eriřim Tarihi: 28.04.2023).

U.S. Senator Ron Wyden of Oregon's Press Release: *Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not for Sale Act*, 2021, (www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-#:~:text=The%20Fourth%20Amendment%20is%20Not%20for%20Sale%20Act%20closes%20the,other%20businesses%20that%20have%20direct, Eriřim Tarihi: 15.01.2023).

Ubaldi, B.: *Rebooting Public Service Delivery: How Can Open Government Data Help to Drive Innovation?* OECD Comparative Study 2016, (<https://www.oecd.org/gov/digital-government/rebooting-public-service-delivery.htm>, Eriřim Tarihi: 22.03.2023) (Drive Innovation).

Ubaldi, B.: *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, OECD Working Papers on Public Governance 2013, No: 22 (Open Government Data).

UK Parliament Post: *Sharing Public Sector Data*, Postnote No:664, (<https://researchbriefings.files.parliament.uk/documents/POST-PN-0664/POST-PN-0664.pdf>, Eriřim Tarihi: 24.03.2023).

UK The Home Office: *Impact Assessment, Data Protection Bill: Implementing the European Union Law Enforcement Directive*, HO0295, 2019, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711221/Law_Enforcement_Directive_Impact_Assessment.pdf, Eriřim Tarihi: 20.04.2023).

Ulusoy, A. D.: *Türk İdare Hukuku*, 5. Baskı, Ankara 2023.

UN e-Government Knowledgebase: “Overview.”, (<https://publicadministration.un.org/egovkb/en-us/Overview#whatis>, Eriřim Tarihi: 25.04.2023).

United Nations Asian and Pacific Training Centre for Information and Communication Technology: *Case Study on Open Government Data Policies and Practices in the Republic of Korea*, s. 3-4. (<https://www.unapcict.org/resources/publications/case-study-open-government-data-policies-and-practices-republic-korea>, Eriřim Tarihi: 17.03.2023).

University of Wisconsin-Madison Research Data Services: *The Benefits of Reusing Research Data*, 2020, <https://researchdata.wisc.edu/uncategorized/the-benefits-of-reusing-research-data/#:~:text=It%20saves%20time%20and%20resources,dramatically%20accelerate%20your%20own%20work.>, Eriřim Tarihi: 07.03.2023).

Us Doğan, E.: *Başvuru ve Şikâyet Usulleri ile Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü*, iç. Kişisel Verilerin Korunmasına Akademik Bakış - KVKK Akademi Derleme Çalışması (ed. Aksoy, Pınar Çağlayan / Aksoy, Hüseyin Can), Ankara 2023, s. 211-252.

Gerards, J./ Xenidis, R.: *Algorithmic discrimination in Europe : challenges and opportunities for gender equality and non-discrimination law*, European Network Of Legal Experts in Gender Equality And Non-Discrimination 2021, (<https://data.europa.eu/doi/10.2838/544956>, Erişim Tarihi: 09.08.2023)

Van Ooijen, C./ da Silva Carvalho, N./ Iordache, A./ Osimo, D.: *Measuring Data Demand Within the Public Sector (Güncellenmiş)*, Data.Europa 2022.

Van Ooijen, C./ Ubaldi, B./ Welby, B.: *A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance*, OECD Working Papers on Public Governance 2019, No. 33, (<https://doi.org/10.1787/09ab162c-en>, Erişim Tarihi: 22.03.2023).

Van Schalkwyk, F.: *Open Data and the Fight Against Corruption in South Africa*, Transparency International 2017, (http://webfoundation.org/docs/2017/04/2017_OpenDataSouthAfrica_EN-2.pdf, Erişim Tarihi: 23.03. 2023).

Vancauwenberghe, G./ Cromptvoets, J.: *Governance of Open Data Initiatives*, iç.: Open Data Exposed (ed. Bastiaan van Loenen/Glenn Vancauwenberghe/Joep Cromptvoets) Information Technology and Law Series, C. XXX, Hague 2018.

Viana, A. C. A.: *“Digital Transformation in Public Administration: From E-Government To Digital Government”*, International Journal Of Digital Law (IJDL), 2021, C.2, S.1, s. 29-46.

