T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Mahmut Furkan BALABAN

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLENEN KİŞİSEL VERİLERİN KORUNMASI

Doktora Tezi
Kamu Hukuku Doktora Programı

Tez Danışmanı
Prof. Dr. Bülent KENT

Ankara 2023

T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Mahmut Furkan BALABAN
195456011

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLENEN KİŞİSEL VERİLERİN KORUNMASI

Doktora Tezi
Kamu Hukuku Doktora Programı

Tez Danışmanı
Prof. Dr. Bülent KENT

Ankara 2023

T.C.
ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ ONAYI

Enstitümüzün ……. Doktora Programı …… numaralı öğrencisi ……'nın hazırladığı "**……**" başlıklı tezi ile ilgili tez savunma sınavı, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri gereğince …./…./…. …… günü saat ...:…'da yapılmış, tezin onayına oy birliği/oy çokluğu ile karar verilmiştir.

Başkan **:** ……(unvanı-adı-soyadı-imza)

Jüri Üyesi **:** ……(unvanı-adı-soyadı-imza)
(Danışman)

Jüri Üyesi **:** ……(unvanı-adı-soyadı-imza)

Jüri Üyesi **:** ……(unvanı-adı-soyadı-imza)

Jüri Üyesi **:** ……(unvanı-adı-soyadı-imza)

ONAY:

Bu tezin kabulü, Enstitü Yönetim Kurulu'nun …../…../…….. tarih ve …….. sayılı Enstitü Yönetim Kurulu Kararı ile onaylanmıştır.

…...../...../.....

Doç. Dr. Murat BAYAR
Müdür

TEŞEKKÜR

Doktora sürecim boyunca danışmanım olarak çalışmalarıma yön veren ve desteğini her zaman hissettiğim Prof. Dr. Bülent KENT'e teşekkürlerimi ve saygılarımı sunarım. Tez çalışmam süresince desteğini esirgemeyen Prof. Dr. Ramazan ÇAĞLAYAN, Doç. Dr. Yasin SÖYLER, Dr. Öğr. Üyesi Adnan KÜÇÜK ve Dr. Öğr. Üyesi Merve Ayşegül KULULAR İBRAHİM hocalarıma teşekkür ederim.

Bu süreçte gösterdiği fedakarlık ve tez çalışmama verdiği katkılarıyla en büyük destekçim olan eşim Fatma Refia BALABAN'a şükranlarımı sunarım.

İÇİNDEKİLER

BÖLÜM 2

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLENMESİ İÇİN ABONEDEN ALINAN VE ELEKTRONİK HABERLEŞME HİZMETİNİN KULLANIMIYLA ORTAYA ÇIKAN KİŞİSEL VERİLER

BÖLÜM 3

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İMHA EDİLMESİNE KADAR GEÇEN SÜREÇ VE DEĞERLENDİRİLMESİ

ÖZET

Elektronik haberleşme sektöründe çok sayıda ve sürekli şekilde veri işlenmesi sebebiyle kişisel verilerin korunması konusu önem arz etmektedir. Aboneden alınan kişisel verilerin yanı sıra haberleşme hizmetlerinin kullanımından kaynaklanan kişisel veriler de ortaya çıkmaktadır. Veri sorumlusu olan elektronik haberleşme sektöründeki işletmecilerin faaliyetlerine ilişkin abonelerin kişisel verilerinin korunmasına yönelik hukuki düzenleme yapılması ihtiyacı geçmişten beri mevcuttur. Teknolojinin gelişmesiyle birlikte bu düzenlemelerin de güncellenme ihtiyacı doğmaktadır. Çalışmada özellikle elektronik haberleşme sektöründe kişisel verilerin korunması hakkında AB düzenlemeleri incelenmiştir. Söz konusu düzenlemelerin Türk hukukundaki yansımalarına yer verilmiştir. Unutulma hakkı ve büyük veri gibi kişisel verilerin korunması konusunda önemli olan kavramlar açıklanmıştır. Elektronik haberleşme sektöründeki terimler, kişisel verilerin korunması bağlamında değerlendirilmiştir. İşletmecilerin, haberleşme hizmetlerinin sunumu esnasında kişisel verilerin korunmasını öncelemesi gerekmektedir. Ayrıca elektronik haberleşme sektöründeki abonenin kimliğinin uzaktan doğrulanabilmesine yönelik gelişmeler ele alınarak; kişisel verilerin korunmasıyla ilgili uygulamadaki sorunlar analiz edilmiş ve çözüm önerileri getirilmiştir.

Anahtar Kelimeler: Elektronik haberleşme, kişisel verilerin korunması, kimlik doğrulama, çerezler, trafik ve konum verisi.

ABSTRACT

In the electronic communication sector, the protection of personal data is important because of the large number of continuous data processing. Besides the personal data received from the subscriber, personal data arising from the use of communication services also appear. The need for legal regulation to protect the personal data of the subscribers regarding the activities of the operators in the electronic communication sector, which is the data controller, has existed since the past. The need for updating these regulations arises with the development of technology. In the study, EU regulations on the protection of personal data, especially in the electronic communication sector, were examined. The reflections of these regulations in Turkish law are given. The important notions about the protection of personal data such as the right to be forgotten and big data were explained. The terms in the electronic communication sector have been evaluated in the context of personal data protection. Operators should prioritize the protection of personal data during the provision of communication services. In addition, the developments in remote verification of the identity of the subscriber in the electronic communications sector were discussed, and the problems related to the protection of personal data in practice were analyzed and solutions have been proposed.

Keywords: Electronic communication, protection of personal data, authentication, cookies, traffic and location data.

KISALTMALAR

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

ABD : Amerika Birleşik Devletleri

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AKN : Adil Kullanım Noktası

ASY : Abonelik Sözleşmeleri Yönetmeliği

A.Ş. : Anonim Şirket

AYM : Anayasa Mahkemesi

BM : Birleşmiş Milletler

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CAs : Certificate Authorities
(Sertifika Yetkilileri)

CB : Türkiye Cumhuriyeti Cumhurbaşkanlığı

CD : Compact Disc

CDR : Call Detail Records
(Arama Detay Kayıtları)

CLIR : Calling Line Identification Restriction
(Arayan Hat Kimlik Kısıtlaması)

CMK : Ceza Muhakemesi Kanunu

DDI : Direct Dial In

(Doğrudan Arama)

DID : Direct Inward Dialling

(Doğrudan Dahili Arama)

DSL : Digital Subscriber Line

(Dijital Abone Hattı)

E2EE : End-to-end Encryption

(Uçtan Uca Şifreleme)

EDPB : European Data Protection Board

(Avrupa Veri Koruma Kurulu)

EHK : Elektronik Haberleşme Kanunu

EHS : Elektronik Haberleşme Sektörü

EKDS : Elektronik Kimlik Doğrulama Sistemi

EPG : Etkin Piyasa Gücü

ETSI : European Telecommunications Standards Institute

(Avrupa Telekomünikasyon Standartları Enstitüsü)

GDPR : General Data Protection Regulation

(Genel Veri Koruma Tüzüğü)

GMPCS : Global Mobile Personal Communications By Satellite

(Küresel Mobil Kişisel İletişim Uydu)

GPS : Global Positioning System

(Küresel Konumlandırma Sistemi)

GSM : Global System for Mobile Communications

(Mobil Haberleşme İçin Küresel Sistem)

GVKT : Genel Veri Koruma Tüzüğü

HTTP : Hyper Text Transfer Protocol

(Hiper Metin Transfer Protokolü)

HTTPS : Hyper Text Transfer Protocol Secure

(Güvenli Hiper Metin Transfer Protokolü)

ICAO : International Civil Aviation Organisation

(Uluslararası Sivil Havacılık Örgütü)

ICO : Information Commissioner's Office

IMEI : International Mobile Equipment Identity

(Uluslararası Mobil Cihaz Kimliği)

IMSI : International Mobile Subscriber Identity

(Uluslararası Mobil Abone Kimliği)

IMT : International Mobile Telecommunications

(Uluslararası Mobil Telekomünikasyon)

IP : Internet Protocol Address

(İnternet Protokolü Adresi)

ISS : Internet Service Service

(İnternet Servis Sağlayıcı)

ITU : International Telecommunication Union

(Uluslararası Telekomünikasyon Birliği)

İYS : İleti Yönetim Sistemi

KDV : Katma Değer Vergisi

KEC : Kart Erişim Cihazı

KEP : Kayıtlı Elektronik Posta

KİK : Kamu İktisadi Kuruluşları

Kurum : Bilgi Teknolojileri ve İletişim Kurumu

KVK : Kişisel Verilerin Korunması

KVKK : Kişisel Verilerin Korunması Kanunu

MHz : Megahertz

MMS : Multimedia Messaging Service

(Mobil Çoklu Ortam Mesajlaşma Hizmeti)

MRZ : Machine Readable Zone

(Makine Tarafından Okunabilir Bölge)

MSISDN : Mobile Station Integrated Services Digital Network

(Mobil İstasyon Entegre Hizmetler Dijital Ağı)

NFC : Near Field Communication

(Yakın Alan İletişimi)

NVİ : Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü

NTS : Numara Taşıma Sistemi

OCSP : Online Certificate Status Protocol

(Çevrimiçi Sertifika Durumu Protokolü)

OECD : Organisation for Economic Co-operation and Development

(Ekonomik İşbirliği ve Kalkınma Örgütü)

OTT : Over the Top

PAdES-LTV : PAdES Long Term Validation

(PAdES Uzun Dönem Doğrulama)

PDF : Portable Document Format

(Taşınabilir Belge Biçimi)

RAFMET : Referans Kiralık Devre ve Referans Al-Sat Yöntemiyle ATM/FR/ME İnternet Toptan Satış Teklifleri

RAT : Referans Arabağlantı Teklifi

RFID : Radio Frequency Identification

(Radyo Frekansı ile Tanımlama)

RG : Resmi Gazete

SIM : Subscriber Identity Module

(Abone Kimlik Modülü)

SMS : Short Message Service

(Kısa Mesaj Servisi)

SSL : Secure Sockets Layer

(Güvenli Giriş Katmanı)

TBK : Türk Borçlar Kanunu

TCK : Türk Ceza Kanunu

TCKK : Türkiye Cumhuriyet Kimlik Kartı

TCPA : Telephone Consumer Protection Act

(Telefon Tüketici Koruma Yasası)

TİB : Telekomünikasyon İletişim Başkanlığı

TKHK : Tüketicinin Korunması Hakkında Kanun

TLS : Transport Layer Security

(Taşıma Katmanı Güvenliği)

TMK : Türk Medeni Kanunu

TS : Türk Standartları

TTK : Türk Ticaret Kanunu

TÜİK : Türkiye İstatistik Kurumu

UHH : Uydu Haberleşme Hizmeti

URL : Uniform Resource Locator

(Tek Tip Kaynak Bulucu)

VERBİS : Veri Sorumluları Sicil Bilgi Sistemi

VoIP : Voice Over Internet Protocol

(İnternet Üzerinden Ses İletimi Protokolü)

VPN : Virtual Private Network

(Sanal Özel Ağ)

YAPA : Yerel Ağın Paylaşıma Açılması

Wi-Fi : Wireless Fidelity

(Kablosuz Bağlantı Alanı)

GİRİŞ

İletişimi sağlayan cihazların taşınabilir olmasıyla birlikte uzakta olan kişiler arasındaki iletişim ihtiyacı daha kolay ve hızlı şekilde sağlanmaya başlamıştır. Başlarda kablo ile iletişim gerçekleştirilebilirken internet üzerinden ileti gönderilebilmesi fikriyle birlikte iletişim çok daha hızlı ve ucuz hale gelmiştir. İnternetin kullanımının yaygınlaşmasıyla haberleşmeyi sağlayan cihazların tek işlevi iletişim olmaktan çıkmış; bu cihazlar, hayatın her alanında kullanılmakta olan araçlar haline gelmiştir. Bu doğrultuda, dünyada haberleşme hizmetinden faydalanan abone sayısı çok hızlı bir şekilde artış göstermiş ve artmaya devam etmektedir. Abone sayısında yaşanan artış işletmeciler arası sunulan hizmette farklılık oluşturma ihtiyacı doğurmuştur. Böylece haberleşme hizmeti sunan işletmeciler, abonelerinin sayısını artırabilmek amacıyla temel iletişim ihtiyacını karşılamanın yanı sıra ek hizmetler sunarak sektörde öne çıkmaya çalışmaktadır.

Abone sayılarının artış göstermesiyle birlikte işletmeciler tarafından işlenmek durumunda kalınan kişisel veriler de giderek artmaya başlamıştır. Elektronik haberleşme sektöründeki düzenlemeler çerçevesinde uzun süreler veri saklamakla yükümlü olan işletmeciler açısından saklama süresince veriyi koruyabilmek büyük bir yük oluşturmaktadır. İşletmeciler, bu durumdan olumlu sonuçlar elde edebilmek ve ekonomik kazançlarını artırabilmek amacıyla; kullanıcıların verilerini yeniden değerlemeye tabi tutarak, hedefleme kriterleri çerçevesinde oluşturulan müşteri profillerine yönelik hizmet geliştirme düşüncesini ön plana çıkarmaya başlamıştır.

Elektronik haberleşme sektörünün aktörlerinden olan ve haberleşme hizmetlerini sunan işletmecilerin, kişisel verilerin korunması bakımından iki rolü bulunmaktadır. Bunlardan ilki, aboneye ait kişisel verilerin işletmeci tarafından işlenmesi sebebiyle işletmecinin veri sorumlusu olması, diğeri ise halihazırda kendi müşterilerinin kişisel verilerini işleyen abonelerin, haberleşme hizmetini kullanabilmek amacıyla müşterilerinin verilerini işletmeciye aktarması sebebiyle işletmecinin veri işleyen sıfatını haiz olmasıdır.

Bu çalışmada, veri yığınları haline gelen abonelerden kaynaklı kişisel verilerin korunması amacıyla işletmeci açısından ortaya çıkabilecek hukuki risklerin nasıl azaltılabileceği, ulusal ve uluslararası düzenlemelerle elektronik haberleşme sektörüne

getirilen yeniliklerin uygulamada yaşanan sorunlara ilişkin ihtiyacı karşılayıp karşılamadığı analiz edilmiştir. Elektronik haberleşme sektöründe işlenen kişisel verilerin çoğunluğunu oluşturan aboneden kaynaklı veya haberleşmenin gerçekleşmesiyle ortaya çıkan kişisel verilerin işlenmesi ve korunmasına yönelik ulusal ve uluslararası mevzuat incelemesi doğrultusunda bu sektördeki uygulamada yaşanan problemlere yönelik önerilerde bulunularak değerlendirmeler yapılmıştır.

Çalışmanın birinci bölümünde, elektronik haberleşme sektörüne ilişkin temel kavramlara ve ilkelere yer verilerek çalışmanın devamındaki bölümlerinde yer verilen konuların temelini oluşturan terimlerin incelenmesi hedeflenmiştir. Yapılan inceleme doğrultusunda, kavram ve ilkeler ile uygulamaya ilişkin farklılıklar hakkında BTK'nın vermiş olduğu kurul kararları değerlendirilmiştir.

Çalışmanın ikinci bölümünde, kişisel verilerin korunması hukuku açısından temel nitelikte olan açık rıza kavramının elektronik haberleşme sektörü açısından ne anlama geldiği, aboneden alınan açık rızaların nasıl olması gerektiği hususları, ulusal ve uluslararası mevzuat kapsamında tartışılmıştır. Bu doğrultuda, aboneye veya kullanıcıya aydınlatma metni sunulması hususunda Kişisel Verilerin Korunması Kurulu kararları ve Kişisel Verilerin Korunması Kurumu'nun düzenlemeleri incelenmiştir. Ayrıca diğer sektörlerde olduğu gibi elektronik haberleşme sektöründe de çokça kullanılan çerezler hakkında AB düzenlemeleri ve Türk hukuku çerçevesinde temel unsurlar irdelenmiştir. Çerezler vasıtasıyla davranışsal pazarlama yapılması konusu ele alınmıştır. Bununla birlikte, elektronik haberleşme sektöründeki AB düzenlemelerinin Türk hukukuna yansımalarına yer verilmiştir.

Elektronik haberleşme sektöründe işletmecinin abonesi olmak isteyen kişi tarafından, abonelik tesisinden önce veya abonelik tesisi esnasında abone olabilmek için birtakım kişisel veriler paylaşılmaktadır. Bu verilerin neler olduğuna ilişkin ayrıntılı bilgilere yer verilerek aboneliğin kurulabilmesi için kişinin kimliğinin doğrulanabilmesi amacıyla uygulamada işletmeciler tarafından istenilen bilgi ve belgelerin yanı sıra karşılaşılan zorlukların çözümüne ilişkin önerilerde bulunulmuştur. Bununla birlikte, aboneliğin yüz yüze veya uzaktan kimliğin doğrulanması suretiyle gerçekleştirilmesi esnasında işletmeciler tarafından alınan kişisel verilerde farklılıklar bulunmaktadır. Bu doğrultuda, konuya ilişkin değerlendirme yapılarak mevzuata göre gerçekleştirilmesi mümkün olan hususlar konusunda sektörde karşılaşılan problemler aktarılmıştır. Ayrıca

elektronik haberleşme sektöründe yeni sayılabilecek bir konu olan uzaktan kimlik doğrulamaya ilişkin açıklamalar yapılmıştır.

Elektronik haberleşme sektöründe, çok sayıda kişisel verinin işlendiği açıktır. Abonelik tesisi amacıyla aboneden alınan kişisel verilerin yanı sıra aboneliğin kullanımı ile ortaya çıkan kişisel veriler de bir o kadar fazladır. Bunların bir kısmı abone desen yapısıyla BTK'ye bilgi verme amacıyla işlenirken bir kısmı da abonenin hizmetleri kullanımıyla ortaya çıkan trafik ve konum verilerinden oluşmaktadır. Söz konusu verilerin işlenmesine dair değerlendirmeler yapılmıştır.

Haberleşmenin hayatın her alanında var olması sebebiyle, işlenen suçların ve şüphelilerin tespiti amacıyla yargı makamları ve kolluk kuvvetleri tarafından işletmecilerden bilgi talep edilebilmektedir. İşletmeciler tarafından bu taleplerin karşılanması da yine kişisel veri işleme faaliyeti kapsamında yer almaktadır. Bu taleplerin karşılanması sürecine ilişkin bilgi verilmiştir.

Her alanda olduğu gibi elektronik haberleşme sektöründe de veri sahipleri verileri hakkında bilgi almak veya imhasını talep etmek amacıyla veri sorumlusu olan işletmeciye başvurabilmektedir. Çalışmanın son bölümünde ilk olarak bu konuya ilişkin değerlendirmelerde bulunulmuştur.

İşletmeciler tarafından hukuka uygun şekilde verilerin toplanması kadar önemli olan bir diğer konu ise verilerin saklanmasıdır. AB düzenlemeleri ve kararları çerçevesinde verilerin saklanması konusu değerlendirildikten sonra; Türk hukukunda verilerin saklanmasına ve sürelerine ilişkin elektronik haberleşme mevzuatı içerisinde bulunan farklılıkların uygulamaya yansıması incelenmiştir.

Bilgi güvenliği konusunun elektronik haberleşme sektöründeki önemi belirtilerek işletmeci tarafından alınabilecek teknik ve idari tedbirlerin yanında AB hukukunda kendine önemli bir yer edinen unutulma hakkı, mahkeme kararları doğrultusunda ülkemize yansımalarıyla birlikte incelenmiştir.

Son olarak kişisel verilerin imhası konusunda hem AB düzenlemeleri hem de Türk hukuku içerisindeki kavramlar kıyaslanarak farklılıkları ortaya konmuştur. Kişisel veri elde edildikten sonra yalnızca saklama yükümlülüğüne katlanmak yerine imha edilene kadar profil oluşturma ve veri madenciliği vasıtasıyla veriler yeniden değerlendirilerek ekonomik bir kazanç elde etme hususunda elektronik haberleşme sektörüne ilişkin analizler yapılmıştır. Bu şekilde, çalışmanın son bölümünde aboneden alınan veya

hizmetin kullanımından kaynaklanan kişisel verilerin işletmeci tarafından elde edildikten sonra imhasına kadar geçen süreç değerlendirilmiştir.

BÖLÜM 1
ELEKTRONİK HABERLEŞME SEKTÖRÜNE İLİŞKİN TEMEL KAVRAM VE İLKELER

1. ELEKTRONİK HABERLEŞME SEKTÖRÜNE İLİŞKİN TEMEL KAVRAMLAR

1.1. ELEKTRONİK HABERLEŞME

1.1.1. Elektronik Haberleşme Kavramı

Haberleşmenin tarihsel olarak uğradığı değişiklikler karşısında teknoloji ile doğrudan ilişkili ve iç içe olduğu görülmektedir.[1] Haberleşmenin elektronik ortamda gerçekleşebileceği fikri, her geçen gün daha çok kabul görmüş ve telekomünikasyon kavramı ortaya çıkmıştır. Telekomünikasyon, eski Yunan dilinde uzak kelimesini karşılayan "tele" ve Latince paylaşmak anlamında kullanılan "kommunikasyon"un birleşiminden türemiştir.[2] "Tele" sözcüğü elektronik, elektromanyetik anlamlarında da kullanılarak "elektronik-elektromanyetik haberleşme" anlamına gelen telekomünikasyon kavramı ortaya çıkmıştır.[3] Genel olarak telekomünikasyon kavramı, bilginin uzun mesafelerde elektronik olarak iletilmesinin sağlanmasına karşılık gelir.[4] Uluslararası Telekomünikasyon Birliği'nin (International Telecommunication Union-ITU) yaptığı tanımda; tel, radyo, optik veya diğer elektromanyetik sistemlerle herhangi bir türde işaret, sinyal, yazı, görüntü ve ses iletimi telekomünikasyon olarak adlandırılır.[5] Bu doğrultuda, bir haberleşme eyleminin telekomünikasyon olarak adlandırılabilmesi için, nitelik unsuru

---

[1] Şerafettin Ekici, *Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)*, (İstanbul: Vedat Kitapçılık, 2006), 1.
[2] Bülent Kent, "Telekomünikasyon Sektöründe Evrensel Hizmet Kavramı," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 16, no.2 (2012): 170.
[3] Ekici, *Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)*, 3.
[4] Uchenna Jerome Orji, *International Telecommunications Law and Policy*, (Newcastle upon Tyne: Cambridge Scholars Publishing, 2018), 3.
[5] International Telecommunication Union, *Collection of The Basic Texts Adopted By The Plenipotentiary Conference*, (ITU Publication, 2019), 65, https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-PLEN-2019-PDF-E.pdf , Erişim Tarihi: 27 Şubat 2022.

denilen iletilecek verinin ses, görüntü, işaret ya da elektronik sinyallere dönüşebilen bir veri olması ve söz konusu verilerin sistem unsuru denilen kablo, optik, elektrik ya da manyetik sistemler ile iletilmesi gerekliliğini sağlaması mutlaktır. Dolayısıyla yaygın kullanımı olan telefon ve internet kullanımı telekomünikasyon terimine dahil edilebilirken, mektupla haberleşme ya da yüz yüze iletişim faaliyetleri telekomünikasyon kapsamında değerlendirilemez.[6]

Özetle, telekomünikasyonun esas rolü, iletişimi başlatarak alışveriş yapılan bilginin yorumlanması ve iletişim kuran insanlar ya da makinelerin depoladığı bilgilerin paylaşılabildiği bir ortam sağlamaktır.[7] Daha sonraları bu kavram, yerini elektronik haberleşme kavramına bırakmıştır.

2002/58/EC[8] sayılı Gizlilik ve Elektronik Haberleşme Direktifi'nin (Elektronik Haberleşme Direktifi) 2. maddesinde haberleşme, bilginin belirli sayıdaki taraflar arasında kamuya açık bir elektronik haberleşme hizmeti vasıtasıyla iletilmesi olarak tanımlanmıştır. Söz konusu hükmün devamında, haberleşmenin gerçekleştiği tarafların belirli veya belirlenebilir olması koşulu aranarak yayın şeklinde kaç kişiye ulaştığı belli olmayan bilgi paylaşımının haberleşme sayılamayacağına yer verilmiştir. Her ne kadar ilgili Direktif'te "communication" denilerek haberleşme tanımı yapıldığı düşünülse de tanımın içeriğine bakıldığında elektronik haberleşme hizmeti vasıtasıyla yapılan bir iletişimden bahsedildiği görülmekte olup aslında elektronik haberleşme teriminin tanımının yapıldığı anlaşılmaktadır.

Avrupa Komisyonu tarafından haberleşme altyapıları ve bununla ilgili hizmetlerin de dahil olduğu yeni düzenlemelere ilişkin 2002 yılında 2002/19/EC[9], 2002/20/EC[10] ve 2002/21/EC'den[11] oluşan mevzuat paketinin kabulüyle[12], Avrupa Birliği'nde neredeyse her sektörde olduğu gibi elektronik haberleşme sektöründe de devlete ait teşebbüsler veya tekel işletmeciler yoluyla faaliyetlerin sürdürülmesi yerine serbestleşme ile sektöre alternatif işletmeciler dahil olmaya başlamıştır. Yaşanan gelişmeler, üye devletlerin iç

---

[6] Ekici, *Türk Telekomünikasyon Hukuku*, 4-5.
[7] David G. Messerschmitt, "Telecommunications in the 21st Century," *University of California* (1996): 1, http://people.eecs.berkeley.edu/~messer/PAPERS/93/Japan1/Japan1.pdf , Erişim Tarihi: 27 Şubat 2022.
[8] Directive 2002/58/EC, *EUR-Lex*, Erişim Tarihi: 28 Şubat 2022.
[9] Directive 2002/19/EC, *EUR-Lex*, Erişim Tarihi: 28 Şubat 2022.
[10] Directive 2002/20/EC, *EUR-Lex*, Erişim Tarihi: 28 Şubat 2022.
[11] Directive 2002/21/EC, *EUR-Lex*, Erişim Tarihi: 28 Şubat 2022.
[12] BTK, AB Elektronik Haberleşme Düzenlemeleri, https://www.btk.gov.tr/ab-elektronik-haberlesme-duzenlemeleri , Erişim Tarihi: 28 Şubat 2022.

pazarlarını ve mevzuatlarını bu doğrultuda uyumlaştırmaları ihtiyacını doğurmuştur.[13] Modern haberleşme yapılarının faaliyete geçmesinin yalnızca telekomünikasyon sektörünü değil, ticari faaliyetleri ve genel olarak hayatın her alanındaki gelişmeleri etkileyeceği düşüncesi ile gelişmiş bir haberleşme altyapısı kurulması gayreti içerisinde bulunulmuştur.[14]

Avrupa Birliği'nde elektronik haberleşme sektöründe yaşanan gelişmeler doğrultusunda, ülkemiz de hem uygulama hem de mevzuatını uyumlaştırma sürecine girmiştir. 1982 Anayasası'nda[15] elektronik haberleşme ve telekomünikasyon kavramlarına doğrudan yer verilmemiştir. Anayasa'nın yalnızca 22. maddesinde, herkesin haberleşme özgürlüğünün bulunduğu ve bu kapsamda haberleşmenin gizlilik esasına dayandığı vurgulanmıştır.

5809 sayılı Elektronik Haberleşme Kanunu'nun (EHK) gerekçesinde belirtildiği üzere; iç hukukumuzda telekomünikasyona dair yapılan ilk düzenleme olan 406 sayılı Telgraf ve Telefon Kanunu'nda[16], diğer ülkelerdeki telekomünikasyon teknolojisinde yaşanan gelişmelere uyum sağlanabilmesi amacıyla zaman zaman çeşitli değişiklikler yapılmıştır. Bu doğrultuda, telekomünikasyon kavramına ilk olarak 1994 yılında yürürlüğe giren 4000 sayılı Kanun[17] ile yer verilmiştir.[18] 2000 yılında yayınlanan 4502 sayılı Kanun[19] ile çoğu telekomünikasyon hizmetlerinin tekel hakkı sona erdirilmiştir.[20] 2003 yılında ise ülkemizdeki ses ve altyapı tekeli tam anlamıyla sona erdirilerek serbestleşmeye gidilmiş ve sektöre yeni işletmeciler de dahil olmaya başlamıştır. 406 sayılı Kanun'da yapılan değişikliklerle elektronik haberleşme sektöründeki hızlı

---

[13] Liyang Hou, *Competition Law and Regulation of the EU Electronic Communications Sector A Comparative Legal Approach*, (Alphen aan den Rijn, Wolters Kluwer Law and Business, 2012), Chapter 1, 1; Christian Koenig, Ernst Roder, "Regulation of Telecommunications in the EU a Challenge for the Countries Acceding to the European Community," *European Business Law Review* 10, no.7/8 (1999): 333-334.

[14] Koenig, "Regulation of Telecommunications in the EU," 333.

[15] R.G. 9.11.1982, S.17863 (Mükerrer).

[16] R.G. 21.2.1924, S.59.

[17] R.G. 18.06.1994, S.21964. Söz konusu Kanun, *"Telgraf ve Telefon Kanununun Bir Maddesinin Değiştirilmesi ve Bu Kanuna Bazı Ek ve Geçici Maddeler Eklenmesine Dair Kanun"* adıyla yayımlanmıştır.

[18] 406 sayılı Kanun'un 1. maddesinde, telekomünikasyon faaliyetlerinin Türk Telekomünikasyon A.Ş. tarafından yürütüleceğinden bahsedilerek telekomünikasyon kavramına yer verilmiştir.

[19] R.G. 29.1.2020, S.23948. Belirtilen Kanun, *"Telgraf ve Telefon Kanunu, Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun, Telsiz Kanunu ve Posta, Telgraf ve Telefon İdaresinin Biriktirme ve Yardım Sandığı Hakkında Kanun ile Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin Eki Cetvellerde Değişiklik Yapılmasına Dair Kanun"* adıyla yayımlanmıştır.

[20] İlgili Kanun'un Geçici 3. maddesiyle Türk Telekomünikasyon A.Ş., 233 sayılı KHK ekinde bulunan Kamu İktisadi Kuruluşları (KİK) tablosundan çıkartılmıştır.

gelişmelere cevap verilemeyeceğinden ve Avrupa Birliği'ndeki uygulamalara entegre olabilmesi açısından telekomünikasyon yerine elektronik haberleşme terimine de yer verilen ve bu hususstaki hükümleri de barındıran yeni bir kanuna ihtiyaç duyulmuştur.[21] Bunun üzerine 2008 yılında 5809 sayılı EHK[22] yayımlanmıştır.

EHK'nın yayımlanmasıyla, elektronik haberleşme sektöründeki çeşitli yeniliklerin derlendiği temel nitelikte bir mevzuat ortaya çıkmıştır. Ayrıca ilgili kanun ile telekomünikasyon ifadesi, elektronik haberleşme olarak anılmaya başlanmıştır.[23]

Elektronik haberleşme kavramı, 5809 sayılı EHK'nın 3/1-(h) maddesinde, *"elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını, ... ifade eder"*. Diğer bir deyişle elektronik haberleşme, birbiriyle duyu organlarıyla haberleşemeyecek kadar uzakta olan gönderen ve alan konumundakilerin iletilerinin elektronik işaretlere çevrilerek taşınmasıdır.

1.1.2. Elektronik Haberleşmenin Kamu Hizmeti Niteliği

Kamu hizmeti, toplumun devamlı ve genel nitelikte olan temel ihtiyaçlarının kamu tüzel kişileri veya bunlar tarafından denetlenen özel teşebbüsler vasıtasıyla karşılanmasıdır.[24] Kamu hizmeti kavramı, organik anlamda kamu hizmeti ve maddi anlamda kamu hizmeti olarak iki farklı anlamda kullanılmaktadır.[25] Organik anlamda kamu hizmeti temel olarak kamu tüzel kişisi tarafından kamu hizmeti görmek amacıyla tahsis edilen kişi ve diğer vasıtaların tamamı şeklinde tanımlanabilmektedir. Anayasa'nın 70. maddesinde yer verilen *"Her Türk, kamu hizmetine girme hakkına sahiptir"* hükmünde belirtilen kamu hizmeti organik anlamda kullanılmıştır.[26] Maddi anlamda kamu hizmeti ise sadece hizmetin türüne bakılarak nitelendirme yapıldığında toplumun

---

[21] EHK Tasarısı ile Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu Raporu (1/1120), https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss1057m.htm , Erişim Tarihi: 1 Mart 2022.
[22] R.G. 10.11.2008, S. 27050 (Mükerrer).
[23] Şerafettin Ekici, *Bilişim ve Teknoloji Hukuku* (Ankara: Seçkin Yayıncılık, 2022), 218.
[24] Ramazan Çağlayan, *İdare Hukuku Dersleri* (Ankara: Adalet Yayınevi, 2021), 243; Mesut Erol, "Kamu Hizmetlerinin Görülüş Usullerinden Ruhsat (Lisans, İdari İzin, Yetkilendirme) Yöntemi ve Düzenleyici ve Denetleyici Kurumların Lisans Konusundaki Yetkilerinin Danıştay Kararları Çerçevesinde Değerlendirilmesi," *Türkiye Barolar Birliği Dergisi*, no.90 (2010): 349.
[25] Çağlayan, *İdare Hukuku Dersleri*, 241-242.
[26] Ender Ethem Atay, *İdare Hukuku* (Ankara: Seçkin Yayıncılık, 2022), 312.

ihtiyacının giderilmesine yönelik olan faaliyetleri karşılayan hizmetlerdir.[27] Anayasa'nın 47. maddesinde, kamu yararı olması halinde kamu niteliğini haiz özel teşebbüslerin devletleştirilebileceği hükmüne yer verilmiştir. Burada kamu hizmeti faaliyet anlamına gelecek şekilde kullanılmıştır.[28] Özetle, bir faaliyetin kamu hizmeti olarak adlandırılabilmesi için hizmetin amacının ne olduğu ve bu hizmeti görmeyi üstlenen organın niteliğinin önemli olduğu görülmektedir.[29] Her faaliyet kamu hizmeti niteliği taşıyabilmekte olup bunun için temel unsur, siyasi organların ilgili faaliyeti kamu hizmeti olarak değerlendirmesidir.[30] Dolayısıyla bir faaliyetin kamu hizmeti olarak adlandırılabilmesi için organik unsur olan kamu tüzel kişisi veya onun yetkilendirdiği özel hukuk tüzel kişi tarafından görülmesi ve maddi unsur olarak adlandırılan faaliyetin, toplumun bir ihtiyacını karşılayan nitelikte olması gerekmektedir.[31]

5809 sayılı EHK'da, elektronik haberleşme hizmetinin kamu hizmeti niteliği taşıdığına ilişkin çıkarımlar yapmaya elverişli bazı hükümler mevcuttur. Buna göre, BTK'nın görev ve yetkilerine yer verilen 6/1-(ş) maddesinde Kurum, kamu hizmeti olan elektronik haberleşme hizmetlerinin gerektiği şekilde yürütülebilmesi için mevzuatta yer alan önlemleri almakla yükümlü kılınmıştır. Ayrıca 27. maddede, elektronik haberleşme şebeke ve ekipmanlarının, işletmecinin geçiş hakkını kullanacağı güzergah veya taşınmaz üzerinde bulunan su kanalı veya elektronik haberleşme şebekesi gibi önceden kurulu olan kamu hizmeti alt yapısını olumsuz etkilemeyecek şekilde kurulması gerektiğine değinilerek elektronik haberleşme şebekeleri de kamu hizmeti altyapısından sayılmıştır. Keza aynı Kanun'un 29. maddesinde, yetkilendirmenin devredilmesi durumunda, kamu hizmeti niteliğindeki elektronik haberleşmenin kesintiye uğramaması için geçiş hakkı anlaşmalarının aynı koşullarda geçerli olacağından bahsedilmiştir. Son olarak, BTK'nın yetkisi ve idari yaptırımlara ilişkin hükümlerin yer aldığı 60. maddede de Kurum yine kamu hizmetlerinin gereken şekilde devamı için önlemler almakla yetkilendirilmiştir.

Diğer yandan kamu hizmeti, konularına göre de farklı bir ayrıma tabi tutulmaktadır. Bu çerçevede bilimsel kamu hizmeti, sosyal kamu hizmeti, idari kamu

---

[27] Halil Kalabalık, *İdare Hukuku Dersleri II* (Ankara: Seçkin Yayıncılık, 2021), 307-308; Çağlayan, *İdare Hukuku Dersleri*, 241.
[28] Atay, *İdare Hukuku,* 312.
[29] Oğuz Sancakdar, Lale Burcu Önüt, Eser Us Doğan, Mine Kasapoğlu Turhan, Serkan Seyhan, *İdare Hukuku Teorik Çalışma Kitabı* (Ankara: Seçkin Yayıncılık, 2021), 558; Kalabalık, *İdare Hukuku Dersleri II*, 308.
[30] Kalabalık, *İdare Hukuku Dersleri II*, 309.
[31] Kalabalık, *İdare Hukuku Dersleri II*, 309-310.

hizmeti gibi çeşitli şekillerde içerdiği konuya göre farklılık göstermektedir.[32] Bunun dışında, bazı kamu hizmeti türlerinin özel sektörde faaliyet gösteren işletmecilere gördürülmesi hususunda ise evrensel hizmet kavramı ortaya çıkmıştır. İlk olarak 406 sayılı Kanun'da asgari hizmet olarak ifade edilen bu kavram, ilgili Kanun'un 1. maddesinde ankesörlü telefon ve acil telekomünikasyon hizmetleri ve telefon hizmetleri, asgari evrensel hizmet türü olarak belirtilmiştir. Daha sonra 5369 sayılı Evrensel Hizmet Kanunu[33] ile 406 sayılı Kanun'da değişiklik yapılarak asgari hizmet ifadesi yerine evrensel hizmet kavramı kullanılmaya başlanmıştır. Evrensel hizmet, 5369 sayılı Kanun'un 2. maddesinde, internet dahil olmak üzere elektronik haberleşme hizmetleri, herkesin erişilebildiği ve belirlenen standartlar çerçevesinde makul bir bedel ile sunulan hizmetler olarak tanımlanmaktadır.[34] Söz konusu tanım incelendiğinde; evrensel hizmet kavramının herkes tarafından erişilebilirlik, makul bedel karşılığında sunulması ve önceden belirlenmiş kalitede olması şeklinde üç temel unsuru barındırdığı görülmektedir. Bu unsurların arasında öncelik sırası bulunmamakla birlikte asgari hizmet düzeyi olarak adlandırıldığı söylenebilir.[35]

1.1.3. Elektronik Haberleşme Hizmetinin Özel Hukuk Tüzel Kişileri Tarafından Görülmesi

Kamu hizmetinin devletin kendisi tarafından görülmesinin yanı sıra özel kişilere gördürülmesi de mümkündür. Fakat özel hukuk tüzel kişileri tarafından kamu hizmetinin görülebilmesi için idare tarafından verilen yetkinin hukuki bir zemine dayanması gerekmektedir. Özel hukuk tüzel kişisi, bir kanunla görevlendirilme, idare tarafından yetki verilmesi olarak adlandırılan ruhsat usulü şeklinde veya kanunun belirlediği sınırlar çerçevesinde idare ve özel hukuk tüzel kişisi arasında düzenlenen bir sözleşme ile kamu hizmetini yerine getirebilmektedir.[36]

---

[32] Aytuğ Altın, "Kamu Hizmeti Anlayışında Değişim," *Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (2013): 105.
[33] R.G. 25.6.2005, S. 25856.
[34] Bahtiyar Akyılmaz, Murat Sezginer, Cemil Kaya, *Türk İdare Hukuku* (Ankara, Savaş Yayınevi, 2021), 572-574.
[35] Kent, "Evrensel Hizmet Kavramı," 183.
[36] Akyılmaz, *Türk İdare Hukuku*, 575; Çağlayan, *İdare Hukuku Dersleri*, 252; Erol, "Kamu Hizmetlerinin Görülüş Usullerinden Ruhsat," 350-351; Kalabalık, *İdare Hukuku Dersleri II*, 309.

Kamu hizmetlerinin emanet usulü ile idare tarafından yerine getirilebilirken özel hukuk tüzel kişileri tarafından müşterek emanet, iltizam, ruhsat ve imtiyaz usulü ile görülebilmektedir.[37]

3996 sayılı Bazı Yatırım ve Hizmetlerin Yap-İşlet-Devret Modeli Çerçevesinde Yaptırılması Hakkında Kanun'un[38] kapsamına yer verilen 2. maddesinde haberleşme hizmetinin, yap-işlet-devret modeli çerçevesinde, diğer bir ifadeyle özel hukuk sözleşmesiyle görülebileceği hüküm altına alınmıştır. Fakat 4502 sayılı Kanun'un 2. maddesiyle 406 sayılı Kanun'un değiştirilen ve daha sonra mülga olan 2. maddesinde belirtildiği üzere, telekomünikasyon hizmetinin görülebilmesi için özel hukuk tüzel kişisi ile Bakanlık arasında imzalanmış olan görev veya imtiyaz sözleşmesi yahut Bakanlığın vermiş olduğu genel izin veya ruhsat bulunması gerektiği hüküm altına alınmıştır. 4502 sayılı Kanun, 3996 sayılı Kanun'a nazaran daha özel nitelikte olduğundan ve sonraki kanun olması nedeniyle, telekomünikasyon hizmetinin niteliği bakımından bu kanunun nazara alınması gerekmektedir. Böylece telekomünikasyon hizmetlerinin yap-işlet-devret gibi özel hukuka tabi işlemlerle gerçekleştirilebilmesinin önü kapatılarak ilgili hizmetin açıkça kamu hizmeti olduğunun altı çizilmiştir.[39]

Elektronik haberleşme hizmetlerinin özel hukuk tüzel kişileri tarafından görülebildiği, 5809 sayılı EHK'nın 8. maddesinde yer alan bu kişilerin yetkilendirilmesi suretiyle hizmetin sunulabileceğine ilişkin hükümden anlaşılmaktadır.

EHK'nın yürürlüğe girmesiyle çoğu maddesi mülga olan 406 sayılı Kanun'un elektronik haberleşme hizmetinin görülme şekillerine yer verilen 2. maddesi de mülga olmuştur. Bununla birlikte, EHK'nın Geçici 2. maddesine göre, 5809 sayılı Kanun yürürlüğe girmeden önce ruhsat veya genel izin ile yetkilendirilen işletmeciler yetkilendirildikleri süreyle sınırlı olmak üzere kullanım hakkına sahip olmakta ve imtiyaz sözleşmeleri geçerliliğini korumaktadır.

EHK'daki bahsi geçen hükümlerden anlaşılacağı üzere; kamu hizmeti olan elektronik haberleşme hizmeti, yetkilendirmeyle özel hukuk tüzel kişilerine gördürülmektedir. Bu sebeple çalışmada yalnızca ruhsat usulüne yer verilecektir.

---

[37] Çağlayan, *İdare Hukuku Dersleri*, 252-257.
[38] R.G. 13.06.1994, S. 21959.
[39] Ali Ulusoy, "Telekomünikasyon Alanındaki Son Yasal Düzenlemeler ve Uygulamaların Değerlendirilmesi," Rekabet Kurumu Perşembe Konferansları, 58-60, https://www.rekabet.gov.tr/Dosya/persembe-konferanslari-yayinlari/perskonfyyn46.pdf , Erişim Tarihi: 1 Mart 2022.

Tekel niteliğinde olmayan kamu hizmetinin özel hukuk tüzel kişisine gördürülmesi olarak adlandırılan ruhsat usulü, idare ile özel hukuk tüzel kişisi arasında herhangi bir sözleşme olmadan idarenin tek taraflı iradesiyle tesis etmiş olduğu idari işlem neticesinde özel hukuk tüzel kişisine verilen ruhsat veya lisans ile kamu hizmetinin görülmesi olarak tanımlanmaktadır.[40] Ruhsat, lisans, izin veya yetkilendirme olarak da anılan bu yöntem her sektörde farklı şekilde tanımlanmasına rağmen genel olarak idare tarafından kamu hizmetinin özel hukuk tüzel kişisi tarafından görülmesine izin verilmesi anlamını taşımaktadır. Örneğin, 6446 sayılı Elektrik Piyasası Kanunu'nun[41] 3/1-(t) maddesinde lisans, ilgili Kanun uyarınca tüzel kişilere piyasada faaliyet gösterebilmeleri için verilen izin olarak tanımlanmıştır. 5809 sayılı EHK'da ise izin kavramı yetkilendirme olarak düzenlenerek yetkilendirme, ilgili Kanun'un 3/1-(ccc) maddesinde elektronik haberleşme hizmeti sunabilmek veya şebeke sağlamaları için şirketlere belirli hak ve yükümlülüklerin verilmesi şeklinde ifade edilmiştir.[42]

Ruhsat usulü, virtüel kamu hizmetlerinin görülmesi için kullanılan usullerden biridir. Organik anlamda kamu hizmeti olmayan fakat haberleşme, ulaşım gibi sürekli şekilde görülmesi gereken ve toplumun zorunlu nitelikteki ihtiyaçlarından olan ve genellikle özel hukuk tüzel kişilerine bu konuda lisans verilerek yerine getirilen kamu hizmetleri virtüel-fonksiyonel kamu hizmetleri olarak adlandırılmaktadır. Bu tür kamu hizmetlerinde idare, özel hukuk tüzel kişisini denetlemenin yanı sıra faaliyetin içeriğini de kendisi düzenlemektedir.[43]

5809 sayılı EHK'nın 8. maddesi uyarınca, şirketler ancak BTK tarafından yetkilendirilmeleri halinde hizmet verebilmektedir. Bununla birlikte, EHK'nın 6/1-(f) maddesindeki bazı elektronik haberleşme hizmetlerinin planlama ve tahsisinin BTK tarafından yapılmasına ilişkin hüküm gibi çeşitli hükümlerden elektronik haberleşme hizmetlerinin de virtüel kamu hizmeti olduğu anlaşılmaktadır.