Vodafone: *Government assistance demands reporting*, (<https://www.vodafone.com/about-vodafone/reporting-centre/government-assistance-demands-reporting>, Erişim Tarihi: 09.07.2023).

Welby, B./ Ubaldi B./ van Oijen, C.: *A Data-driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance*, OECD Working Papers on Public Governance No: 33 2019, s. 6 (<https://doi.org/10.1787/09ab162c-en> Erişim Tarihi: 17.06.2023).

Wessel-Tolvig, B.: *CNIL to Enforce Cookie Rules in France*, Cookie Information 2021, (<https://cookieinformation.com/resources/blog/cnil-to-enforce-cookie-rules-in-france/>, Erişim Tarihi: 27.06.2023).

Wetzling, T./Sarkesian,L./Dietrich,C.: *Solving the Transatlantic Data Dilemma : Surveillance Reforms to Break the International Gridlock*, 2021, (<https://www.newamerica.org/oti/reports/solving-the-transatlantic-data-dilemma/>, Erişim Tarihi: 15.11.2022).

Wigmore, I.: *Definition log (log file)*, (<https://www.techtarget.com/whatis/definition/log-log-file>, Erişim Tarihi: 25.05.2023).

Wikrent, K.: *Red Flags for Integrity: Giving the Green Light to Open Data Solutions*, Open Contracting Partnership 2016, (<https://www.open->

contracting.org/2016/11/30/red-flags-integrity-giving-green-light-open-data-solutions, Eriřim Tarihi: 23.03.2023).

Word Bank Group: *The e-government handbook for developing countries: a project of InfoDev and the Center for Democracy and Technology*, 2002, (<https://documents1.worldbank.org/curated/en/317081468164642250/pdf/320450egovhandbook01public12002111114.pdf>, Eriřim Tarihi: 17.06.2023).

World Economic Forum: *The EU's Artificial Intelligence Act Explained*, 2023, (www.weforum.org/agenda/2023/03/the-european-union-s-ai-act-explained, Eriřim tarihi: 22.04.2023).

Wu, Y.: *Personal Data Protection in E-Government: Globalization or Glocalization? A Comparative Study Of The United States, Germany And China*, Yayınlanmamış Doktora Tezi, Michigan State University, 2010.

Yang, W./ Chuanshen, Q./ Bo,F.: *Do Institutional Pressures Increase Reactive Transparency of Government? Evidence From a Field Experiment*, Public Management Review 2022, s.1–20.

Yasar, K: *Definition Black Box AI*, (<https://www.techtarget.com/whatis/definition/black-box-AI>, Eriřim Tarihi: 23.05.2023).

Yenisey, F. /Nuhođlu, A.: *Ceza Muhakemesi Hukuku*, 9. Baskı, Ankara 2021.

Yılmaz, D./ Türkođlu, İ.: *Türkiye'de E-Devlet Uygulamalarının Bazı Yönetim Süreçlerine Etkisinin Örnek Projeler Bağlamında Deđerlendirilmesi*, Uluslararası Yönetim İktisat ve İşletme Dergisi 2010, C. 10, S. 22, s. 235-256.

Yılmaz, M.: *Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi*, Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 2009, C. XLIX, S. 1, s. 95-118.

Zakrzewska, M/ Ireneusz M.: *Using E-government Services and Ensuring the Protection of Sensitive Data in EU Member Countries*, Procedia Computer Science 2021, C. 192, s. 3457–3466.

Zillner, S./ Bretschneider, C./ Oberkamp, H./ Neurerer, S./ Munné, R./ Lippell, H., /Paradowski, D.: *Final version of Sector's Roadmap* (318062). 2014, (https://www.big-project.eu/sites/default/files/BIG_D2_4_2_FINAL_v0_851.pdf, Erişim Tarihi: 15.01.2023).

Zimmerman, A.: *New Knowledge From Old Data: The Role of Standarts in the Sharing and Reuse of Ecological Data*, Science, Technology&Human Values 2008, C. XXXIII, S. 5, s. 631-652.

Zins, C.: *Conceptual Approaches for Defining Data, Information, and Knowledge*, Journal Of The American Society for Information Science and Technology 2007, C. LVIII, S. 4, s. 479-493.