1.1.4. Elektronik Haberleşme Kavramının Kişisel Verilerle İlişkisi

Elektronik haberleşmenin yaygınlaşmasından önce iletişimin genellikle iki kişi arasında olması sebebiyle gizliliğin daha kolay sağlandığı söylenebilirdi. Fakat elektronik

[40] Akyılmaz, *Türk İdare Hukuku*, 577.
[41] R.G. 30.03.2013, S. 28603.
[42] Erol, "Kamu Hizmetlerinin Görülüş Usullerinden Ruhsat," 352.
[43] Akyılmaz, *Türk İdare Hukuku*, 577; Kalabalık, *İdare Hukuku Dersleri II*, 322.

haberleşmenin getirdiği tek bir tuşla birden fazla kişiye ulaşabilme ve iletişime geçebilme imkanı, bilginin kolay ve hızlı bir şekilde işlenmesine yol açmıştır. Bu sebeple de kişisel veri,[44] elektronik ortamlarla veri aktarımı ve veri güvenliği konularına duyulan hassasiyet her geçen gün artmaktadır.

Elektronik haberleşme sektöründe korunması gereken kişisel verilere ilişkin Anayasa'nın 22. maddesinde haberleşmenin engellenemeyeceği ve gizliliğinin sağlanması gerektiğini belirten hüküm uygulama alanı bulmaktadır. Bireyin haberleşme verilerinin gizliliğinin esas olması kapsamında, Anayasa'nın "Özel Hayatın Gizliliği" başlıklı 20/3 madde hükmü de elektronik haberleşme sektöründe kişisel verilerin korunması bakımından önem teşkil etmektedir. Buna göre kişiler, kişisel verilerinin korunmasını talep etme, işlenen kişisel verileriyle ilgili bilgilendirilme ve bilgi talep etme, işlenen kişisel verilerinin silinmesini veya yanlışsa düzeltilmesini talep etme, kişisel verilerin işlenmeden önce bildirilen amaçlara uygun işlenip işlenmediğini öğrenme haklarına sahip olmanın yanı sıra kişisel verilerin işlenebilmesi için kişinin açık rızası aranmakta olup; ancak kanunda öngörülen hallerde açık rıza aranmaksızın kişisel verilerin işlenebileceği vurgulanmıştır.

Elektronik haberleşme sektöründe de abonelerin kişisel verilerinin işlenmesi nedeniyle veri sorumlusu[45] sıfatını haiz olan işletmeciler, ilgili kişilerin[46] Anayasa'da bahsi geçen hükümdeki hakları doğrultusunda yükümlülüklerini yerine getirirken genel nitelikteki 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)[47] ve elektronik haberleşme mevzuatında bulunan özel nitelikli hükümler çerçevesinde faaliyetlerini yürütmektedir.

[44] 6698 sayılı KVKK'nın 3/1-(d) maddesinde, kişisel veri, *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak adlandırılmıştır.
[45] Veri sorumlusu, 6698 sayılı Kanun'un 3/1-(ı) maddesine göre, *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak tanımlanmıştır.
[46] 6698 sayılı Kanun'un 3/1-(ç) maddesinde, ilgili kişinin, *"kişisel verisi işlenen gerçek kişi"* olduğu ifade edilmiştir.
[47] R.G. 7.4.1016, S. 29677.

1.2. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLETMECİ VE YETKİLENDİRİLMESİ

1.2.1. İşletmeci Tanımı

5809 sayılı EHK'nın 3/1-(z) maddesinde işletmeci kavramı, *"Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirket"* şeklinde tanımlanmıştır. Aynı tanıma, Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nin[48] (Tüketici Hakları Yönetmeliği) 4/1-(d) maddesinde de yer verilmiştir.

BTK mevzuatının yanı sıra tüketicinin korunması mevzuatına göre işletmeciyi tanımlamak gerektiğinde; elektronik haberleşme sektöründeki işletmecilerin hizmet sundukları şahsın gerçek kişi olması halinde Tüketicinin Korunması Hakkında Kanun (TKHK)[49] ve ilgili yönetmeliği olan Abonelik Sözleşmeleri Yönetmeliği (ASY)[50] hükümlerinin de uygulama alanı bulacağı aşikardır. ASY'nin 2. maddesinde ilgili Yönetmeliğin kapsamının, tüketicilerin belirli olan mal ya da hizmetleri devamlı şekilde ya da belirli periyotlarla almasını sağlayan abonelik sözleşmeleri olduğu belirtilmektedir. Söz konusu hükmün 2. fıkrasından ise ASY'nin tüm hükümlerinin elektronik haberleşme sektöründeki abonelik sözleşmelerine uygulanabileceği anlaşılmaktadır. Ayrıca elektronik haberleşme sektöründeki işletmecinin sunduğu hizmet ve bu hizmetin sunumu için mal temini faaliyetleri düşünüldüğünde, ASY'nin 4/1-(ğ) maddesinde ifade edilen sağlayıcı[51] ile yine aynı hükmün (h) bendinde yer alan satıcı[52] tanımlarının faaliyetin türüne göre değişkenlik göstererek uygulanabilir olduğu görülebilecektir.

Bu çalışmada, genel olarak elektronik haberleşme mevzuatı çerçevesinde işletmeci kavramı incelenecektir. EHK ve Tüketici Hakları Yönetmeliği'nde yapılan işletmeci tanımına göre elektronik haberleşme sektöründe faaliyet gösteren bir işletmeci olabilmenin ilk şartı şirket tüzel kişiliğini haiz olmak, ikinci şartı ise BTK tarafından yetkilendirilmiş olmaktır.

---

[48] R.G. 28.10.2017, S. 30224.
[49] R.G. 28.11.2013, S. 28835.
[50] R.G. 24.01.2015, S. 29246.
[51] ASY'nin 4/1-(ğ) maddesinde sağlayıcı, *"Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki amaçlarla tüketiciye hizmet sunan ya da hizmet sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişiyi,"* tanımlamaktadır.
[52] ASY'nin 4/1-(h) maddesinde satıcı, *"Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki amaçlarla tüketiciye mal sunan ya da mal sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişiyi,"* ifade etmektedir.

1.2.2. İşletmecinin Şirket Olması Şartı

EHK'ya göre işletmeci olabilmenin ilk şartı şirket niteliğini haiz olmak, ikinci şartı ise Kurum tarafından yetkilendirilmektir. Dolayısıyla ilgili hüküm uyarınca, gerçek kişiler yetkilendirilememekte yalnızca tüzel kişiler yetkilendirilebilmektedir.

İşletmecinin şirket olması ve bu şirketlerin taşıması gereken özellikler ise Yetkilendirme Yönetmeliği'nin 7/1 maddesinde yedi madde halinde sıralanmıştır.

1.2.2.1. Türk Hukukuna Göre Kurulma Şartı

Yetkilendirme Yönetmeliği'nin 7/1-(a) maddesi uyarınca, yetkilendirilerek elektronik haberleşme hizmeti sunmak isteyen şirketler Türkiye Cumhuriyeti kanunlarına göre kurulmalıdır. Diğer bir deyişle, yurtdışı menşeili elektronik haberleşme şirketlerinin Türkiye'de hizmet sunabilmeleri için Türkiye'de ayrıca bir şirket kurmaları gerekmektedir. Ayrıca yetkilendirilen işletmeci yalnızca yetkilendirildiği faaliyeti yerine getirebilecek, yetkilendirildiği konu dışında hizmetleri yerine getiremeyecektir.[53] Yetkilendirme Yönetmeliği'nin 7/1-(a) maddesinde bahsi geçen bir diğer husus ise işletmeci olmak isteyen şirketlerin sermaye şirketleri olan anonim ve limited şirket olması gerekliliğidir. Böylece şahıs şirketleri olan adi şirket, kollektif şirket ve adi komandit şirketlerin sektöre girişleri engellenmiştir. Kamu hizmeti niteliğinde olan elektronik haberleşme hizmetinin sunumu, şahıslardan çok sermayenin ön planda olduğu şirketler ile sağlanmak istenmiştir. Şahıs şirketlerinde şirket sahibi kişinin ölümü gibi durumlar sebebiyle şirketin de tüzel kişiliği sona ereceğinden, Anayasa'nın 22. maddesinde belirtilen haberleşmenin devamlılığı ilkesi gereğince elektronik haberleşme hizmetinin sunumuna devam edilebilmesi için şahsa değil sermayeye dayalı şirketler ile bu hizmetin sunumu şartı getirildiği anlaşılmaktadır.

1.2.2.2. Esas Sözleşmede Elektronik Haberleşme Konusunun Bulunması Şartı

İşletmeci olacak şirketlere ilişkin Yetkilendirme Yönetmeliği'nde getirilen ikinci şart, Ticaret Sicil Gazetesinde şirketin esas sözleşmesindeki faaliyet konusunda

[53] Konuya ilişkin 16.05.2017 tarih ve 2017/DK-YED/163 sayılı BTK Kurul Kararı ile, Yetkilendirme Yönetmeliği'ne aykırı olarak yetkilendirmesinin kapsamı haricinde hizmet veren işletmeci hakkında idari para cezası verilmeden önce ilgili şirketin uyarılmasına karar verilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/yetkisiz-hizmet-sunumu-sazak-haberlesme.pdf , Erişim Tarihi: 2 Mart 2022.

"elektronik haberleşme hizmeti/telekomünikasyon hizmeti sunulması ve/veya şebekesi veya altyapısı kurulup işletilmesi" hususuna ya da talep edilen yetkilendirmeye konu olan hizmetin adına yer verilmesi gerekmektedir. Böylelikle işletmeci olacak şirketin faaliyet alanı kısıtlanmıştır.

1.2.2.3. Hisse Sahiplerinin Belirli Suçlardan Mahkumiyetinin Bulunmaması Şartı

İşletmeci olacak şirketlere getirilen üçüncü şart ise işletmeci olacak şirketin hisse sahiplerinin 5237 sayılı Türk Ceza Kanunu'nda[54] yer verilen bilişim suçlarından, devletin güvenliğine ve anayasal düzene karşı suçlardan hürriyeti bağlayıcı ceza almamış, taksirli suçlar dışında beş seneden çok hapis cezasının alınmamış olması ya da dolandırıcılık ve benzeri yüz kızartıcı suçlardan veya 5809 sayılı EHK'nın 63. maddesinin 1. ve 2. fıkraları[55] kapsamında sayılan suçlardan hüküm giymemiş olmasıdır. Yine aynı Yönetmeliğin 19/1-(c) maddesinde hisse devri konusunda işletmecilere getirilmiş olan yüzde on ve üstündeki hisse devri, edinimi ve hareketlerinden önce BTK'dan izin alma yükümlülüğünde de görülebileceği üzere; haberleşmenin denetlenmesi gereken sektörlerin başında gelmesi sebebiyle Kurum, yüzde on ve üzeri hisseye sahip kişilerin sektöre girişlerini takip etmekte ve bahsi geçen hallerden biri dahi olsa şirket kuruluşu veya hisse devri aşamasında onay vermemektedir. Önceden yetkilendirilmiş bir işletmecinin bahsi geçen durumda olan bir kişiye Kurum'dan onay almadan hisse devri halinde ise Kurum, idari para cezasının yanı sıra hisselerin eski hale getirilmesini isteme veya işletmecinin lisansını iptal etme yoluna gidebilmektedir.[56]

---

[54] R.G. 12.10.2004, S. 25611.

[55] 5809 sayılı EHK'nın 63. maddesinde; aynı Kanun'un 9. maddesinde bahsi geçen BTK'ya bildirimde bulunarak veya kullanım hakkı elde ederek yetkilendirilen işletmeciler tarafından sunulabilen elektronik haberleşme hizmetlerini yetkilendirilmeden sunanlar hakkında adli para cezasına hükmedilmesi halinden söz edilmektedir.

[56] 24.03.2020 tarih ve 2020/İK-YED/085 sayılı BTK Kurul Kararı ile, Yetkilendirme Yönetmeliği'nin 19/1-c maddesinin ihlal edilmesi nedeniyle *"1. Kurumumuzdan izin almadan, %66,6 oranında hisse devri işlemi gerçekleştirmesi nedeni ile … hakkında; … idari para cezası uygulanması,*
2. Kurumumuzdan izin almadan, … yaklaşık %33,3 oranında hisse devri işlemi gerçekleştirmesi nedeni ile … hakkında; … idari para cezası uygulanması,
3. İşbu Kurul Kararı'nın tebliğ tarihinden itibaren 30 gün içinde; …'nin %66,6 oranında hissedarı olan …'a ait ortaklık oranının %5'in altına düşürülmesi ve yeni ortaklık yapısı ile birlikte gerçekleştirilen işlemin ivedilikle Kurumumuza bildirilmesi, hususlarına karar verilmiştir." https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-izinsiz-hisse-devri-ve-mevzuata-aykiri-islemler-lodosnet/85-2020-web.pdf , Erişim Tarihi: 3 Mart 2022.

1.2.2.4. Ödenmiş Sermayede Asgari Miktar Şartı

Yetkilendirilecek şirkette aranan dördüncü şart, ödenmiş olan sermayenin minimum BTK'nın belirlediği asgari tutar kadar olmasıdır. Bu tutar, BTK Yetkilendirme Dairesi Başkanlığı tarafından hazırlanan yetkilendirme yönetmeliği değişikliği ile gündeme getirilerek 31 Mart 2016 tarihli BTK kurul kararının 8. maddesiyle söz konusu asgari tutar, Ortak Kullanımlı Telsiz Hizmeti'ne yönelik yetkilendirme için asgari 250.000-TL, bildirimle ya da kullanım hakkı yoluyla yetkilendirme için asgari 1.000.000-TL olarak belirlenmiştir.[57]

5809 sayılı EHK'da işletmeci tanımlanırken *"işleten şirket"* ifadesine yer verilerek işletmecinin sermaye şirketi olması şartı aranmıyor gibi görünse de Yetkilendirme Yönetmeliği'nin 7/1-(ç) maddesinde ödenmiş sermayenin Kurum'un belirlediği tutar kadar olması gerektiğinden bahsedilerek aslında işletmecinin sermaye şirketi olması gerektiği anlaşılmaktadır.

1.2.2.5. Bilgi ve Belge Sunma Şartı

İşletmeci olacak şirketler için öngörülen beşinci şart, şirketin hizmet sunduğu işyeri ortamında çalışanların yeterliliğine kadar pek çok konuda Kurum'a bildirim veya kullanım hakkı başvuru formu vasıtasıyla bilgi verilmesi gerekliliğidir. İlgili başvuru formunda,[58] şirketin Yetkilendirme Yönetmeliği'nin 7/1 maddesinde belirtilen şartları taşıdığına ilişkin taahhüt vermesi ve şirket ve yetkilisine ilişkin birtakım iletişim bilgileri ve ödenmiş sermaye ve benzeri konularda bilgi ve belge sunulması talep edilmektedir. 16 Mart 2021 tarihindeki BTK Kurul Kararı'nın 5. maddesiyle işletmecilerin en az bir tane lisans mezunu personeliyle birlikte yine Kurum tarafından belirlenecek nitelik ve görevdeki personelinin Kurum'un belirlediği usul ve esaslar çerçevesinde sertifika alması gerektiğine karar verilmiştir. Bununla birlikte, aynı kararın ekinde yayımlanan ve bu kararla onaylanan Bildirim Hakkı Formu Taslağı ve Kullanım Hakkı Başvuru Formu Taslağı'nda da işletmecinin tam zamanlı çalışanlardan en az iki tanesinin lisans

[57] 31.03.2016 tarih ve 2016/DK-YED/195 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/yetkilendirme-yonetmeligi-degisikligi.pdf , Erişim Tarihi: 3 Mart 2022.

[58] Yetkilendirme İçin Başvuru Adımları, https://www.btk.gov.tr/yetkilendirme-icin-basvuru-adimlari Erişim Tarihi: 3 Mart 2022.

düzeyinde eğitim görmüş olması ve şirketin işyerine ilişkin ise asgari elli metrekare kullanım alanına sahip olduğunu ispatlayıcı belgenin sunulması şartı aranmaktadır.[59]

1.2.2.6. Adli Sürecin Bulunmaması Şartı

Yetkilendirilecek olan şirkette bulunması gereken altıncı husus, 5809 sayılı EHK'nın 9. maddesine aykırı şekilde yetkilendirilmeksizin elektronik haberleşme hizmeti sunan şirket, şirket ortağı veya temsile veya idareye yetkili kişiler hakkında 63. maddenin 1. ve 2. fıkraları kapsamında BTK tarafından başlatılan idari soruşturmanın akabinde yürütülen bir adli sürecin bulunmaması gerektiğidir.

1.2.2.7. Yetkilendirmenin İptal Edilmemiş Olması Şartı

Yetkilendirme Yönetmeliği'nin 7. maddesi uyarınca işletmeci olacak şirket için aranan son şart, şirketin en az yüzde onuna sahip yönetim kurulu üyesi, ortak ya da şirketin idaresinde yetkili olan kişilerin kurmuş olduğu şirketlerin Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği'ndeki[60] (İdari Yaptırımlar Yönetmeliği) yeniden yetkilendirmemeye ilişkin hususlar dışında, son üç yıl içerisinde yetkilendirmelerinin iptal edilmemiş olması ve ayrıca yetkilendirmesi iptal edilmiş ise bu sebebin ortadan kalkmış olması hali aranmaktadır.

1.2.3. İşletmecinin Yetkilendirilmiş Olması Şartı ve Yetkilendirme Usulü

5809 sayılı EHK'da yer verilen işletmeci kavramının unsurlarından biri olan yetkilendirilmiş olma şartı, yine aynı Kanun'un 8/1 maddesinde, elektronik haberleşme hizmeti sunulabilmesi, şebeke ve altyapısının kurulup işletilebilmesi için Kurum tarafından yetkilendirilmiş olma koşuluna bağlanarak pekiştirilmiştir. Ayrıca ilgili maddenin 2. fıkrası uyarınca, kişinin ticari amaç gütmeyen ve üçüncü kişilerin kullanımına sunulmayan elektronik haberleşme hizmeti gibi ayrıksı haller dışında, elektronik haberleşme hizmeti yalnızca yetkilendirilmiş işletmeciler tarafından sağlanabilmektedir. Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme

[59] BTK'nın 16.03.2021 tarih ve 2021/DK-YED/80 sayılı Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorune-iliskin-yetkilendirme-yonetmeligi-nde-degisiklik-yapilmasina-dair-yonetmelik-ile-yetkilendirme-basvurusu-sartlarina-ve-surelerine-iliskin-duzenlemeler/80-2021-web.pdf , Erişim Tarihi: 4 Mart 2022.
[60] R.G. 15.02.2014, S. 28914.

Yönetmeliği'nin (Yetkilendirme Yönetmeliği)[61] 5/1 maddesinde de bu hizmetin yetkilendirilmiş işletmeciler tarafından sunulabileceğine değinilmiştir.

Yetkilendirme, EHK'nın 3/1-(ccc) maddesinde, elektronik haberleşme şebekesi temini veya hizmetinin sunulması amacıyla BTK tarafından kayıt altına alınan şirketlere bu hizmetlere mahsus hak ve yükümlülük tanınması durumu olarak ifade edilmektedir.

Ülkemizde, elektronik haberleşme hizmetine ilişkin kanun dışındaki diğer hukuki düzenlemelerin yapılması ve bu hizmeti sunan işletmecilerin ve pazarın denetlenmesi konusunda, düzenleyici ve denetleyici merci sıfatını taşıyan BTK yetkili kılınmıştır. Yetkilendirilmiş işletmecilerin güncel listesine Kurum'un internet sayfasında yer verilmektedir.[62]

Yetkilendirmeye ilişkin usule EHK'nın 9. maddesinde yer verilmiştir. Kurum tarafından bildirim veya kullanım hakkı verilmesi yoluyla yetkilendirilen şirketler işletmeci sıfatını haiz olabilmektedir.

1.2.3.1. Bildirim Yoluyla Yetkilendirme

EHK'nın 9. maddesinin 2. ve 3. fıkrasında bildirim yoluyla yetkilendirmeye yer verilerek elektronik haberleşme hizmeti sunabilmek veya şebeke ve altyapı kurulumunu ve işletmesini yapabilmek için Kurum'a bildirimde bulunulması gerektiği vurgulanmıştır. Bu çerçevede, sunulacak olan hizmet için frekans, numara veya uydu pozisyonu gibi kaynakların işletmeciye tahsisinin gerekli olması halinde kendilerine kullanım hakkı tanınarak yetkilendirileceklerinden, sınırlı kaynakların tahsisi gerekmediğinde ise yalnızca Kurum'a yapmış oldukları usulüne uygun bildirimle birlikte faaliyete başlayabilecekleri belirtilmektedir.[63]

1.2.3.2. Kullanım Hakkı Yoluyla Yetkilendirme

EHK'nın 9/4 maddesi ve devamında kullanım hakkı verilmesi yoluyla yetkilendirmeden söz edilmektedir. Kurum tarafından kullanım hakkının sınırlandırılmasının gerekip gerekmediğine karar verilerek uygun başvuru olması halinde başvuruyu müteakip en fazla 30 gün içerisinde kullanım hakkının verilmesi gerektiği,

---

[61] R.G. 28.5.2009, S. 27241.

[62] BTK Yetkilendirme Yönetim Sistemi, https://yetkilendirme.btk.gov.tr/Yetkilendirme/isletmeci-arama.xhtml;jsessionid=3UGcwEIkVM3KfxvHMeVfdxgurRAyEVYtNxF5uCm4.be1 , Erişim Tarihi: 4 Mart 2022.

[63] Burak Öztürk, "Elektronik Haberleşme Hizmetlerinde Yetkilendirmenin Hukuki Niteliği," *Ankara Barosu Dergisi,* no.1 (2009): 29-31.

kaynakların etkin ve verimli kullanılabilmesi amacıyla sınırlı kaynakların olduğu alanlarda sınırlı işletmeciye izin verilebileceği ve böyle durumlarda kullanım hakkı sayısının sınırlandırılabileceğinden söz edilmiştir. Bu doğrultuda, kaynakların etkin kullanımı amacıyla Bakanlığın görüşüne başvurulabileceği ve Kurum'un ihale için usul ve esasları düzenleyebileceği, şebeke ve hizmetin niteliğine bağlı olarak başvurucunun talebi doğrultusunda kullanım hakkı süresinin belirlenebileceği fakat her halükarda bir işletmeciye en fazla 25 yıl kullanım hakkı verilebileceği vurgulanmıştır. Ayrıca Kurum'un, kamu düzeni ve benzeri kamu yararını gerektiren hallerin varlığı halinde veya ihale aşamasında başvurucunun yeterli koşulları sağlayamadığının tespiti halinde başvuruyu reddedebileceği; kullanım hakkının verilmesi halinde ise işletmecinin hukuka aykırı eylemleri sebebiyle işletmeci tarafından elde edilen hakkın iptal edilebileceği hüküm altına alınmıştır.

Yetkilendirme Yönetmeliği'nin 10. maddesinde yetkilendirme türlerinden biri olan kullanım hakkının hangi hallerde sınırlandırılabileceği belirtilerek sınırlı sayıda kaynakların etkin ve verimli kullanılabilmesi amacıyla kullanım hakkının sınırlandırılabileceği hüküm altına alınmıştır. BTK tarafından verilen yetkinin kaynağının sınırlı olması halinde, yapılan yetkilendirme sayısı sınırlandırılmış yetkilendirme olarak anılmaktadır. Uydu pozisyonuna bağlı olarak ülke genelinde verilecek olan frekans bandı kullanımını içeren elektronik haberleşme hizmetlerinden olan mobil haberleşme hizmetleri buna örnek olarak gösterilebilir.[64] Bunun gibi alanlarda yetkilendirme almak isteyen işletmeciler için Yetkilendirme Yönetmeliği'nin 7. maddesinin 2. fıkra hükmü uygulama alanı bulmaktadır. Bu hüküm uyarınca, aynı maddenin 1. fıkrasının (a) bendi haricindeki tüm şartların aynen uygulanacağı, bunlara ek olarak ise kurulmuş veya kurulacak olan şirketin anonim şirket olması ve bu şirketin hisselerinin hepsinin nama yazılı olmasının yanı sıra ilgili mevzuat ve/veya ihale şartnamesinde belirtilen hususları taşıması gerekmektedir.

İlgili Yetkilendirme Yönetmeliği'nin 7/2 hükmünün (a) bendinde Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği'nde Değişiklik Yapılmasına

[64] Mobil genişbant hizmetlerinin kullanıcılara daha az maliyetle ve daha hızlı şekilde sunulabilmesi için önceden işletmecilere tahsis edilen frekanslara daha fazla frekans eklenerek belirli frekans aralıkları IMT İhalesi (4.5G İhalesi) ile toplamda 390,4 MHz frekans satışa sunulmuştur. BTK, Mobil İletişimde Yeni Teknoloji 4.5G Broşürü, 22, https://www.btk.gov.tr/uploads/pages/slug/45g-brosur.pdf , Erişim Tarihi: 5 Mart 2022.

Dair Yönetmelik[65] (Değişik Yetkilendirme Yönetmeliği) ile yapılan değişiklikte görülmektedir ki; sayısı sınırlandırılmış kullanım hakkı elde etmek isteyen işletmecinin, aynı 7. madde hükmünün 1. fıkrasının (a) bendinde belirtildiği üzere anonim veya limited şirket olabilmesinin aksine, yalnızca anonim şirket olabileceği hüküm altına alınmıştır.[66]

Sayısı sınırlandırılmış kullanım haklarına ilişkin yetkilendirmeler hususunda, kullanım hakkı sayısının sınırlandırıldığı alanlarda hizmet vermek isteyen şirketlerin işletmeci olarak elektronik haberleşme hizmeti sunabilmesi için yetkilendirilmeleri gerekliliğinin yanı sıra şirket yapısına dair sayılan şartların dışında şirket türünde farklılık bulunduğu görülmektedir.

1.2.4. Elektronik Haberleşme Sektöründe Şirketlerin Yetkilendirilmesine İlişkin Diğer Durumlar

Elektronik haberleşme sektöründe işletmeci olabilmek için şirketler gerekli şartları sağlamış olsa da EHK'nın 9. maddesinin 11. ve 12. fıkralarında belirtildiği üzere kamu güvenliği ve kamu sağlığı gibi gerekçelerle ve gerektiğinde Bakanlığın da görüşü doğrultusunda Kurum tarafından şirketlerin işletmeci olabilmeleri engellenebilmekte, faaliyete geçmiş olanlar ise mülki amirlerce kapatılabilmektedir.

Yetkilendirmeye ilişkin bir başka durum ise EHK'dan önce yayımlanan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in[67] (Faaliyet Belgesi Yönetmeliği) 3/1-(k) maddesindeki işletmeci tanımında, işletmecinin faaliyet gösterebilmesi için Kurum tarafından ruhsat veya genel izin verilmesi, kayıtlanmasından söz edilmiştir. Bu doğrultuda, erişim sağlayıcı[68] ve yer sağlayıcılar[69] için 5809 sayılı

---

[65] R.G. 11.06.2016, S. 29739.

[66] Değişik Yetkilendirme Yönetmeliği'nin yayımlandığı gösteren BTK'nın 16.03.2021 tarih ve 2021/DK-YED/80 sayılı Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorune-iliskin-yetkilendirme-yonetmeligi-nde-degisiklik-yapilmasina-dair-yonetmelik-ile-yetkilendirme-basvurusu-sartlarina-ve-surelerine-iliskin-duzenlemeler/80-2021-web.pdf , Erişim Tarihi: 5 Mart 2022.

[67] R.G. 24.10.2007, S.26680.

[68] 5651 sayılı Kanun'un 2/1-(e) bendinde, erişim sağlayıcı, *"Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler"* şeklinde ifade edilmiştir.

Erişim sağlayıcı, işletmeci ile kullanıcı arasında abonelik sözleşmesi imzalanarak internet kullanıcılarının internete ulaşabilmelerini sağlar. Erişim sağlayıcı, herhangi bir internet içeriği üretmez, üretilen içeriğe ulaşılmasını sağlar. Buradan hareketle, erişim sağlayıcıları yayıncı olarak nitelendirilmez, dağıtıcı olarak kabul edilir. (Yasin Söyler, *Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi*, (Ankara: Savaş Yayınevi, 2014), 169.)

[69] 5651 sayılı Kanun'un 2/1-(m) bendinde yer sağlayıcının, *"Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler"* olduğu hususuna yer verilmiştir. İnternet sitelerinin resim,

EHK'da yer verilen yetkilendirmenin dışında ayrıca bir faaliyet belgesinin daha gerekli olduğu anlaşılmaktadır.[70] Erişim sağlayıcı veya yer sağlayıcı olmak isteyen işletmecilerin Kurumdan aldıkları yetkilendirmenin yanı sıra yer sağlayıcılığı için beş yıl süreyle geçerli olan ve erişim sağlayıcılığı için Kurum tarafından yetkilendirildiği süre kadar hizmet sağlanabilen bu faaliyet belgeleri için Kurum'a ayrı ayrı başvurması gerektiği hüküm altına alınmıştır.[71] 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un[72] 11/2 maddesinde yer alan erişim ve yer sağlayıcıların faaliyetlerini yerine getirebilmeleri amacıyla Kurum'dan belge almaları gerektiğine ilişkin hükümde, 6518 sayılı Kanun'un 96. maddesiyle "yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine" şeklinde değişiklik yapılarak erişim ve yer sağlayıcılarının faaliyet belgesi alma yükümlülüğü ortadan kalkmıştır. Ayrıca yine 6518 sayılı Kanun'un 88. maddesiyle, yer sağlayıcıların yükümlülüklerine yer verilen 5651 sayılı Kanun'un 5. maddesine 6. fıkra hükmü eklenerek yer sağlayıcılara yalnızca BTK'ya bildirim yapma yükümlülüğü getirilmesinden, yer sağlayıcıların faaliyet belgesi alma zorunluluğunun ortadan kalktığı söylenebilir.

1.3. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ABONE, ABONE ADAYI, TÜKETİCİ, KULLANICI VE SON KULLANICI KAVRAMLARI

Elektronik haberleşme sektöründeki hizmetlerden faydalanmak isteyen veya faydalanan kişiler abone adayı, abone, tüketici, kullanıcı ve son kullanıcı olarak adlandırılmaktadır. Bu kavramlar işletmeci ile hizmetten faydalanan kişi arasında sözleşme olup olmamasına veya hizmetten faydalanan kişinin gerçek veya tüzel kişi olmasına göre farklılık göstermektedir.

Abone dışında, abonelik kapsamında elektronik haberleşme sektöründeki hizmetleri kullanan başka kişiler de olabilir.[73] "Kullanıcı" olarak adlandırılan bu kişiler,

---

video gibi bütün unsurlarının web sunucusunda bulundurularak kullanıcılar tarafından bunlara erişim sağlanması işlemleri yer sağlayıcıları vasıtasıyla gerçekleştirilmektedir. Söz konusu sunucuların yer aldığı "data center" olarak adlandırılan sistem odaları, yer sağlayıcı işletmeciler tarafından kullanılmaktadır. (Bülent Kent, *Türkiye'de İnternet Sitelerine Erişimin Engellenmesi,* (Ankara: Adalet Yayınevi, 2019), 45.

[70] Alp Öztekin, *Teori ve Uygulamada Türk İnternet Hukuku*, (Ankara, Seçkin Yayıncılık, 2021), 166, 207.

[71] Faaliyet Belgesi Yönetmeliği'nin 4., 5. ve 6.maddelerinde ilgili hususlar düzenlenmiştir.

[72] R.G. 23.05.2007, S. 26530.

[73] Alman Telekomünikasyon Kanunu'nda elektronik haberleşme sektöründeki hizmet sunumlarına ilişkin sözleşmelerde abone kavramı yerine, Türkçe'de katılan ya da katılımcı olarak tercüme edilen "Teilnehmer"

abonenin yararlandığı hizmetleri aynı şekilde kullanmakta ancak elektronik haberleşme hizmetinin kullanımı çerçevesinde sorumluluk yönünden bazı farklılıklar ortaya çıkmaktadır.

1.3.1. Abone Tanımı

Abone, EHK'nın 3/1-(a) maddesinde, *"Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişi"* olarak tanımlanmıştır. Tüketici Hakları Yönetmeliği'nin 4/1-(a) maddesinde de aynı tanıma yer verilmiştir. Diğer bir ifadeyle, elektronik haberleşme mevzuatı çerçevesinde genel anlamda bir tanım yapmak gerekirse; sabit telefon hizmeti, internet hizmeti, GSM hizmeti gibi elektronik haberleşme hizmetlerinden yararlanabilmek için işletmeci ile iletişime geçerek abonelik sözleşmesi imzalayan kişi abone olarak tanımlanabilir.

TKHK ve ASY'de ise abone kavramına yer verilmemiş, tüketici kavramı kullanılmıştır.

1.3.2. Abone ve Tüketici Kavramları Arasındaki İlişki

EHK'nın 3/1-(uu) maddesinde tüketici, *"Elektronik haberleşme hizmetini ticari veya mesleki olmayan amaçlarla kullanan veya talep eden gerçek veya tüzel kişiyi, ..."* ifade etmektedir.

TKHK'nın 3/1-(k) maddesinde ise tüketici, *"Ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişi"* şeklinde tanımlanmaktadır. Söz konusu hüküm çerçevesinde hem gerçek kişi tacirler hem de tüzel kişi tacirler tüketici vasfına bürünebilir. Tüzel kişi tacirlerin, tüketici vasfına sahip olup olamayacakları hususunda doktrinde bazı tartışmalar bulunmaktadır. Bu görüşlerden birincisi, Türk Ticaret Kanunu'nun[74] (TTK) 19/1 maddesinde, tacirin borçlarının ticari olduğu kuralına yer verilerek bu kuralın istisnasının ise ancak gerçek kişi tacir tarafından yapılan işlemin kendi işletmesiyle ilgisinin bulunmadığının karşı tarafa açık bir şekilde bildirilmesi halinde adi borç sayılabileceği belirtilmektedir. Söz konusu hükümden hareketle, tüzel kişi tacirlerin istisnaya yer vermeyecek biçimde tüm borçlarının ticari iş kapsamında

kavramı kullanılmıştır. Elektronik haberleşme sektöründeki hizmetlerin geniş kapsamlı olması ve bunları kullananlar düşünüldüğünde ilgili kavramın abone kavramına göre daha isabetli olduğu söylenebilir. (Mustafa Göktürk Yıldız, *Son Kullanıcıyla Akdedilen Elektronik Haberleşme Sözleşmesi*, (On İki Levha Yayınları: İstanbul, 2012), 11-12.)

[74] R.G. 14.02.2011, S. 27846.

değerlendirilmesi gerektiği vurgulanarak gerçek kişi tacirlere ticari işlerinin haricinde adi bir alanın ayrılması gerektiği belirtilmektedir.[75] Bu doğrultuda, TKHK'da yapılan tüketici tanımındaki tüzel kişi kavramının yalnızca ticaret şirketleri haricindeki tüzel kişiler anlamında kullanılması gerektiğini, tüzel kişi olan tacirlerin tüketici vasfına haiz olamayacağı vurgulanmaktadır.[76]

İkinci görüş[77] ise TTK'nın 19. maddesinde belirtilen ticari iş karinesinin ancak ilgili işin ticari işletmeyle bağlantısı olması halinde geçerli olacağına ilişkindir. Ticari işletmeyle ilgisi bulunmadan tüketim amacıyla hareket edilmesi durumunda tacir şirket olsa bile tüketici sıfatını kazanarak bu doğrultuda değerlendirmenin yapılması gerektiği düşünülmektedir.[78]

Her ne kadar EHK'da yer verilen tüketici tanımında ticari veya mesleki amaç haricinde elektronik haberleşme hizmetinin kullanılması ve talep edilmesinin tüketici olmanın koşulu olarak gösterilmiş olsa da elektronik haberleşme hizmeti, abonenin bu hizmeti ne amaçla kullandığının kolaylıkla bilinemediği bir sektöre ilişkin sunulan hizmettir. Anayasa'nın 22. madde hükmünde yer alan haberleşmenin gizliliği ilkesi gereğince, işletmeci tarafından abonesinin haberleşmesi izlenemeyeceğinden; kurumsal abonelik yetkilisi olan kişinin işletmeci tarafından sunulan bu hizmeti şahsi amaçlarla mı yoksa yetkilisi olduğu tüzel kişiliğin ticari veya mesleki amacına yönelik mi kullandığının takibi yapılamamaktadır. Bu sebeple de tüzel kişilik adına açılan elektronik haberleşme aboneliğinin karineten ticari amaçlarla kullanıldığının kabulü gerekmektedir. Adına abonelik açılan tüzel kişiliğin ise tüketici sıfatını haiz olamayacağını söyleyebiliriz.

Tüzel kişi abonenin tüketici sıfatını haiz olup olmaması, aboneyle işletmeci arasında çıkan uyuşmazlığın çözümünde uygulanacak olan kanunların ve görevli mahkemenin belirlenmesi açısından önemli iken bu hususun kişisel verilerin korunması

---

[75] Şaban Kayıhan, *Ticari İşletme Hukuku*, (Ankara: Seçkin Yayıncılık, 2018), 84-85; İsmail Kayar, *6102 sayılı Türk Ticaret Kanunu'na Göre Ticaret Hukuku*, (Ankara: Seçkin Yayıncılık, 2018), 88-89.

[76] Yakup Bal, *6502 sayılı Tüketicinin Korunması Hakkında Kanun Kapsamında Abonelik Sözleşmeleri*, (Ankara: Seçkin Yayıncılık, 2020), 34-35.

[77] İpek Yücer Aktürk, "Tüzel Kişi Tacirin Tüketici Sıfatı," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 20, no.2 (2016): 118.

[78] Yargıtay 20. Hukuk Dairesi tarafından verilen 2017/9858 E., 2017/9664 K. sayılı kararda, telefon aboneliğine ilişkin abonelik sözleşmesine dayanarak ödenmeyen alacak için açılan icra takibine itiraz edilmesi sonucunda itirazın iptali davasının hangi mahkemede açılması gerektiği konusunda, davacının uyuşmazlığa konu telefon numarasını ticari veya mesleki amaç dışında şahsi amaçla edinmesi sebebiyle abonelik sözleşmesinin TKHK kapsamında değerlendirilerek abonenin tüketici işlemi gerçekleştirdiği düşünülmesi sebebiyle uyuşmazlığın tüketici mahkemesinde görülmesinin uygun olduğu kanaatine varılmıştır. www.kazanci.com.tr , Erişim Tarihi: 5 Mart 2022.

bakımından işletmecinin konumuna herhangi bir etkisi bulunmamaktadır. Şöyle ki; işletmeci, abonenin yetkilisinin kişisel verilerini işlemesi bakımından veri sorumlusu olmakla birlikte abonenin haberleşme hizmeti gerçekleştirirken ulaştığı telefon numarası veya trafik ve konum verileri gibi bilgileri iletişimin gerçekleştirilebilmesi amacıyla işlemesi bakımından ise veri işleyen[79] konumundadır. İşletmeci ve abone arasındaki bu konum, abonenin hukuki nitelendirilmesine göre değişmemektedir.

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'in[80] (Kişisel Verilerin İşlenmesi Yönetmeliği) kapsamına yer verilen 2. maddesinde, ilgili Yönetmeliğin tüzel kişi abonelikler için de uygulanacağı bildirilmiş, tüzel kişi aboneliğin tüketici sıfatını haiz olup olmaması ayrımına değinilmemiş, tüketici tanımına da yer verilmemiştir.

1.3.3. Abone Adayı Kavramı

EHK'daki tüketici tanımından da anlaşılacağı üzere elektronik haberleşme hizmetini kullanan abonenin yanı sıra abone olmak isteyen kişiler de tüketici kapsamına dahil edilmiştir. İşletmeciyle gerek bizzat iletişime geçerek gerekse işletmeciye ait internet sitesi vasıtasıyla kişisel bilgilerini vermek suretiyle kendisiyle iletişime geçilmesini talep ederek elektronik haberleşme hizmeti almak isteyen potansiyel abone, daha sonra işletmecinin abonesi olmasa bile işletmeci tarafından bu kişinin bilgileri elektronik haberleşme hizmeti sunumu amacıyla toplanmaktadır. Abone olma potansiyeline sahip olan bu kişiler, çalışmamızda "abone adayı" olarak adlandırılacaktır.

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 2. maddesinde belirtilen kapsamının, elektronik haberleşme hizmeti sunma amacıyla işletmecilerin edindikleri veriler olması sebebiyle, her ne kadar abone adayı henüz işletmeciden hizmet almaya başlamamış olsa bile işletmeci abone adayının kişisel verisini, hizmetin sunumuna başlayabilmek ve elektronik haberleşme hizmeti sunumu için abone adayını kendi abonesi yapabilmek adına işlediğinden; Kişisel Verilerin İşlenmesi Yönetmeliği hükümleri abone adayı için de uygulanacaktır.

---

[79] Veri işleyen, 6698 sayılı Kanun'un 3/1-(ğ) maddesine göre, *"veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak adlandırılmıştır.
[80] R.G. 04.12.2020, S. 31324.

1.3.4. Kullanıcı ve Son Kullanıcı Kavramları

2002/58/EC sayılı Direktif'in 2.maddesinde, kullanıcı, *"kamuya açık olan bir elektronik haberleşme hizmetini, bu hizmete abone olmak zorunda olmaksızın, özel veya ticari amaçlarla kullanan herhangi bir gerçek kişi"* olarak tanımlanmıştır.

EHK'nın 3/1-(cc) maddesine göre ise kullanıcı, abone olmasa bile elektronik haberleşme hizmetlerinden faydalanan gerçek ya da tüzel kişilerdir. İlgili tanım doğrultusunda, abone ve kullanıcı arasındaki ayrımı belirleyen temel hususun sözleşmeye taraf olmak bakımından belirginleştiği görülmekle birlikte elektronik haberleşme hizmetinden abone ismiyle tanımlanan kişilerin dışında başka kimselerin de faydalanabildiği anlaşılmaktadır. Kullanıcı olarak tanımlanan kimselerin, işletmeci ile arasında abonelik sözleşmesi bulunması gerekmemektedir.[81]

Son kullanıcı ise EHK'nın 3/1-(jj) maddesi uyarınca, elektronik haberleşme hizmetinden yalnızca kendisi için faydalanan, diğer bir deyişle üçüncü kişilere elektronik haberleşme hizmeti veya şebekesi sunma faaliyeti gerçekleştirmek amacıyla ilgili hizmetten faydalanmayan kişilerdir.[82]

Her ne kadar kullanıcı ve son kullanıcı abone gibi işletmeciyle abonelik sözleşmesi imzalamamış olsa da elektronik haberleşme hizmetinden faydalanan kişiler olarak adlandırılabileceklerinden; Kurum'un görevlerinden bahsedildiği EHK'nın 6/1-(c) maddesinde yer verilen kullanıcı ve son kullanıcının kişisel verilerinin de abone ve tüketicinin kişisel verileri ve haklarıyla aynı şekilde işlenmesine ve korunmasına dair düzenlemelerin Kurum tarafından yapılmasına ilişkin hükümden ve EHK'nın Dördüncü Kısım'ında yer verilen haklar ve kişisel verilerin korunmasına ilişkin hükümlerden[83] anlaşılacağı üzere, herhangi bir haberleşme sözleşmesine taraf olmamasına rağmen bu hizmetten faydalanan herkesin bahsi geçen hükümler çerçevesinde korunacağı belirtilmiştir.[84] Keza Tüketici ve Kullanıcı Şikâyetlerinin İşletmeciler ve Posta Hizmet Sağlayıcıları Tarafından Çözümlenmesine İlişkin Usul ve Esaslar'ın (Tüketici Şikâyetleri Usul Esasları)[85] kapsamına kullanıcılar dahil edilerek elektronik haberleşme sektöründe

---

[81] Yıldız, *Son Kullanıcı Sözleşmesi*, 13.
[82] Yıldız, *Son Kullanıcı Sözleşmesi*, 12-13.
[83] EHK'nın Dördüncü Kısım'ında eşit hizmet alabilme hakkı, tüketici ve son kullanıcının korunması hakkı, şeffaflığın sağlanması ve bilgilendirme, abonelik sözleşmeleri ve kişisel verilerin işlenmesi ve gizliliğin korunması başlıklı 47. ve 52. maddeleri yer almaktadır.
[84] Yıldız, *Son Kullanıcı Sözleşmesi*, 13-14.
[85] BTK'nın 22.05.2018 tarih ve 2018/DK-THD/162 sayılı Kurul Kararı ile yayımlanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/tuketici-ve-kullanici-sikayetlerinin-isletmeciler-ve-posta-

hizmet alan kişi abone olmasa da hizmete ilişkin şikayetlerinin işletmeciler tarafından tüketicilerle aynı ihtimam gösterilerek cevaplanması gerektiği anlaşılmaktadır.

1.4. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ABONELİK SÖZLEŞMESİ

1.4.1. Abonelik Sözleşmesi Kavramı

EHK'nın 3/1-(b) maddesinde abonelik sözleşmesi, *"İşletmeci ile abone arasında akdedilen ve işletmecinin bir bedel karşılığında dönemsel ya da sürekli olarak bir hizmeti yerine getirmeyi veya mal teminini üstlendiği ya da her ikisini birden kapsayan sözleşme"* olarak tanımlanmıştır. Aynı tanıma, Tüketici Hakları Yönetmeliği'nin 4/1-(b) bendinde de yer verilmiştir. Söz konusu tanımın elektronik haberleşme sektöründeki abonelik sözleşmelerine özgü olmadığı, genel olarak bütün abonelik sözleşmeleri için kullanılabileceği söylenebilir. Çünkü esas itibarıyla, elektronik haberleşme sektöründe aboneye elektrik, su ve gaz gibi sürekli nitelikte sunulabilen mal temininin aksine hizmet sunumu gerçekleştirilmektedir. Bu sebeple genel nitelikteki bu tanıma özel nitelikli kanun olan EHK yerine, daha genel nitelikte olan TKHK'da yer verilmesi daha uygun olabilirdi.[86] Abonelik sözleşmeleri, 6502 sayılı TKHK'da ise 52/1 maddesinde, *"Abonelik sözleşmesi, tüketicinin, belirli bir mal veya hizmeti sürekli veya düzenli aralıklarla edinmesini sağlayan sözleşmelerdir"* şeklinde ifade edilmiştir. ASY'nin 4/1-(a) bendinde de aynı tanıma yer verilmiştir.

Elektronik haberleşme sektöründe işletmeci ve abone tanımları incelediğinde görüleceği üzere; abone elektronik haberleşme hizmetini alan, işletmeci ise bu hizmeti sunan taraf olup; abonelik sözleşmelerinin konusu ise bu hizmetin sunumudur. Diğer bir deyişle, abonelik sözleşmelerinin konusu, söz konusu tanımlarda yer aldığı gibi mal temini değildir. İşletmeciler elektronik haberleşme hizmeti sunmakta, bu hizmeti sunmaları için gerekli olan telefon ve benzeri cihazların abone tarafından temini ise elektronik haberleşme hizmetinden faydalanabilmek için gerekmektedir. İlgili mevzuatta abonelik sözleşmesine ilişkin yer alan tanımlarda bahsedildiği üzere, elektronik haberleşme hizmeti sunmak için yetkilendirilmiş olan işletmecilerin yalnızca mal

hizmet-saglayicilari-tarafindan-cozumlenmesine-iliskin-usul-ve-esaslar/162-2018-web.pdf , Erişim Tarihi: 12 Mart 2022.

[86] Yıldız, *Son Kullanıcı Sözleşmesi*, 5-6.

teminini içeren sözleşmelere taraf olması halinin özel nitelikte olan elektronik haberleşme mevzuatı kapsamında yapılan abonelik sözleşmelerinden ayrılması ve daha genel nitelikte olan Türk Borçlar Kanunu (TBK)[87] ve TKHK kapsamında incelenmesi gerektiği söylenebilir. Bu sebeple abonelik sözleşmesi tanımlarında yer alan mal temini ifadesi yerine elektronik haberleşme hizmetini yerine getirme veya bu hizmetin sağlanmasıyla beraber mal temininin üstlenilmesi benzerinde bir ifadenin kullanılması, elektronik haberleşme sektöründe aboneye sunulan hizmeti daha doğru şekilde karşılayacaktır.[88]

Borçlar hukukunun temel ilkelerinden olan sözleşme özgürlüğüne karşılık kamu hukukunda elektrik, su, doğalgaz, ulaştırma gibi alanlarda imtiyaz hakkına sahip olan işletmecilerin, bu hizmetlerden faydalanmak isteyen kişilerle abonelik sözleşmesi imzalama yükümlülüğü mevcuttur.[89] Elektronik haberleşme alanında ise sektörün tekel niteliğe sahip olmaktan çıkarak rekabete açılması sonucunda işletmecilerin hala abonelik sözleşmesi yapma yükümlülüğünün bulunup bulunmadığı incelenmesi gereken bir durumdur. 2009/136/EC sayılı Vatandaş Hakları Direktifi'nde[90] söz konusu hususa açıklık getirilmiş; haberleşme şebekesi işletmecileri veya kamuya açık olan elektronik haberleşme servisi işletmecilerinin, abone olmak isteyen tüketici veya diğer son kullanıcılara sözleşme yapma hakkını sağlamaları gerektiği belirtilmiştir.[91]

Avrupa Birliği ile uyumlaşma çalışmaları çerçevesinde iç hukukumuzda da abonelik sözleşmelerine ilişkin yeni düzenlemeler yapılma ihtiyacı ortaya çıkmıştır. EHK'nın 50/1 maddesinde elektronik haberleşme hizmeti almak isteyen tüketicilerin, işletmecilerle sözleşme yapma hakkının bulunduğu belirtilmiştir. Aynı şekilde Tüketici Hakları Yönetmeliği'nin 5/1-(b) maddesinde abonelere işletmecilerle abonelik sözleşmesi yapma hakkı verildiği görülmektedir. Bu doğrultuda abonelik sözleşmesi, abonelere sunulmuş bir hak olarak nitelendirilmiştir. İşletmeciler açısından ise abonelik sözleşmesi yapmanın bir yükümlülük olduğu, yine EHK'nın 50/2 maddesindeki Kurumun işletmecilerden abonelik sözleşmelerini isteyebilmeleri ve gerektiğinde değişiklik yapılmasını talep edebilmesinden anlaşılabilmektedir.

---

[87] R.G. 4.2.2011, S. 27836.
[88] Bal, *TKHK Abonelik Sözleşmeleri*, 31.
[89] Ayşe Özkaya, *Elektronik Haberleşme Sektöründe Tüketicinin Korunması Açısından Abonelik Sözleşmelerinin İncelenmesi*, 2011, BTK Bilişim Uzmanlığı Tezi, 75. https://www.btk.gov.tr/uploads/thesis/elektronik-haberlesme-sektorunde-tuketicinin-korunmasi-acisindan-abonelik-sozlesmelerinin-incelenmesi.PDF , Erişim Tarihi: 6 Mart 2022.
[90] Directive 2009/136/EC, *EUR-Lex,* Erişim Tarihi: 6 Mart 2022.
[91] Özkaya, EHS'de Abonelik Sözleşmelerinin İncelenmesi, 76.

Ayrıca Anayasa'nın 22. maddesinde belirtilen haberleşme hürriyeti, herkesin haberleşme hizmetinden faydalanabilmesini esas almıştır. Bu sebeple de makul bir sebep olmaksızın abone olmak isteyen kişiyle abonelik sözleşmesi yapılmaması hali yasaklanmıştır. Bununla birlikte, elektronik haberleşme hizmetinin kamu hizmetini haiz olması ve hayatın her anında kullanılan bir temel ihtiyaca dönüşmüş olması sebebiyle makul bir sebep gösterilmediği takdirde bu hizmetten faydalanmak isteyen kişilere sunulması gerekmektedir.

Tüketici Hakları Yönetmeliği'nin 9. maddesi uyarınca BTK, işletmecilerden abonelik sözleşmelerinin sunulmasını ve gerekli gördüğü hususların değiştirilmesini isteyebilir. BTK kurul kararlarında, işletmeciden talep edilen abonelik sözleşmelerinin sunulamaması veya abonelik sözleşmelerinde eksik unsurlar bulunması halinde işletmeciye idari para cezası uygulandığı görülmektedir.[92] Ayrıca BTK, konuya ilişkin vermiş olduğu bir kararda, mobil telefon hizmeti sunan işletmecilere ilişkin abonelik sözleşmesi yapılması gerektiği, aksi halde abonelik sözleşmesi bulunmayan hatların iptal edileceğine yer vermiştir.[93]

İlgili mevzuat doğrultusunda, elektronik haberleşme sektöründe abonelik sözleşmesinin aboneye sunulan bir hak olduğu, işletmeci açısından ise yerine getirilmesi gereken bir yükümlülük olduğu anlaşılmaktadır.

1.4.2. Abonelik Sözleşmelerinin Hukuki Niteliği

Sözleşmeyi oluşturan tarafların hukuki sıfatı, sözleşmenin türünü belirleyen ilk unsurdur. Taraflardan en az birinin idare olduğu sözleşmeler, idarenin sözleşmesi olarak adlandırılabilirken; taraflardan birinin idare olduğu her sözleşme idari sözleşme olmayabilir. İdari sözleşmeler, idare hukukuna tabidir ve uyuşmazlıkların çözüm yeri de

[92] 04.05.2021 tarih ve 2021/İK-SDD/120 sayılı BTK Kurul Kararında, Tüketici Hakları Yönetmeliği'nin 7/1, 7/2-(b), (c), 7/4 maddelerine aykırı olarak, işletmecinin düzenlediği abonelik sözleşmelerinde işletmecinin imza, kaşe, tarih bilgisinin bulunmadığı, bu sebeple ilgili sözleşmeleri eksik şekilde düzenlemesi sebebiyle İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) maddesinin 7. alt bendi ve yine İdari Yaptırımlar Yönetmeliği'nin 44'üncü maddesi doğrultusunda işletmeci hakkında idari para cezası düzenlenmiştir. https://www.btk.gov.tr/uploads/boarddecisions/inceleme-sebeke-ve-bilgi-guvenligine-acentelik-faaliyetlerine-abonelik-sozlesmelerine-ve-cli-a-iliskin-mevzuat-yukumlulukleri-bir-telekom-alfa-iletisim-regnum-nehir-telekom/120-2021-web.pdf , Erişim Tarihi: 6 Mart 2022.

[93] 11.08.2014 tarih ve 2014/DK-THD/395 sayılı BTK Kurul Kararında, 5809 sayılı EHK'nın 4. ve 6. maddeleri, Tüketici Hakları Yönetmeliği'nin 15. maddesi ile diğer mevzuat hükümleri doğrultusunda; mobil işletmecilerin abonelik sözleşmesi bulunmadan hizmet sundukları hatlarının olup olmadığının, varsa iptal işlemleri tamamlanarak BTK'ya bilgi verilmesi gerektiğine yer verilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/abonelik-sozlesmesi-olmaksizin-hizmet-sunulmasi.pdf , Erişim Tarihi: 6 Mart 2022.

idari yargıdır. Bunun yanı sıra idare ile imzalanan sözleşmeler de özel hukuk sözleşmesi olabilir. Her ne kadar bu sözleşmeler özel hukuk sözleşmesi olsa da taraflardan birinin idare olması hasebiyle sözleşme hükümleri idare hukuku hükümlerine göre hazırlandığından; bu sürece ilişkin herhangi bir uyuşmazlık olması halinde uyuşmazlık idari yargıda çözümlenmektedir. Lakin sözleşmenin imzalanmasından sonraki uygulama aşamasında ortaya çıkan uyuşmazlıkların ise adli yargıda çözüme kavuşturulduğu söylenebilir.[94] Anayasa'nın 47. maddesi gereğince, hangi hizmetlerin özel hukuk sözleşmeleri vasıtasıyla görülebileceğine kanunla karar verileceği hüküm altına alınmıştır. Dolayısıyla idare ile yapılan sözleşmelerin hangi tür sözleşme olduğuna ancak kanunla karar verilmektedir.[95]

Her iki tarafın özel hukuk tüzel kişisi olması halinde ise sözleşme özel hukuk sözleşmesidir. Özellikle Anayasa'nın 48. maddesi uyarınca, kişiler sözleşme hürriyetine sahiptir. İrade özgürlüğünün bir yansıması olan ilgili hüküm gereğince, devletin piyasalardaki gerekli sosyal ve siyasi dengeyi sağlayabilmek adına kişilerin irade özgürlüğü çerçevesinde sözleşme yapmalarını destekleyici ortamı sağlaması gerektiği açıktır. İrade özgürlüğünün borçlar hukukundaki yansıması olan sözleşme serbestisidir. Sözleşme serbestisi çerçevesinde taraflar, sözleşme hükümlerini serbestçe belirleyebilmektedir.[96] Ancak sözleşmenin konusunu oluşturan mal veya hizmetin kamuyu ilgilendirmesi halinde idarenin müdahalesi söz konusu oluyorsa, bu sözleşmeler birleşme sözleşme şeklinde adlandırılmaktadır.[97]

Birleşme sözleşmeler, genellikle iki özel hukuk tüzel kişisi arasında akdedilmek istenen ve tarafların mali ve diğer yükümlülüklerinin idare tarafından belirlendiği sözleşmeler olarak tanımlanabilmektedir. Elektronik haberleşme sektöründeki abonelik sözleşmeleri ve arabağlantı sözleşmeleri[98] özel hukuk sözleşmesidir. Bu sözleşmelere ilişkin taraflar arasında ortaya çıkan uyuşmazlıklarda idareye yani elektronik haberleşme

---

[94] Akyılmaz, Türk İdare Hukuku, 478-479; Sancakdar, İdare Hukuku, 597.
[95] Çağlayan, İdare Hukuku Dersleri, 447.
[96] Kübra Ercoşkun Şenol, "Sözleşmenin İçeriğini Belirleme Özgürlüğü ve Bunun Genel Sınırı: TBK m.27," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 74, no.2 (2016): 710-711, 718.
[97] Murat Sezginer, "İdarenin Müdahale Ettiği Özel Hukuk Sözleşmeleri (Bileşik İradeli "Birleşme" Sözleşmeler)," *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17, no.1-2 (2013): 1595.
[98] EHK'nın 16/2 maddesiyle işletmecilerden birinin talebi olması halinde, diğer işletmecilerin arabağlantı görüşmeleri yapmak zorunda olduğu, görüşmelerde anlaşma sağlanamadığında ise Kurum'un ilgili arabağlantının gerçekleştirilmesi yönünde yükümlülük getirme yetkisinin bulunduğuna yer verilmiştir. Bu çerçevede, kamu menfaati açısından işletmeciler arasında arabağlantının kurularak haberleşmenin sağlanabilmesi için gerekli müdahalelerin yapılabileceği anlaşılmaktadır.

sektöründeki düzenleyici kurum olan BTK'ya başvurarak müdahale etmesi istenebilmektedir. Bu da abonelik sözleşmelerinin birleşme sözleşme olduğunu göstermektedir.[99]

EHK'da abonelik sözleşmelerinin nasıl kurulması gerektiğine ilişkin düzenlenmiş olan 50. madde hükmü ile bu hüküm doğrultusunda düzenlenen elektronik haberleşme mevzuatındaki abonelik sözleşmelerinin kurulmasına ilişkin Tüketici Hakları Yönetmeliği'nin 7., 8., 9. ve 10. maddeleri gibi hükümler incelendiğinde idarenin, abonelik sözleşmelerinin kuruluş ve işleyişine yönelik birçok müdahalesinin söz konusu olduğu görülmektedir. Elektronik haberleşme hizmetlerine yönelik abonelik sözleşmeleri, özel hukuk sözleşmesi olması ve bu sebeple sözleşme hükümleri taraflar arasında serbestçe belirlenebilir olmasına rağmen idarenin ilgili sözleşmelere müdahalesi söz konusu olabilmektedir. Bu sebeple elektronik haberleşme hizmetlerine yönelik abonelik sözleşmelerinin birleşme sözleşme olarak değerlendirilmesi mümkündür.

1.4.3. Abonelik Sözleşmelerinde Genel İşlem Koşullarının Varlığı

Abone ile elektronik haberleşme hizmeti sunan kişi arasında karşılıklı yükümlülükleri ihtiva eden bireysel ya da kurumsal olan bir abonelik sözleşmesinde; akdin taraflarının bilgisi, sözleşmede yer alan teknik tanımlar, sözleşmenin konusu, işletmecinin ve abonenin hak ve yükümlülükleri, sözleşmenin süresi ve feshi, uyuşmazlıkların çözüm yerine dair düzenlemeler yer alır.[100] Bu sözleşmeler, çoğu zaman matbu metinler şeklinde hazırlanır ve abone ile karşılıklı olarak imzalanır.[101] Sözleşme hükümlerinin hazırlanmasında, tarafların uymakla yükümlü olduğu elektronik haberleşmeye ilişkin yayımlanan kanunların yanı sıra elektronik haberleşme sektörünün düzenleyicisi konumunda olan üst kurul mahiyetindeki BTK tarafından yayımlanan yönetmelik ve diğer düzenlemelerle birlikte kurul kararları da önem arz etmektedir.

Sözleşmenin taraflarından birinin sözleşmenin kurulmasından önce birden çok kişiyle ayrı ayrı imzalanabilecek şekilde standart hükümler içeren sözleşme hazırlaması durumunda, değiştirilmesi konusunda karşı tarafa pazarlık imkanı sunulmayan hükümler

---

[99] Sezginer, "Birleşme Sözleşmeler," 1595-1596.
[100] Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Kurumsal Sabit Telefon Hizmeti Abonelik Sözleşmesi, https://www.netgsm.com.tr/abonelik/sozlesme/kurumsalabonelik.php , Erişim Tarihi: 7 Mart 2022.
[101] Osman Açıkgöz, *Tüketicinin Korunması Çerçevesinde Mobil Haberleşme Abonelik Sözleşmesinde Genel İşlem Koşulları*, (İstanbul: On İki Levha Yayıncılık, 2013), 209.

genel işlem koşulları olarak anılmaktadır.[102] Her ne kadar sözleşme serbestisi ilkesi çerçevesinde taraflar sözleşmenin hükümlerini serbestçe değiştirme ve içeriğini belirleme özgürlüğüne sahip olsalar[103] da bazı sözleşmeleri mahiyeti gereği taraflardan biri tek yanlı olarak önceden hazırlamaktadır. Sözleşmeyi akdetmek üzere gelen karşı tarafa sözleşme hükümlerini değiştirme hakkı tanınmayan sözleşmeler, tip diğer bir ifadeyle standart sözleşme olarak anılmaktadır.[104] Özellikle banka, elektrik, su aboneliği yapmak üzere imzalanan sözleşmelerde abone olmak isteyen kişiye sözleşme hükümlerini değiştirme hakkı tanınmamakta, sözleşme hükümlerini kabul edemeyecek olanlara yalnızca sözleşmeyi reddetme imkanı tanınmaktadır. Bu durumda sözleşmede zayıf konumunda olanların korunması amacıyla genel işlem koşulları olarak adlandırılan kanuni düzenlemeler öngörülmüştür.[105] TBK'nın 20/1 maddesinde de daha sonra benzer durumlarda kullanılmak için sözleşme kuruluş anından önce sözleşmeyi düzenleyen tarafından tek başına hazırlanarak karşı tarafa sunulan sözleşme maddeleri genel işlem koşulları şeklinde tanımlanmaktadır.

İşletmeciler açısından bakıldığında abonelik sözleşmesinin BTK mevzuatına uygunluğu ön planda olurken aboneler açısından matbu nitelikte olan sözleşmelerdeki genel işlem koşullarının kendileri için aleyhe hususlar içermemesi önemli olmaktadır. Elektronik haberleşme sektöründe düzenlenen abonelik sözleşmelerinin de bu kapsamda incelenebileceği düşünülebilir. Ayrıca TBK'nın 20/4 maddesiyle, yetkili makamlarca verilen izinler doğrultusunda faaliyet gösteren kişi ve kuruluşlar tarafından hazırlanan sözleşmelere de ilgili Kanun'un genel işlem koşullarına ilişkin düzenlemelerinin uygulanacağına dair hüküm uyarınca, BTK'dan yetkilendirilerek hizmet sunabilen işletmeciler tarafından hazırlanan abonelik sözleşmeleri, genel işlem koşulları kapsamında incelenebilecektir.

Tüketici Hakları Yönetmeliği'nin 10. maddesinde; dürüstlük kuralına aykırı olarak aboneyi zarara uğratacak şekilde düzenlenen abonelik sözleşmesi hükümlerinin yazılmamış sayılacağı, hükümlerin birden fazla anlama gelmesi halinde abone lehine

---

[102] Oğuz Ersöz, "Genel İşlem Koşullarının Kişi Bakımından Uygulama Alanı ve Tacirler Hakkında Uygulanması," *İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi* 3, no.1 (2017): 70.
[103] Ezgi Kutluay, "Türk Borçlar Kanunu'nda Genel İşlem Koşulları," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 19, no.3 (2017): 1371.
[104] Eray Aksın Atar, Ertuğrul Erzengin, "Mukayeseli Hukukta Standart Sözleşme Hükümlerinin Çatışması ve Bu Duruma Bağlanan Hukuki Sonuçlar," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 26, no.1 (2020):339-341.
[105] Ersöz, "Genel İşlem Koşulları ," 71-72.

yorumun esas olacağı, sözleşmede belirlenen hak ve yükümlülüklerin sözleşmenin asıl amacına ve ilgili mevzuatın mahiyetine aykırı düşmesi halinde yine dürüstlük kuralı gereğince abonenin aleyhine hüküm olarak kabul edileceği, normal şartlar altında aboneden düşünmesi beklenmeyecek olan hükümlerin yazılmamış sayılacağı, abonelik sözleşmesinde yazılmamış sayılan hükümlerin olması halinde bu hususların elektronik haberleşme sektöründeki hukuki düzenlemelere göre uygulanacağı, yapılan değişiklik ile abonenin beklemeyeceği sonuçlar ortaya çıkması halinde ise sözleşmenin tamamen geçersiz sayılacağı belirtilmiştir. Söz konusu hükmün devamında, ilgili Yönetmeliğin EK-1'inde yer alan abonelik sözleşmelerinde haksız şartların örnekseme yoluyla belirtildiği ve bunların yalnızca abonelik sözleşmeleri için değil, sözleşme ekleri, tarife ve kampanyalar için de geçerli olduğu hüküm altına alınmıştır.

1.4.4. Abonelik Sözleşmelerinin Kuruluş Anı

Tüketici Hakları Yönetmeliği'nin 8/1 maddesinde belirtilen, abonelik sözleşmesinin kurulmasının akabinde hizmetin aboneye fiili olarak sunulmaya başlanmasıyla birlikte hizmete dair ücretlendirmenin gerçekleştirilebileceğine dair hüküm ile ücretlendirme, hizmetin sunumuna başlanmasına bağlanmıştır.[106] Dolayısıyla işletmecinin aboneyi ücretlendirmeye başlamasının ilk ayağı sözleşmenin kuruluş anı kabul edildiğinden abonelik sözleşmeleriyle ilgili incelenmesi gereken bir diğer husus da sözleşmenin kuruluş anıdır.

Abonelik sözleşmeleri, hazırlar arasında ve elektronik ortamda olmak üzere iki şekilde kurulabilir. Hazırlar arasında gerçekleşen abonelik sözleşmeleriyle elektronik ortamda, diğer bir deyişle uzaktan kurulan sözleşmelerin kuruluş anında farklılık bulunmaktadır.[107]

Elektronik haberleşme sektöründe işletmeciler tarafından hazırlanan abonelik sözleşmeleri, tüm abonelere uygulanabilecek şekilde hazırlanmaktadır. İşletmeciler, abonelik başlatmak isteyen her aboneye aynı sözleşmeyi sunmakta ve kendi internet

---

[106] 25.05.2021 tarih ve 2021/İK-THD/134 sayılı BTK Kurul Kararına göre, Tüketici Hakları Yönetmeliği'nin 8/1 maddesine aykırı şekilde abonenin hizmetten faydalanmasına engel olan arızalar giderilmeden veya kurulum yapılmadan önce ücretlendirmeye başlanması sebebiyle İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) ve 44. maddesi uyarınca idari para cezası uygulanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-abonelik-sozlesmesinin-tesisine-iliskin-mevzuat-ihlali-turknet/134-2021-web.pdf , Erişim Tarihi: 7 Mart 2022.

[107] Sinan Sami Akkurt, "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 60, no.1 (2011):31.

sitesinde aboneleriyle imzalamaya hazır olduğu abonelik sözleşmesinin bir örneğini de yayınlamaktadır.[108]

Hazırlar arasında yapılan bir abonelik sözleşmesinden bahsedilirken işletmecinin hazırladığı tek tip abonelik sözleşmesini abone adayına anında sunması davranışı icap, abone adayı tarafından imzalanması da kabul niteliğindedir.[109] Lakin gelişen teknoloji sayesinde elektronik ortamda sözleşme kurulabilmesine imkan sağlanması sonucunda Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik (Kimlik Doğrulama Yönetmeliği)[110] yayımlanarak elektronik haberleşme hizmeti almak isteyen kişinin uzaktan kimliğinin doğrulanması imkanı sağlanmıştır. Bu Yönetmelik akabinde, Tüketici Hakları Yönetmeliği'nde de değişiklik yapılarak ilgili hükümlerin uyumlaştırılması ihtiyacına cevap verilmiştir.

Tüketici Hakları Yönetmeliği'nin 7/1 maddesinde 18 Ocak 2022 tarihinde yapılan değişiklik ile elektronik ortamda abonelik sözleşmesinin kurulduğu hallerde Kimlik Doğrulama Yönetmeliği'nin 9/3 maddesi uyarınca hazırlanan işlem belgesinin başvurana gönderilmeden önce işletmeci tarafından hizmetin sunulamayacağı ve ücretlendirmeye başlanamayacağına ilişkin hüküm eklenerek abonelik sözleşmesinin elektronik ortamda kurulması halinde işlem belgesinin aboneye teslimi, sözleşmenin kurulma anı olarak belirlenmiştir. İlgili maddede atıfta bulunulan Kimlik Doğrulama Yönetmeliği'nin *"İşlem belgesi ve verilerin saklanması"* başlıklı 9. madde hükmünde, kimlik doğrulamaya ilişkin sürecin tüm adımları, aboneye ve doğrulamaya ilişkin bilgileri içeren metnin PDF dosyasına çevrildikten sonra abone adayının onayına sunularak, bu onayın akabinde işletmeci veya hizmet sağlayıcı adına işlemi gerçekleştiren temsilcinin nitelikli elektronik sertifikası veya TCKK sertifikasıyla zaman damgası oluşturularak ilgili PDF dosyasının PAdES-LTV formatına dönüştürülmesi[111], devamında ise oluşturulan bu işlem belgesinin yine ilgili hükümde belirtilen usullerden biri ile başvuru sahibi olan abone adayına gönderilmesi gerektiği belirtilmiştir. Görülmektedir ki; işlem belgesinin abone adayına gönderilebilmesi için elektronik ortamda oluşturulan ilgili sözleşmenin işletmeci

[108] Tüketici Hakları Yönetmeliği'nin 7/3 maddesinde, abonelik sözleşmelerinin zahmetsizce erişilebilir biçimde işletmecinin internet sayfasında yayınlanması yükümlülüğü getirilmiştir.
[109] Özkaya, EHS'de Abonelik Sözleşmelerinin İncelenmesi, 79-80.
[110] R.G. 26.06.2021, S. 31523.
[111] Kimlik doğrulamasını uzaktan yapabilmeyi mümkün kılan Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik'in 3/1-(o) maddesinde PAdES-LTV (PAdES Long Term Validation), PAdES Uzun Dönem Doğrulama şeklinde tanımlanmıştır.

tarafından da imzalanarak onaylanması gerekmektedir. Bu durum, hazırlar arasında yapılan abonelik sözleşmesinin kuruluş anını, elektronik ortamda yapılan abonelik sözleşmelerinin kuruluş anından farklılaştırmaktadır.

Elektronik ortamda kurulan abonelik sözleşmelerinin kuruluş anı, Tüketici Hakları Yönetmeliği'nin 7/1 maddesinde belirtildiği üzere, işletmeci tarafından imzalanmış işlem belgesinin abone adayına gönderilmesi anı olarak kabul edileceğinden; işletmeci tarafından abone adayına sözleşmenin sunulması icaba davet, abone adayı tarafından imzalanması icap, işletmeci tarafından onaylanan abonelik sözleşmesinin abone adayına gönderilmesi anı ise kabul olarak nitelendirilebilecektir.

1.4.5. Abonelik Sözleşmelerinin Muhteviyatı

Tüketici Hakları Yönetmeliği'nin 7/2 maddesinde, Kurum tarafından yapılması zorunlu tutulan abonelik sözleşmelerinin muhteviyatında asgari düzeyde bulunması gerekenler belirlenmiştir. Buna göre sözleşmenin hangi konuları içerdiği, taraf bilgisi ve yükümlülükleri, sözleşme kurulduğu yer ve zaman bilgisi, fesih ve yenilemeye ilişkin koşullar, abonenin hizmeti kullanım esnasında meydana gelebilecek durumlara karşı tarafların alması gereken tedbirlere ilişkin bilgilendirme, olması gereken hizmet kalitesi seviyesi sağlanamadığında abonenin oluşan zararını işletmecinin nasıl gidereceği, tarife bilgisi, faturanın ödenmemesi durumunda hizmetin durdurulma ve kısıtlanması halleri, uyuşmazlık halinde uygulanacak çözüm yolları, işletmeci tarafından aboneye cihaz temin edildiği hallerde sözleşmenin feshi durumunda cihazın iade süreci hakkında bilgilendirme ve benzeri hususlara elektronik haberleşme sektöründeki abonelik sözleşmelerinde yer verilmelidir.

Tüketici Hakları Yönetmeliği'nin 7/3 maddesiyle, abonelik sözleşmelerinin asgari on iki punto ile düzenlenerek abonenin yükümlülüklerinin kolayca anlaşılmasının sağlanması ve koyulaştırılarak yazılmasının yanı sıra işletmecinin internet sitesinde rahatlıkla ulaşılabilecek şekilde yayınlanması mecburiyetini içeren hüküm ile yine aynı Yönetmelik'teki *"Abonelik sözleşmelerinin uygulanması"* başlıklı 8/7 madde hükmünde belirtilen abonelik sözleşmesi, aboneden alınan taahhütname ve benzeri yazılı olarak alınan ve abonenin mali yükümlülüğünü gerektiren evrakın çevrimiçi işlem merkezi[112] vasıtasıyla görülebilmesinin sağlanmasına dair yükümlülük getirilmiştir.

[112] Uygulamada, işletmeciler tarafından abonenin kullanımına sunulan arayüzler, çevrimiçi işlem merkezi olarak ifade edilmektedir.

Özetle, abonelik sözleşmelerinde abonelerin yükümlülüklerinin daha belirgin halde ve kolay erişilebilir olması istenmiştir. Görece işletmeciden daha savunmasız halde olduğu düşünülen abonelerin haklarının hukuken koruma altına alınabilmesi için işletmecilere yükümlülükler getirilmiştir. Küçük puntolarla hazırlanan ve aboneye ait önemli yükümlülüklerin sözleşme içerisindeki diğer hükümler arasında adeta kaybolmasının sağlanması gibi yanıltıcı yöntemlerle abonelerin abonelik sözleşmelerini imzalamak zorunda bırakılmasıyla sıklıkla karşılaşılmaktadır.[113] Bu ve benzeri durumlardan kaçınabilmek adına, Kurum tarafından yapılan söz konusu düzenlemelerin isabetli olduğu söylenebilir. Kişisel verilerin çokça işlendiği veya işlenmek zorunda kalındığı elektronik haberleşme sektöründe, abonenin kendi haklarını ve yükümlülüklerini bilmesi ve bunları bilerek söz konusu aboneliğe onay vermesi elzemdir.

2. ELEKTRONİK HABERLEŞME SEKTÖRÜNE İLİŞKİN İLKELER

5809 sayılı EHK'nın 4. maddesinde belirtildiği üzere elektronik haberleşme sektöründeki işletmecilere numara, uydu pozisyonu, frekans ve benzeri konuların tahsisinde Devletin yetkili ve sorumlu olduğu belirtilerek gereken sistem ve şebekelerin kurulmasına izin verilmesi noktasında da yine Devletin kendisi yetkili kılınmıştır. Devletin bu alanlardaki görünümü bakanlık olarak Ulaştırma ve Altyapı Bakanlığı, düzenleyici ve denetleyici Kurum bakımından tezahürü ise BTK'dır. Bahsi geçen hususları düzenlemesi ve kamu hizmeti niteliğini haiz olan elektronik haberleşme hizmetlerinin yürütülmesi amacıyla temel hakların korunması açısından Kurum'a verilen yetki çerçevesinde, Kurum gerekli düzenlemeleri yaparken birtakım ilkeleri gözetmek zorundadır. Bu ilkelere 5809 sayılı EHK'nın *"İlkeler"* başlıklı 4. maddesinde yer verilmiştir. Genel olarak elektronik haberleşme sektöründeki ilkeler; tüketici hak ve menfaatlerinin gözetilmesi, eşitlik ilkesi-ayrım gözetmeme yükümlülüğü, şeffaflık ilkesi,

[113] 16.03.2021 tarih ve 2021/İK-THD/76 sayılı BTK Kurul Kararı'nda, Tüketici Hakları Yönetmeliği'nin 10/1, 2, 3, 5 maddesi ve aynı Yönetmeliğin Ek-1'inde yer alan 1., 8. ve 9. fıkra hükümleri doğrultusunda, işletmecinin sunduğu kampanyaya ilişkin düzenlenen sözleşme koşullarında yer alan tarifelerin ilgili taahhüt kapsamında olmadığı ve ücret gibi tüm koşullarda işletmecinin değişiklik yapabileceği yönündeki ifadelere yer verilen ilgili sözleşme maddelerinin haksız şart olarak nitelendirilmesi sebebiyle geçersiz olduğuna karar verilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-tuketici-haklarina-iliskin-mevzuat-ihlali-katlama-kampanyasi-turkcell/76-2021-web.pdf , Erişim Tarihi: 7 Mart 2022.

serbest rekabetin sağlanması ve korunması ilkesi, hizmet kalitesi artırımının teşvik edilmesi ilkesi, değişkenlik (uyarlanma) ilkesi ve süreklilik ilkesi olarak sıralanabilir.

2.1. TÜKETİCİ HAK VE MENFAATLERİNİN GÖZETİLMESİ

Elektronik haberleşme sektörüne ilişkin ilkelerden en önemlisi ve temel nitelikte olanı şüphesiz 5809 sayılı EHK'nın 4/1-(b) maddesinde belirtilen tüketicinin hak ve menfaatinin korunmasıdır. Anayasa'da, kendilerini korumaları için devletin tüketicileri desteklemesinin yanı sıra devletin kendisinin de tüketiciyi koruma amacıyla gerekli tedbirleri alacağına ilişkin 172. madde hükmüne yer verilmiştir. Yalnızca elektronik haberleşme sektörünü düzenleyen özel nitelikli kanun olan EHK'da değil, temel borç ilişkisini düzenleyen genel nitelikli 6098 sayılı TBK'da alıcının hak ve menfaatlerinin korunmasına dair hükümlerin yanı sıra 6502 sayılı TKHK'da da tüketicinin hak ve menfaati, satıcı veya hizmet verene karşı korunması gereken taraf olarak görülmekte ve çoğu düzenleme bu anlayış çerçevesinde geliştirilmektedir.

6502 sayılı TKHK'nın *"Amaç"* başlıklı 1. maddesinde tüketicinin bireysel sağlığına ilişkin menfaatinin ve toplum içerisindeki varlığının maruz kalabileceği tehlikelere karşı korunmasının yanı sıra bireyin bilinçlenmesini sağlayacak şekilde ilgili Kanun'da düzenlenmeler yer aldığı belirtilmiştir.

EHK'nın 6/1-(t) maddesiyle Kurum'a verilen görev ile, elektronik haberleşmenin sağlanabilmesi için işletmeciler arasında imzalanan arabağlantı gibi sözleşmelerde mevzuatla belirlenen tedbirleri alarak elektronik haberleşme sektöründeki aktörler için hazırlanacak olan düzenlemelerin tüketicinin hak ve menfaatlerine aykırı hüküm içermeyecek şekilde belirlenmesi gerektiği düzenlenmiştir. Örneğin, tüketicilerin kullandığı akıllı cihaz sayısındaki artış ve videoların genel olarak yüksek kalitede çekilmesi, veri tüketimini artırarak daha yüksek internet erişim hızı ihtiyacını doğurmaktadır. AKN'li olan limitsiz paketlerin tüketici açısından yanılgıya sebep olması sonucunda tüketici şikayetleri de artmaya başlamıştır. Kullanıcıların internet veri kullanım miktarlarının fazla olması sebebiyle diğer kullanıcıların erişim hızlarının olumsuz etkilenmesinin önüne geçilebilmesi için uygulanmaya başlayan Adil Kullanım Noktası (AKN)[114] uygulamasında, yeniden düzenlemeye gidilerek bir süreliğine daha

[114] AKN, BTK'nın 01.09.2016 tarih ve 2016/DK-THD/393 sayılı Kararında *"bir kullanıcının internet veri kullanım miktarının belirli bir orana ulaşması sonrasında kullanıcının internet erişim hızının indirme*

uygulamanın devam etmesi, akabinde Kurul tarafından bu uygulamaya 31 Aralık 2018 tarihi itibariyla son verilmesi kararı[115] alınmıştır. Söz konusu karara rağmen AKN uygulamasına paketlerinde yer veren işletmeciler hakkında tüketicinin haklarının korunması çerçevesinde yaptırım uygulanmaktadır. BTK, bir kararında,[116] *""31.12.2018 tarihi itibarıyla AKN uygulamasına son verilmesi" hükmüne aykırı olarak, "... Aşmayan 10 GB" tarifesini kullanan abonelere, tarifelerinde belirlenmiş mobil veri kullanım sınırının aşılmasını müteakip hatta tanımlı başka mobil veri hakkı yok ise, hizmete ilişkin mobil veri kullanım hızını 256 Kbps'a düşürülerek devam ettirilmesi suretiyle Adil Kullanım Noktası (AKN) uygulamasına fiilen devam etmesi nedeniyle ... A.Ş.'nin; ... uyarılması"*na karar vermiştir.

Elektronik haberleşme sektörünün temelini oluşturan yetkilendirilmeksizin faaliyet gösterememe hususunda dahi tüketicinin mağdur edilmemesi ve haklarının korunması esas alınarak; EHK'nın 9/10 maddesinde *"... Kullanım hakkının iptal edildiği hallerde abonelerin menfaatlerini korumak için gerekli tedbirler alınır."* hükmüne yer verilmiştir. Ayrıca EHK'nın 14/1-(g) maddesi uyarınca, tarifelerin düzenlenmesi hususunda da tüketici menfaatinin ön planda olacağı belirtilmiştir. Aynı Kanun'un 16/3 maddesinde ise BTK'nın erişim ve arabağlantı yükümlülükleri konusundaki düzenlemeleri kamu menfaati için gerekli olması halinde sınırlandırabileceği hüküm altına alınmıştır.

Tüketici Hakları Yönetmeliği'nin 5. maddesinde tüketicilerin haklarından bahsedilerek buna aykırı davranan işletmecilerin abone şikayetlerinin cevaplanması süreçleri ise Tüketici Şikâyetlerinin İşletmeciler Tarafından Çözülmesine İlişkin Usul ve Esaslar[117] ile belirlenmiştir. İlgili düzenlemenin 6. maddesinde şikayette bulunan

---

(download) yönünde yeni fatura dönemine girilene kadar ya da paketin geçerli olduğu sürenin sonuna kadar azami olarak belirli bir erişim hızına düşürülmesi" şeklinde tanımlanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/adil-kullanim-noktasi-akn-uygulamasi.pdf , Erişim Tarihi: 22 Mart 2022.

[115] 27.12.2016 tarih ve 2016/DK-THD/518 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/adil-kullanim-noktasi-akn.pdf , Erişim Tarihi: 22 Mart 2022.

[116] 22.06.2021 tarih ve 2021/İK-ETD/169 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorunde-basvuru-sahibinin-kimliginin-dogrulanma-sureci-hakkinda-yonetmelik/169-2021-web.pdf , Erişim Tarihi: 22 Mart 2022.

[117] Tüketici Şikâyetlerinin İşletmeciler Tarafından Çözülmesine İlişkin Usul ve Esaslar, https://tuketici.btk.gov.tr/uploads/pages/usul-ve-esaslar/tuketici-sikayetlerinin-cozumune-iliskin-usul-esaslar.pdf , Erişim Tarihi: 22 Mart 2022.

abonenin, şikayet sürecine ilişkin bilgilendirilmesinin yanı sıra tüketici menfaatinin korunması amacıyla alınabilecek tedbirler hakkında da bilgilendirilmesi esas alınmıştır.

Yaşlı, engelli ve korunmaya muhtaç tüketicilerin özel ihtiyaçlarının göz önünde bulundurulmasıyla, söz konusu kişilere teknolojik yenilikler doğrultusunda elektronik haberleşme hizmetlerinden kolaylıkla faydalanabilmeleri için bazı düzenlemeler yapılmıştır. Bu doğrultuda Kurum tarafından işletmecilere Tüketici Hakları Yönetmeliği'nin 7. maddesinin 11. fıkrasıyla abonelik sözleşmesinin Braille alfabesiyle veya sesli olarak dinletilebilecek şekilde sunulması ve aynı Yönetmeliğin 14. maddesiyle uluslararası dolaşım hizmeti kullanılmaya başlandığında talepte bulunan aboneye sesli mesaj olarak bilgi verilmesi ve benzeri yükümlülükler getirilerek verilen hizmetlerle, tüketicilerin hak ve menfaatlerinin korunması amaçlanmıştır. BTK, bir Kurul kararında işletmecilerden, engellilere özel olarak hazırlanmış hizmetlerin internet sitesinde tek bir başlığın altında toplanması[118], bu kişilere ekonomik olarak avantaj sağlayan birtakım tarifelerin oluşturulması, GSM işletmecilerinin sesli konum bilgisi hizmetini engellilere ücretsiz olarak sağlamaları gerektiği ve benzeri uygulamaların geliştirilerek uygulanmaya başlanması yönünde karar vermiştir.[119]

Elektronik haberleşme sektöründeki serbestleşme ve sektördeki rekabetin her geçen gün artış göstermesi ile tüketiciler kolaylıkla sektörde faaliyet gösteren farklı işletmecilere yönelebilse de işletmeciler; elde ettikleri güçleri kötüye kullanmamaları için haksız sözleşme şartları, fiyatlama kriterleri, ayrıntılı fatura gönderilmesi, veri güvenliği ve gizliliğinin sağlanması, tüketicilerin bilgilendirilmesi ve şikayetlerinin dikkate alınması gibi hususlarda sürekli olarak düzenleyici ve denetleyici Kurum'un takibine maruz kalmaktadır.[120] Bu doğrultuda Kurum, işletmecileri şikayete bağlı veya resen denetleyebilmektedir. EHK'nın 59. maddesinde ve Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Yönetmelik'in[121] (Denetim Çalışmalarına İlişkin Yönetmelik) 9. maddesinde belirtildiği üzere, işletmeci denetim sırasında Kurum

---

[118] Türk Telekomünikasyon A.Ş., Engellilere Özel Hizmetler, https://www.turktelekom.com.tr/destek/engellilere-ozel-hizmetler , Erişim Tarihi: 22 Mart 2022.

[119] 06.01.2014 tarih ve 2014/DK-THD/25 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/engelli-tuketicilere-yonelik-duzenlemeler-konulu-kurul-karari.pdf , Erişim Tarihi: 22 Mart 2022.

[120] Güneş Koca, "Mukayeseli Açıdan Telekomünikasyon Hukukunda Tüketicinin Korunması," Telekomünikasyon Kurumu Uzmanlık Tezi, 2005: 18, https://www.btk.gov.tr/uploads/thesis/mukayeseli-acidan-telekomunikasyon-hukukunda-tuketicinin-korunmasi-duzenleyici-otoritelerin-rolu-alinmasi-gereken-tedbirler-olmasi-gereken-hukuk-acisindan-oneriler.PDF , Erişim Tarihi: 22 Mart 2022.

[121] R.G. 14.12.2011, S. 28142.

görevlileri ve varsa diğer kamu kurumu memurlarına ve kolluk kuvvetlerine kolaylık sağlamalı, gizli bilgi veya belge olduğu iddiası ileri sürülmeksizin istenilen her türlü evrakı süresi içerisinde sunmalı, sistemlerini denetlenebilir hale getirmelidir. Denetimler sırasında bahsi geçen yükümlülüklerini yerine getirmeyen işletmeciler hakkında İdari Yaptırımlar Yönetmeliği'nin 27. madde hükmü uyarınca, ilgili ihlalin gerçekleştiği tarihten önceki yıla ilişkin net satışın yüzde 3'üne kadar idari para cezası uygulanmaktadır. Bununla birlikte söz konusu işletmecinin, Kurum tarafından yetkilendirilmiş bir e-posta hizmet sağlayıcısı, denetim yapma konusunda yetkilendirilmiş işletmeci veya ölçüm konusunda yetkilendirilmiş bir işletmeci olması halinde ise ilgili izin ve ruhsatları da iptal edilebilmektedir.

İlgili hususlar çerçevesinde BTK bir kurul kararında,[122] EHK'nın ilkelerinden olan tüketicinin korunması ilkesine aykırı şekilde abonelerin onayı ve bilgisi olmadan hatlarına çeşitli hizmetleri tanımlaması, EHK'nın 60/9 maddesi uyarınca abonelerden alınan fazla ücretlerin iade edilmesine ve yine EHK'nın 59. maddesi ve Denetim Çalışmalarına İlişkin Yönetmelik'in 9/1-(b) maddesine aykırı şekilde çeşitli tarifeler hakkında eksik ve hiç bilgi verilmemesi nedeniyle işletmeci hakkında idari para cezası uygulanmasına karar vermiştir.

2.2. EŞİTLİK İLKESİ-AYRIM GÖZETMEME YÜKÜMLÜLÜĞÜ

Hukuk karşısında eşitlik, kamu makamlarının herhangi bir ayrım yapmadan herkese eşit şekilde davranması anlamına gelmektedir. Hukuk kurallarının mahiyetinin genel olması ve hukuki anlamda eşitlik ilkesi sayesinde toplum içerisinde ekonomik ve sosyal anlamda eşit olmayan bireyler, hayatlarını güvenli ve bilinmezlikten uzak şekilde idame ettirebilmektedir.[123]

Hukuk kurallarını uygulama yükümlülüğü olan idarenin, işlem ve eylemlerini gerçekleştirirken eşitlik ilkesine riayet etmesi zorunludur. Bilhassa takdir yetkisinin uygulanması gereken hallerde eşitlik ilkesine riayet edilememesi, gerçekleştirilen işlemin hukuka aykırı olmasına yol açar.[124]

---

[122] 17.10.2018 tarih ve 2018/İK-SDD/309 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/inceleme-vodafone-muhtelif-tuketici-sikayetleri/309-web.pdf , Erişim Tarihi: 23 Mart 2022.
[123] Akyılmaz, *Türk İdare Hukuku*, 87.
[124] Çağlayan, *İdare Hukuku Dersleri*, 112.

Eşitlik ilkesi doğrultusunda, idarenin ayrım gözetmeme yükümlülüğü olup; işlem ve eylemlerinde eşit muamele etme zorunluluğu vardır. Ancak idarenin eşitlik ilkesi mutlak eşitlik olmayıp; nispi (göreceli) eşitliktir. Diğer bir deyişle idarenin eşitlik kavramı, tüm bireylere aynı şekilde davranılması yerine hukuken aynı durumda olanlar ya da olması gerekenler arasında ayrım yapılmaması şeklinde anlaşılmaktadır.[125] Bu doğrultuda, durum veya konumları bakımından kişiler arasındaki farklılıklar sebebiyle farklı uygulamalar geliştirilmesi, eşitlik ilkesinin ihlal edildiği sonucunu ortaya çıkarmaz.[126] Dolayısıyla eşitlik ilkesi ile kanunların uygulanma sürecindeki etkileri ön plana çıkarılsa dahi bu ilke yalnızca hukuksal olarak eşit davranmaya ilişkin olup sosyal yaşama dair eşitsizlikleri değiştirmez.[127] Hukuki durumların ve bireylerin içinde bulunduğu şartların farklılıkları dikkate alındığında, hem yasama işlemleri hem de idari işlemlerin hukuka uygun sonuçlarının olmasını sağlamak ancak nispi eşitlik uygulamasıyla olabilir.[128]

Anayasa'nın 10. maddesinde düzenlenen eşitlik ilkesi, cinsiyet, inanç ve köken fark etmeden herkesin kanunlar karşısında eşitlikten yararlanabilmesini sağlamak için devletin gerekli tedbirleri alacağı, engellilere ve sosyal bakımdan desteğe ihtiyaç duyan kimselere yönelik alınacak olan tedbirlerin ise bu ilkeye aykırılık olarak kabul edilmeyeceği, kimseye ayrıcalık tanınmayacağı ve tüm bu hususlar çerçevesinde devletin tüm organ ve makamlarının gerçekleştirdikleri işlemlerinde eşitlik ilkesine riayet etmeleri gerektiği şeklinde açıklanmıştır.

Elektronik haberleşme sektörünü düzenleyen mevzuatta ise eşitlik ilkesine, ilk olarak mülga 406 sayılı Kanun'un 4. maddesinin (d) bendinde yer verilerek abone, kullanıcı ve işletmeci arasında fark gözetilmeden temel bir hak olan haberleşmenin eşitlik ilkesi çerçevesinde bireylere sunulması gerektiği belirtilmiştir. Ayrıca yine aynı Kanun'un 10. maddesinde arabağlantı yükümlüsü olan işletmecilerin kendi hizmetleri için gözettikleri hizmet kalitesinin aynısını arabağlantı yapmak isteyen diğer işletmeci için de karşılaması gerektiğine yer verilmiştir.

---

[125] Ali Ulusoy, *Yeni Türk İdare Hukuku*, (Ankara: Yetkin Yayınları, 2019), 103.
[126] Çağlayan, *İdare Hukuku Dersleri*, 111.
[127] Zafer Gören, "Genel Eşitlik İlkesi," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 22, no.3 (2016): 3285.
[128] Turan Yıldırım, Muhammed Göçgün, "İdarenin Düzenleyici İşlemlerinde Eşitlik İlkesi," *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 3, no.2 (2016): 43.

EHK'nın 4/1-(d) maddesinde, aksi şekilde davranmaya ilişkin objektif sebepler bulunmadığı sürece, ihtiyaç sahibi kimselere özel olarak sağlanan kolaylıklar dışında, benzer konumdaki kimseler arasında ayrım gözetilmeden elektronik haberleşme hizmetlerinin herkese eşit şekilde sunulması gerektiği vurgulanmıştır. Keza Tüketici Hakları Yönetmeliği'nin 5. maddesinde sayılan tüketicinin haklarından birisi de herkesin hizmetlere eşit olarak ulaşabilmesi ve hizmetlerin ücretlerinin adil olmasıdır. Aynı şekilde EHK'nın tarifelerle ilgili 14/1-(b) maddesinde benzer şekilde ayrım gözetmeme ilkesinden bahsedilmiştir.

Elektronik haberleşme sektöründe işletmecilere getirilen eşitlik ilkesi çerçevesinde ayrım gözetmeme yükümlülüğünün istisnası, engellilere ve sosyal bakımdan desteğe ihtiyaç duyan kimselere sağlanan sınırları ve kapsamı açıkça belirlenmiş olan ekonomik ve sosyal kolaylıklardır. Buna ilişkin Kurum tarafından çeşitli düzenlemeler yapılmıştır. Bunlardan en yenisi "Engelli, Gazi ve Şehit Yakınlarına Yönelik İndirimli İnternet Tarifelerinin Uygulama Esaslarının Güncellenmesi"[129] konulu düzenlemedir.

EHK'nın 16/5 maddesinde erişim yükümlüsü işletmeciler arasında eşitlik ilkesinin geçerli olduğu, 23. maddesinin 2. fıkrasında geçiş hakkı talebinde bulunan işletmeciler arasında kamu kurum ve kuruluşları tarafından ayrım gözetilmemesi gerektiği, 31. maddesinin 1. fıkrasında numara kaynaklarının verimli ve adil kullanımı çerçevesinde işletmecilere numara tahsisinin ayrım gözetilmeksizin yapılması, 47. maddesinin 1. fıkrasında işletmecilerin benzer konumdaki tüketicilere eşit davranması gerektiği ve 48. maddesinin 1. fıkrasında ise tüketici ve son kullanıcının haberleşme hizmetinden eşit koşullarda hizmet alabilmesine yönelik Kurum tarafından usul ve esasların belirlenebileceği düzenlenmiştir.

Ayrıca Tarife Yönetmeliği'nde[130] ilkelere yer verilen 5. maddede de eşitlik ilkesine değinilerek ilgili Yönetmeliğin 7/1-(c) maddesinde aynı ya da benzer nitelikte olan elektronik haberleşme hizmetleri için belirlenen tarifelerde son kullanıcılar arasında ayrım gözetilmemesinin esas olduğu belirtilmiştir.

---

[129] İlgili düzenleme, 23.07.2018 tarih ve 2018/DK-ETD/222 sayılı BTK Kurul Kararı ile yayımlanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/engelli-gazi-ve-sehit-yakinlarina-yonelik-indirimli-internet-tarifelerinin-uygulama-esaslarinin-guncellenmesi/222-02-engelli-gazi-ve-sehit-yakinlarina-yonelik-indirimli-internet-tarifelerinin-uyg-23-07-2018.pdf Erişim Tarihi: 23 Mart 2022.

[130] R.G. 12.11.2009, S. 27404.

Ayrım gözetmeme ilkesine aykırılık teşkil eden hallerde işletmecilere uygulanacak yaptırımları düzenleyen hükümlerden biri olan İdari Yaptırımlar Yönetmeliği'nin 11/1-(a) maddesinin 2 numaralı alt bendinde, tarifelerin yüksek fiyatlar veya işletmeciler arası rekabeti engelleyici fiyat indirimlerini içermesi, haksız sebeplerle tüketiciler arasında ayrıma sebep olunması ve bir hizmetin var olan maliyetinin bir başka hizmetin ücretiyle finanse edilmesi gibi çeşitli ihlallere sebep olunması durumunda, işletmeciye ihlalin gerçekleştirildiği yılın öncesindeki net satış tutarının yüzde 3'üne kadar idari para cezası uygulanması öngörülmüştür. Erişim ve arabağlantı konularında eşitlik ilkesine riayet etmeyen işletmeci hakkında ise İdari Yaptırımlar Yönetmeliği'nin 10/1-(b) maddesinin 2 numaralı alt bendi uyarınca, ihlalin gerçekleştirildiği yılın öncesindeki net satış tutarının yüzde 1'ine kadar idari para cezası uygulanmaktadır.

Eşitlik ilkesi doğrultusunda, işletmeciler ile aboneler arasındaki abonelik sürecinin başlangıcı olan abonelik sözleşmesinin kurulmasında, şablon nitelikteki sözleşmeyi önceden hazırlayıp aboneye sunan işletmeci, hizmeti sunan taraf olarak aboneye nazaran daha güçlü olduğundan; taraflar arasındaki eşitlik ilkesinin sağlanması adına Kurum tarafından aboneyi koruyan düzenlemeler ve kurul kararları ile işletmeciler karşısında aboneler korunmaya çalışılmaktadır. BTK konuyla ilgili bir kurul kararında,[131] işletmeci hakkında var olan iddiaların tespiti amacıyla fiber altyapısı olan devrelere ilişkin yapılan denetimde, EHK'nın 47/1 maddesi ve Tarife Yönetmeliği'nin 7/1-(c) maddesinde belirtilen ayrım gözetmeme ilkesine aykırı olacak şekilde haklı sebep olmadan bazı devrelere ücret tahakkuk ettirilmediği, bazılarının ücretlerinin eksik alındığı, bazılarında ise ücret tahakkukuna etki edecek olan gerçek mesafe verilerinin düşürüldüğünün tespit edilmesi sonucunda, İdari Yaptırımlar Yönetmeliği'nin 44. maddesi çerçevesinde işletmeci hakkında idari para cezası uygulanmasına karar vermiştir.

2.3. ŞEFFAFLIK İLKESİ

Yönetimde şeffaf olma ile bilgi edinme hakkı ve hukuk devleti, birbirini tamamlayan kavramlardır. Şeffaflık, bilgi edinme özgürlüğünün kaynağı anlamına gelirken bilgi edinme hakkı olmadan şeffaflık çerçevesinde hareket edilmesi de söz

[131] 19.11.2015 tarih ve 2015/DK-SDD/516 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/inceleme-turk-telekom-ayrim-gozetmeme.pdf , Erişim Tarihi: 24 Mart 2022.

konusu değildir. Bu iki tamamlayıcı kavramın, idarenin işlem ve eylemlerine hakim olması gerekmektedir.[132]

İdarenin hareketlerinin, toplumun alışkanlıklarının, elektronik haberleşme sektöründeki işletmecilerin şeffaflık ve bilgi edinme kavramlarına verdiği önem toplumun bütün paydaşlarının hukuka uygun hareket etmesi sonucunu doğuracaktır. Bu doğrultuda işletmeciler de belirli aralıklarla şeffaflığı sağladıklarına dair rapor yayınlayabilmektedir. Örneğin, bir İspanyol telekomünikasyon şirketi olan Telefonica, ifade özgürlüğü, kişisel verilerin korunması ve genel olarak insan haklarına bağlılık ve uyum açısından şeffaflığı teşvik etmek için her yıl Şeffaflık Raporu yayınlamaktadır.[133]

İşletmeciler, şeffaflık ilkesinin yerine getirilmesi için Kurum'un belirlediği yükümlülükler yanında tacir olmalarından kaynaklı TTK'nın ilgili hükümlerine de uygun hareket etmek zorundadır. TTK'nın 64. maddesi, ticari defter tutma yükümlülüğünden söz ederek her tacirin TTK'ya göre ticari defterlerini açıkça görülecek şekilde ortaya koyma mecburiyeti olduğunu vurgulamaktadır.

EHK'nın 4/1-(e) maddesinde yer verilen şeffaflık ilkesi doğrultusunda, aynı Kanun'un 49. maddesinde Kurum'un; işletmecilerden şeffaflık ilkesi çerçevesinde son kullanıcı, tüketici ve abonelerin menfaati için tarife, paketler ve hizmet kalitesine ilişkin bilgilendirmeleri yapmalarına ilişkin yükümlülük getirebileceği, abonelik sözleşmesinin kuruluşu aşamasında abone olacak kişinin tercihini değiştirmesine etki edebilecek durumlar hakkında dürüstlük kuralı çerçevesinde işletmecilerin gerekli bilgilendirmeyi yapmaları ve bu hususlar doğrultusunda gereken usul ve esasları belirleyeceğinden söz edilmektedir.

EHK'nın söz konusu 49. maddesinin ilk fıkrasında birey-devlet ilişkisi görülmektedir. Bu doğrultuda Kurum'un şeffaflık ilkesi çerçevesinde sınırlı sayı ilkesine bağlı olmadan işletmecilere aboneleri bilgilendirme kapsamında birtakım yükümlülükler getirebileceğine yer verilmiştir. EHK'nın 49.maddesinin ikinci fıkrasında ise birey-birey ilişkisi bağlamında özellikle abonelik kuruluşu aşamasında işletmeci ve abone arasındaki menfaat çatışması konu alınarak dürüstlük kuralı doğrultusunda görece daha korunmaya muhtaç taraf olan abonenin korunması için şeffaflık ilkesi çerçevesinde bilgilendirilmesi

[132] Adnan Küçük, "Hukukun Hakim Kılınmasının Bir Gereği Olarak İdari Şeffaflık ve Bilgi Edinme Hürriyeti," *Liberal Düşünce Dergisi* 22*,* no.86 (2017): 93.
[133] Son yayınlanan 2021 yılına ait Şeffaflık Raporu için bkz. https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/08/Report-on-Transparency-in-Communications-2021.pdf , 3, Erişim Tarihi: 24 Mart 2022.

gerektiğine yer verilmiştir. Ayrıca bahsi geçen hükümden, yalnızca abonelik sözleşmesine taraf olan abone değil, aboneliği kullanmakta olan son kullanıcının da aynı şekilde korunması için bilgilendirilmesi gerektiği anlaşılmaktadır.[134]

Ayrıca Tüketici Hakları Yönetmeliği'nin 6. madde hükmü ile; işletmeciler, elektronik haberleşme hizmeti sunacağı vakit, bilhassa abonenin hizmetleri seçtiği sırada ve sözleşme kuruluşu esnasında, tüketicinin karar vermesinde veya kararını değiştirmesinde etki edeceği düşünülen konular hakkında dürüstlük kuralı çerçevesinde, tüketicilerin elektronik haberleşme hizmetini kullanımı ve hizmete erişimi esnasında gerekli bilgilendirmeleri yapmak ve bu bilgilere kolayca erişimini sağlamakla yükümlü kılınmıştır. Bu çerçevede işletmeci; işletmeci unvanını ve adresini, sunduğu hizmetlere ilişkin kapsam ve kullanımı konusundaki genel şartlarını, tarifeleri ve bunların içerikleri, hizmetlerin ücretleri, aboneden taahhüt alınıyorsa buna ilişkin şartlar, işletmeci tarafından taahhüt edilen hizmet kalite seviyesinin sağlanamaması halinde abonenin zararının ne şekilde giderileceği ve tüketici şikayetlerinin çözümü süreci hakkında bilgilendirme yapmak zorundadır. İşletmeci, şikayet süreçlerinin yönetimi ve tarife, kampanya ve ücrete ilişkin genel hususlara yönelik bilgilendirmesinin[135] yanı sıra abonelik feshi gibi konular hakkında tüketicilerin bilgilendirilmesi açısından bir internet sitesi kurmakla yükümlendirilmiştir.[136]

---

[134] Mesut Serdar Çekin, "Telekomünikasyon Sektöründe Şeffaflık İlkesi ve Sağlayıcının Bilgilendirme Yükümlülüğü," iç. *Telekomünikasyon Hukuku,* ed. Halil Akkanat, (İstanbul: Filiz Kitabevi, 2017), 88-89.

[135] BTK, 16.03.2021 tarih ve 2021/İK-THD/76 sayılı Kurul Kararının 3. ve 4. sayılı paragraflarında, Tüketici Hakları Yönetmeliği'nin 12/2 maddesi uyarınca taahhütnamelerde bulunması gereken aylık indirimli hizmet ücreti, taahhüdün süresi, varsa cihaz bedeli gibi taahhüde ilişkin olması gereken bilgileri taahhütnamesinde belirtmeyen işletmeci hakkında İdari Yaptırımlar Yönetmeliği'nin 12/3 maddesi uyarınca idari para cezası uygulanmasına ve yine Tüketici Hakları Yönetmeliği'nin 12/3 maddesinde belirtilen aboneden sesli onay alınarak başlatılan taahhütlerde, aynı madde hükmünün 2.fıkrasında yer verilen hususlar hakkındaki bilgilendirmenin yine sesli olarak aboneye yapılması gerektiği, kısa mesaj ile alınan taahhütlerde ise bilgilendirmenin kısa mesaj ile yapılması gerekmesine rağmen işletmecinin hem kısa mesaj hem de çağrı merkeziyle almış olduğu taahhütlerde söz konusu bilgilendirme yükümlülüğünü yerine getirmediği için yine İdari Yaptırımlar Yönetmeliği'nin 12/3 ve 44. maddeleri doğrultusunda idari para cezası uygulanmasına karar verilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-tuketici-haklarina-iliskin-mevzuat-ihlali-katlama-kampanyasi-turkcell/76-2021-web.pdf , Erişim Tarihi: 25 Mart 2022.

[136] Tüm işletmecilere getirilen internet sitesinde bilgilendirme yapma yükümlülüğü, mobil işletmecilere 27.01.2010 tarihinde BTK'nın 2010/DK-10/49 sayılı Kurul Kararı ile Avrupa Birliği Düzenleyici Grubu tarafından hazırlanan rapor ve şeffaflık ilkesi çerçevesinde tüketici lehine düzenlemelerin artırılması amacıyla, mobil işletmecilere tarifelerinin ücret ve içeriğine ilişkin bilgilerini internet sayfaları üzerinden yayınlayarak tüketicilere bilgilendirme yapma yükümlülüğü getirilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/mobil-elektronik-haberlesme-sektorunde-seffafligin-saglanmasi.pdf , Erişim Tarihi: 25 Mart 2022.

İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) maddesinin 4 numaralı alt bendinde şeffaflık ilkesi çerçevesinde bilgilendirme yükümlülüğünü yerine getirmeyen işletmeci hakkında, ihlalin gerçekleştiği tarihten önceki yıla ait net satışın yüzde 2'sine kadar idari para cezası uygulanması öngörülmüştür.

BTK bir kurul kararında,[137] Tüketici Hakları Yönetmeliği'nin 6/1 maddesine aykırı şekilde, çözüm ortağının internet sitesi ve müşteri hizmetleri vasıtasıyla tüketicileri yanlış bilgilendiren işletmeci hakkında İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) maddesinin 4 numaralı alt bendi ve 44. maddesi gereğince idari para ceza uygulanmasına karar vermiştir.

Son olarak Kurum tarafından her yıl, sektörde o yılın her çeyreğinde yaşanan gelişmeleri şeffaflık ilkesi çerçevesinde duyurabilmek adına Pazar Analizi Rapor'ları[138] yayınlamaktadır. İlgili rapora esas olan istatistiki bilgileri, işletmecilerden üçer aylık dönemlerde İşletmeci Veri Formları'yla alan Kurum,[139] söz konusu bilgiler çerçevesinde ve sektördeki diğer gelişmeler doğrultusunda rapor haline getirmektedir.

2.4. SERBEST REKABET ORTAMININ SAĞLANMASI VE KORUNMASI İLKESİ

Ülkemizde uzun süreler, elektronik haberleşme sektöründe sunulan hizmetlerin kamu hizmeti niteliğini haiz olması sebebiyle kamu hizmetini yalnızca devletin kendi eliyle yürütebilmesi anlayışı doğrultusunda hareket edilerek sektörün rekabete açılmasına karşı olan bir düşünce hakim olmuştur.[140] Dünya çapında genel olarak her işi devletin kendisinin yerine getirmesinin ekonomik açıdan devleti zorladığı düşüncesinin yayılmasıyla, çoğu sektördeki aktörlerin artmasıyla ve devletin genellikle hakem rolünü

---

[137] 22.07.2020 tarih ve 2020/İK-THD/210 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-tuketici-sikayetleri-vodafone-net/210-2020-web.pdf , Erişim Tarihi: 25 Mart 2022.

[138] BTK tarafından yayınlanan tüm Pazar Analizi Raporları'na https://www.btk.gov.tr/pazar-verileri url adresinden ulaşılabilir. Erişim Tarihi: 1 Nisan 2022.

[139] EHK'nın 12/2-(f) maddesinde yer verilen, işletmecinin *"Kuruma bilgi ve belge verilmesi"* yükümlülüğü kapsamında; işletmeciler üçer aylık dönemlerde Kurum tarafından verilen talimat doğrultusunda, işletmeci veri formlarını doldurarak Kurum'a göndermektedir. (BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, İşletmeci Veri Formunun Doldurulmasına Yönelik Kılavuz, 1, 8, https://www.btk.gov.tr/uploads/pages/isletmeci-veri-formlari/isletmeci-veri-formu-doldurma-kilavuzu-final1.pdf , Erişim Tarihi: 1 Nisan 2022.)

[140] Ali Ulusoy, *Telekomünikasyon Hukuku*, (Ankara: Turhan Kitabevi, 2002), 142-143.

üstlenmeye başlamasıyla beraber oluşan rekabetin etkisiyle sunulan hizmetlerdeki kalite artarak piyasalardaki fiyatlarda da azalma yaşanmıştır.[141]

Anayasa'nın 48. maddesinde belirtilen özel teşebbüs kurma serbestisi, milli ekonominin gereği ve sosyal amaçlar doğrultusunda devletin özel teşebbüslerin çalışmalarına yönelik tedbirleri alması hususundaki hüküm çerçevesinde ve 2002/77/EC sayılı Elektronik Haberleşme Şebeke ve Hizmetleri Piyasasında Rekabet Direktifi[142] gibi AB düzenlemelerine uyum sağlanması amacıyla, elektronik haberleşme sektöründe serbest rekabet ortamının sağlanmak istenmesi sonucunda yeni düzenlemeler yapılmıştır. Kamu hizmeti kavramına aykırı olduğu düşünülen serbest rekabet ilkesinin, kamu hizmeti mahiyetindeki elektronik haberleşme sektörüne ilişkin ilkelerin en önemlilerinden biri olmasıyla birlikte, faaliyet gösteren işletmeci sayısında artış yaşanması yönünde devletin yaklaşımıyla beraber, hizmet kalitesi ve fiyatlandırmasında rekabet sağlanabilir hale gelmiştir.[143]

EHK'nın 5/1-(b) maddesinde, elektronik haberleşme sektöründe bilgi toplumuna dönüşme, serbest ve etkin rekabet ortamının sağlanması doğrultusunda Bakanlığın gerekli politikaları belirleyerek tedbirleri alma görevi olduğuna yer verilmiştir. Aynı şekilde BTK'ya verilen görevler arasında da EHK'nın 6/1-(a) maddesinde belirtildiği üzere, etkin rekabetin sağlanabilmesi amacıyla rekabete engel olan uygulamalara son vererek bu konuyla ilgili etkin piyasa gücüne sahip işletmecilere ve diğer işletmecilere yükümlülük getirmesi hususu sayılmıştır.

Herkesin haberleşme özgürlüğü olduğuna dair Anayasa'nın 22. madde hükmü gereğince, makul ücret karşılığında bundan faydalanabilmesine imkan sağlanması gerekmektedir. Söz konusu haberleşme özgürlüğünü teminen EHK'nın 4/1-(ç) maddesinde uygun ücret karşılığında herkesin haberleşme hizmetlerinden yararlanabilmesi amacıyla teşvik edici uygulamaların artırılması ilkesi benimsenmiştir.

2003 yılı sonlarına doğru tekelleşmenin kaldırılarak serbest rekabet ortamının sağlanmaya çalışıldığı elektronik haberleşme sektöründe, yeni bir kanuna ihtiyaç duyulması ile, serbest rekabet ortamını sağlayacak olan sektöre yeni giriş yapan aktörlerin, diğer bir deyişle işletmecilerin yetkilendirilmesi hususunda yayımlanan 5809

[141] Aytaç Yüksel, *Elektronik Haberleşme Hukukundaki İdari Yaptırımlar ve Yargısal Denetimi*, (Ankara: Adalet Yayınevi, 2018), 27-28; Ekici, *Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)*, 18.
[142] Directive 2002/77/EC, *EUR-Lex*, Erişim Tarihi: 1 Nisan 2022.
[143] Ekici, *Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)*, 18-20.

sayılı EHK tasarısı ve gerekçesinde,[144] EHK'nın *"Elektronik haberleşme hizmetlerinin yetkilendirilmesi"* başlıklı 8. maddenin gerekçelerinden biri de tüketicilerin uygun ücretler ile belirli kalitede hizmet alabilmesinin mümkün kılınması olarak belirtilmiştir. EHK'da benimsenen temel ilkeler çerçevesinde faaliyetlerini sürdüren teşebbüsler, serbest ve etkin rekabeti sağlamak ve korumak ilkesine riayet ederek piyasa fiyatlarını belirleyebilmektedir.[145] Sektörde serbest rekabetin sağlanması sayesinde hizmetlerin birden fazla işletmeci tarafından sunulabilmesiyle tüketiciler daha makul fiyatlarla aynı kalitede hizmetten faydalanabilmeye başlamıştır.

EHK'da rekabete ilişkin düzenlenen bir diğer hüküm ise *"Rekabetin sağlanması"* başlıklı 7. maddedir. İlgili maddede BTK, resen veya şikayete bağlı olarak elektronik haberleşme sektöründe rekabete aykırı olduğu düşünülen uygulamaları inceleme ve gerekli tedbirleri almaya yetkili kılınmıştır. Ayrıca sektördeki işletmecilerin birleşme ve devralmalarına yönelik Rekabet Kurulu tarafından verilecek kararlarda ise BTK'nın görüşlerinin ve düzenlemelerinin öncelikle dikkate alınacağı belirtilmiştir.

EHK'nın 7. maddesinin 3. fıkrasında Kurum'a, elektronik haberleşme sektöründe rekabetin sağlanarak korunması maksadıyla yetki verildiği görülmektedir. Bu doğrultuda BTK, etkin piyasa gücüne (EPG)[146] sahip işletmecileri belirleyerek[147] yükümlülükler getirebilmektedir.[148]

---

[144] 17.10.2005 tarihinde yayımlanan Elektronik Haberleşme Kanunu Tasarısı ile Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu Raporu (1/1120), https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss1057m.htm , Erişim Tarihi: 1 Nisan 2022.

[145] Çekin, "Telekomünikasyon Sektöründe Şeffaflık İlkesi ve Sağlayıcının Bilgilendirme Yükümlülüğü," 80.

[146] EHK'nın 3/1-(r) maddesinde belirtildiği üzere etkin piyasa gücü, elektronik haberleşme sektöründe işletmecinin kendi başına veya başka bir işletmeciyle birlikte diğer işletmeci, kullanıcı veya tüketicilerden bağımsız şekilde davranabilmesine olanak sağlayan ekonomik güç anlamına gelmektedir.

[147] Örneğin, BTK'nın 17.02.2010 tarih ve 2010/DK-10/103 sayılı Kurul Kararı ile Türk Telekomünikasyon A.Ş., sabit şebekede çağrının taşınması piyasasında EPG'ye sahip işletmeci olarak belirlenmiştir. https://www.btk.gov.tr/uploads/boarddecisions/turk-telekomunikasyon-a-s-nin-sabit-sebekede-cagri-tasima-piyasasinda-etkin-piyasa-gucune-sahip-isletmeci-olarak-belirlenmesi.pdf , Erişim Tarihi: 1 Nisan 2022.

[148] BTK'nın EPG'ye sahip işletmecilere getirdiği yükümlülüklere örnek olarak, EPG'ye sahip işletmecilerin bir takım telekomünikasyon hizmetlerine dair tarifelerinde tavan fiyat esasına göre onaylanması hususu ve buna ilişkin ayrıntılara yer verilerek yayımlanan, *"Sabit Telefon Şebekesine Erişim veya Sabit Şebeke Üzerinden Arama Hizmetlerine Yönelik İlgili Piyasalarda Etkin Piyasa Gücüne Sahip İşletmecilerin Bazı Hizmetlerine İlişkin Tarifelerin Tavan Fiyat Yöntemi İle Onaylanmasına Yönelik Usul ve Esaslara İlişkin Tebliğ"* gösterilebilir. (R.G. 16.01.2007, S.26405) Keza etkin piyasa gücüne sahip işletmecilere getirilen yükümlülüklere yer verilen bir başka düzenleme olan *"Elektronik Haberleşme Sektöründe Etkin Piyasa Gücüne Sahip İşletmeciler ile Bu İşletmecilere Getirilecek Yükümlülüklerin Belirlenmesi Hakkında Yönetmelik"* (R.G. 01.09.2009, S. 27336) ise yürürlükten kaldırılmıştır.

Ayrıca işletmecilerin kullanıcılarının arasında haberleşmenin sağlanabilmesi için gerekli olan arabağlantının[149] tamamlanabilmesi adına işletmeciler arasında arabağlantı sözleşmeleri imzalanmaktadır. Söz konusu arabağlantı sözleşmeleri genellikle devlet ile imtiyaz sözleşmesi imzalamış olan EPG'ye sahip güçlü konumdaki işletmeciler ile piyasaya yeni giriş yapmış olan görece daha küçük işletmeciler arasında imzalanmaktadır. Bu durum ile, arabağlantı için ücretlerin yüksek tutulması veya yeterli arabağlantı kapasitesi oluşturulmaması gibi çeşitli faaliyetler ile yeni işletmecilerin piyasaya girişi engellenmek istenmektedir.[150]

Her ne kadar arabağlantı kurmak isteyen her iki işletmecinin de ticari faaliyet yerine getiren şirket olarak temel amaçları kar elde etmek olsa da hem EHK'daki rekabete ilişkin hükümler hem de daha genel nitelikte olan TTK'nın rekabete ilişkin hükümlerinden biri olan 54. maddesi ve devamında belirtilen rakipler arasında aldatıcı ve dürüstlük kuralına aykırı uygulamaların hukuka aykırı olacağına ilişkin hükümler ve 4054 sayılı Rekabetin Korunması Hakkında Kanun[151] hükümleri uyarınca; Kurum tarafından Referans Arabağlantı Teklifi (RAT),[152] Referans Ortak Yerleşim ve Tesis Paylaşımı Teklifi,[153] Referans Kiralık Devre ve Referans Al-Sat Yöntemiyle ATM/FR/ME İnternet

---

[149] Arabağlantı, EHK'nın 3/1-(e) maddesinde belirtildiği üzere, bir işletmecinin kullanıcılarının bir başka işletmecinin kullanıcısıyla haberleşebilmesi ve hizmetlerinden faydalanabilmesi amacıyla aynı ya da farklı işletmecilerin şebekelerinin fiziksel ve mantıksal bağlanmalarını ifade eder.

[150] InfoDev, *Telecommunications Regulation Handbook Module 3 Interconnection,* ed. Hank Intven, (Washington, The World Bank, 2000), 1.

[151] R.G. 13.12.1994, S. 22140.

[152] BTK'nın 08.06.2021 tarih ve 2021/DK-ETD/151 sayılı Kurul Kararı ile (https://www.btk.gov.tr/uploads/boarddecisions/mobil-cagri-sonlandirma-ucretleri/151-2021-web.pdf , Erişim Tarihi: 3 Nisan 2022.) güncellenen RAT'ların genel olarak amacı, Türk Telekomünikasyon A.Ş. RAT'ın 1.1.2.maddesinde yer aldığı üzere, mevzuat doğrultusunda işletmecilerin şebekeleri arasında elektronik haberleşme trafiğinin kurulması amacıyla şebekelerin birbirine bağlantısının sağlanmasına yönelik hususlara yer verilmesidir. Türk Telekomünikasyon A.Ş. RAT, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/turk-telekom-rat-22-02-2022.pdf , Erişim Tarihi: 3 Nisan 2022; Vodafone Telekomünikasyon A.Ş. RAT, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/vodafone-rat-08-06-2021.pdf , Erişim Tarihi: 3 Nisan 2022; Turkcell İletişim Hizmetleri A.Ş. RAT, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/turkcell-rat-08-06-2021.pdf , Erişim Tarihi: 3 Nisan 2022; TT Mobil İletişim Hizmetleri A.Ş. RAT, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/tt-mobil-rat-08-06-2021.pdf , Erişim Tarihi: 3 Nisan 2022.

[153] BTK'nın 17.06.2014 tarih ve 2014/DK-ETD/324 sayılı Kurul Kararı (https://www.btk.gov.tr/uploads/boarddecisions/referans-tesis-paylasimi-ve-aydinlatilmamis-fiber-teklifi.pdf) ile güncellenen Türk Telekomünikasyon A.Ş. Referans Ortak Yerleşim ve Tesis Paylaşımı Teklifi'nin 1.2.1. maddesinde belirtildiği üzere bu teklifin amacı, Türk Telekom'un altyapısı üzerinden yer kullanımı, bina içi bağlantı, enerji gibi hizmetlerden yararlanmak isteyen diğer işletmecilerin taleplerinin karşılanmasına ilişkin hususların açıklanmasıdır. https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/roytept-27-04-2014-tarihli-kk-geregi-05-05-2016.pdf , Erişim Tarihi: 3 Nisan 2022.

Toptan Satış Teklifleri (RAFMET)[154] ve benzeri referans teklifler yayımlanarak; işletmeciler arasında imzalanacak olan arabağlantı sözleşmelerinin bu tekliflere uygun olması şartı getirilmiştir. Sözleşme maddelerinin görüşüldüğü süreçte, ilgili tekliflere aykırı olan hükümlerin söz konusu olması halinde, işletmeciler öncelikle müzakere yoluyla çözüme ulaşmaya çalışır. İşletmecilerin kendi aralarında çözülemeyen konularda ise taraflar uzlaştırma için Kurum'a başvurabilirler. Arabağlantıya ilişkin böyle durumlarda BTK, mevzuat ve Kurum düzenlemeleri çerçevesinde uzlaştırma süreçlerini[155] yürüterek sözleşme hükümlerinin RAT ve benzeri tekliflere uygun olacak şekilde düzeltilmesine karar vererek anlaşmazlık olan hususlarda bu süreçten sonra nasıl hareket edileceğini belirlemektedir.[156] Böylece sektöre yeni giriş yapan işletmecilerin görece daha avantajlı konumda olan etkin piyasa gücüne sahip işletmeciler karşısında korunması amaçlanmıştır.

2.5. HİZMET KALİTESİ ARTIRIMININ TEŞVİK EDİLMESİ İLKESİ

İnternet üzerinden hizmet sunumu ve bu hizmetin takibi, geleneksel hizmet sunumu olarak adlandırılan yüz yüze karşılaşmalardan farklı olduğundan, rekabete ayak

---

[154] BTK'nın 22.02.2022 tarih ve 2022/DK-ETD/53 sayılı Kurul Kararı (https://www.btk.gov.tr/uploads/boarddecisions/referans-teklif-degisiklikleri-kimlik-dogrulama-yonetmeligi/53-2022-web.pdf) ile güncellenen Türk Telekomünikasyon A.Ş. RAFMET'in 1.2. maddesinde bu teklifin amacının, Türk Telekom'un diğer işletmeciye Al-Sat Yöntemi ile ATM/FR/ME İnternet Hizmetlerini sunabilmesi için gereken hususların belirlenmesi olduğuna yer verilmiştir. https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/rafmet-22-02-2022-53.pdf , Erişim Tarihi: 3 Nisan 2022.

[155] EHK'nın 18. maddesinde belirtildiği üzere, arabağlantı müzakerelerini yürüten işletmeciler arasında anlaşmanın iki ay içerisinde sağlanamadığı hallerde, işletmecilerden birinin BTK'ya başvurması halinde, BTK'nın sürece dahil olarak kamu menfaati için ücret de dahil olmak üzere anlaşılamayan konular hakkında tedbir almaya veya uzlaştırma talebini reddetme yetkisi bulunmaktadır. Bu yetki çerçevesinde BTK iki ay içinde, anlaşma sağlanamayan ücret veya sözleşme maddeleri gibi hususları belirleyebilmektedir. Bunun akabinde, belirlenen hükümler çerçevesinde imzalanan arabağlantı sözleşmeleri işletmeciler tarafından BTK'ya sunulur ve Kurum'un mevzuata aykırılık tespit etmesi halinde ise işletmecilerden değişiklik yapmasını isteme yetkisi bulunmaktadır.

[156] BTK'nın 14.12.2016 tarih ve 2016/UK-ETD/490 sayılı Kurul Kararı'nda işletmecilerden biri, Toptan Hat Kiralama (THK) abonelerinin Yerel Ağın Paylaşıma Açılması (YAPA) erişim metoduna geçiş işlemlerinde, bir günde yapılabilecek geçiş sayısı ve bu işleme ilişkin ücretin belirlenmesi konusunda Referans Yerel Ağa Ayrıştırılmış Erişim Teklifi'ne uygun olan taleplerinin EPG'ye sahip işletmeci tarafından karşılamaması sebebiyle, Kurum'dan uzlaştırma talep etmiş olup; BTK tarafından Teklif'e uygun karar verilmiş ve her iki tarafın bu karara uymaları istenmiştir. https://www.btk.gov.tr/uploads/boarddecisions/uzlastirma-turknet-ile-turk-telekom.pdf , Erişim Tarihi: 3 Nisan 2022.

BTK, 05.09.2012 tarih ve 2012/DK-07/415 sayılı bir başka kararında ise arabağlantı sürecinde olan işletmeciler arasında müzakere yoluyla çözülemeyen sözleşme hükümlerinin nasıl olacağına karar vererek uzlaşmayı sağlamıştır. https://www.btk.gov.tr/uploads/boarddecisions/netgsm-ile-vodafone-net-ve-netgsm-ile-vodafone-alternatif-arasinda-isletilen-uzlastirma-prosedurleri.pdf , Erişim Tarihi: 3 Nisan 2022.

uydurmak ve internet üzerinden müşterilere daha iyi hizmet sunmak adına yeni stratejilerin benimsenmesi gerekliliği elzem hale gelmiştir. İnternet üzerinden sunulan hizmetlerin kullanımı benimsendikçe, geleneksel anlamda hizmet kalitesinin ölçülmesine ilişkin metotlar yetersiz kalmaya başlamıştır. Bu durumun farkına varan şirketler, öncelikli olarak internet üzerinden verilen hizmet kalitesinin ölçümü için güvenlik, kullanım kolaylığı, mahremiyet, internet sitesinin kullanıcı dostu olması gibi çeşitli konularda yeni stratejiler belirlemeye başlamıştır.[157]

İnternet sitesi üzerinden hizmet veren bir işletme; öncelikle internet sitesine erişim ve erişim hızı, kullanım kolaylığı gibi aboneye/kullanıcıya elektronik ortamdaki verimliliği artıcı çalışmaları yapmalıdır. Hizmet sağlayıcı işletmelerin, internet sitesi üzerinden verilen hizmete yönelik taahhütleri ne ölçüde yerine getirdiği de abone ile güvenilirlik ilişkisinin kurulmasına yardımcı olur. İşletmecilerin sistemlerinin kullanılabilir olması, gizlilik ve güvenlik ilkelerine riayet edilerek başta finansal işlemlerin korunması, hizmetin kesintisiz olarak sunulması, yaşanabilecek problemler karşısında geri dönüşlerin etkin bir şekilde sağlanması ve sorunlar karşısında abone hassasiyetlerine duyarlı olunması, gerektiğinde telefon ya da çevrimiçi temsilciler vasıtasıyla yardım kanallarının oluşturularak aboneyle irtibat sağlanması, hizmet kalitesinin artırılmasına yönelik önemli hususlar olarak dikkat çekmektedir. Elektronik haberleşme sektöründe internet üzerinden verilen hizmetlere yönelik kalite ölçümünün, hizmetin tamamen elektronik tabanlı olması ve teknolojinin her geçen gün ileriye gitmesi, hizmet kalitesinin belirlenmesine yönelik ilkeler ve kategorilerin de düzenli olarak güncellenmesini gerektirmektedir.[158] Uluslararası Telekomünikasyon Birliği'nin hizmet kalitesi ile ilgili tanımlara yer verdiği E.800 metninde[159] hizmet kalitesinin ölçümünde ele alınan kriterler; hız, doğruluk, güvenilirlik, kullanılabilir durumda olması, belirtilen sürede hizmetin yerine getirilmesi, kullanım kolaylığı olmak üzere altı başlık halinde belirtilmiştir.

EHK'nın 4/1-(ğ) maddesinde, hizmet kalitesinin artırımı hususunda işletmecilerin teşvik edilmesi, Kurum tarafından yapılacak olan düzenlemelerde dikkate alınması

---

[157] Sadaf Firdous, Rahela Farooqi, *Service Quality To E-Service Quality: A Paradigm Shift*, (Bangkok: Industrial Engineering and Operations Management Society International-IEOM, 2019), 1662, http://www.ieomsociety.org/ieom2019/papers/404.pdf , Erişim Tarihi: 10 Nisan 2022.
[158] Firdous, *Service Quality To E-Service Quality: A Paradigm Shift*, 1663.
[159] ITU, E.800 Definitions of Terms Related to Quality Of Service, 7, https://www.itu.int/rec/T-REC-E.800-200809-I/en , Erişim Tarihi: 10 Nisan 2022.

gereken ilkelerden bir diğeri olarak gösterilmiştir. Bu doğrultuda, EHK 6/1-(u) maddesinde Kurumun görevlerinden biri olarak hizmet kalitesine ilişkin gerekli denetimleri yapmak ve uyulması gereken standartları belirlemek adına usul ve esasları yayımlamak sayılmıştır. Ayrıca işletmecilere hizmet kalitesi standartlarına uyum sağlamak, yükümlülük olarak getirilerek bu doğrultuda EHK'nın 50. maddesinin 1. fıkrasıyla, abonelik sözleşmelerinde hizmet kalitesi seviyeleri hakkında bilgi vererek bu seviyenin sağlanamaması halinde tazminat ya da iadeye ilişkin hükümlerin bulunması gerektiği vurgulanmıştır.

Ayrıca EHK'nın 52. maddesinde, işletmeciler tarafından tüketici ve son kullanıcılara verilen bilgilerin doğruluğu amacıyla hizmet kalitesi seviyelerine ilişkin ölçütlerin Kurum tarafından belirleneceği, belirlenen bu ölçütlere işletmeciler tarafından uyum sağlama yükümlülüğü olduğu, işletmecilerden elektronik haberleşme sektöründe sunulan hizmetlere ve altyapıya ilişkin hususlarda hizmet seviyesi taahhütleri hazırlamaları istenebileceği, doğru faturalama yapma ve faturanın içeriğinin mevzuata uygunluğunun hizmet kalitesine ilişkin önemine yer verilmiştir.

Hizmet kalitesine ilişkin belirlenen standartların ne olduğuna ilişkin ise Elektronik Haberleşme Sektöründe Hizmet Kalitesi Yönetmeliği[160] (Hizmet Kalitesi Yönetmeliği) yayımlanmıştır. İlgili Yönetmelik ekinde bulunan ve işletmeciler tarafından verilen hizmetlere ilişkin müşteri hizmetlerinin çağrıya cevap verme süresinden, tüketicinin şikayetinin giderilme süresine kadar ayrıntılı hazırlanması gereken hizmet kalitesine ilişkin raporları, üç ayda bir BTK'ya bildirmeleri istenilmiştir.[161] Böylece herkesin elektronik haberleşme hizmetine ulaşmasının önemli olması kadar, verilen hizmetin uluslararası standartlara uygun şekilde sunulması da aynı ölçüde önem teşkil etmektedir. Bu doğrultuda, işletmeciler tarafından sunulan hizmetlere ilişkin Kurum tarafından hizmet kalitesinin takibi yapılmaktadır. BTK bir kararında,[162] hizmet kalitesi bildiriminde bulunan işletmecinin, müşteri hizmetlerinin aboneye 20 saniye içerisinde cevap verme

[160] R.G. 12.09.2010, S. 27697.
[161] Hizmet Kalitesi Yönetmeliği'nin 7.maddesinde ilgili raporların hangi zamanlarda Kurum'a sunulması gerektiğine yer verilmiştir.
[162] BTK, 28.12.2021 tarih ve 2021/İK-THD/408 sayılı Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-2020-yili-birinci-ceyrek-donem-cagri-merkezi-hizmetine-iliskin-hizmet-kalitesi-yukumlulukleri-ttnet-turkcell-vodafone-millenicom-andromeda/408-2021-web.pdf , Erişim Tarihi: 12 Nisan 2022.

süresi[163] kriteri için belirlenen hizmet kalitesi ölçütü olan %80 hedefine ulaşamadığı gerekçesiyle uyarılmasına ve ilgili hizmet kalitesi kriterini sağlayamadığı bilgisine internet sayfasında yer verilmesine karar vermiştir.

2.6. DEĞİŞKENLİK (UYARLANMA) İLKESİ

Kamu hizmeti, değişken niteliktedir. Toplumun gereksinimlerinin farklılaşması ve teknolojinin gelişimiyle birlikte uyarlanmaktadır. Kamu hizmetlerinin toplum yararı hedeflenerek ifa edilmesi esas olup değişkenlikler nedeniyle bireyler bu durumdan olumsuz etkilense dahi uyum sağlamak zorunda kalabilmektedir. Kamu hizmetinin farklılaşarak yürütülmesine örnek olarak geçmişten günümüze daktilo kullanımının yerini bilgisayara bırakması, fiziki ortamda tutulan belgelerin dijital ortama aktarılması, çeşitli kurum ve kuruluşlara yerinde yapılan başvuruların e-Devlet üzerinden elektronik ortamda yapılabilir hale getirmeyi mümkün kılan uygulamalar vasıtasıyla yapılabilmesi, elektronik imzaların her geçen gün yaygınlaşması, COVID-19 pandemisi sebebiyle eğitim faaliyetlerinin çevrimiçi şekilde yürütülmesi ve devam eden süreçte uzaktan eğitim ve çalışmanın mümkün olduğu konusunda toplumun genelinde farkındalık oluşması gösterilebilir.[164]

Elektronik haberleşme sektöründe hizmet veren işletmeciler de toplumun gereksinimlerine uygun olarak, sundukları hizmetleri uyarlamalıdır. Abonelere birden fazla dil erişimi sunulması, ayrıntılı faturalar ile abonelerin aldıkları hizmetin içeriği hakkında bilgilenmelerinin sağlanması, abonelere çevrimiçi verilen desteklerle abonelerin taleplerinin karşılanması ve benzeri faaliyetlerle işletmecilerin sundukları hizmetleri gelişmelere uygun şekilde uyarlamalarının hizmet kalitesini de artırdığı sonucuna ulaşılmaktadır.[165] Dolayısıyla tüketicinin hak ve menfaatlerinin korunması açısından işletmeci tarafından tüketicinin ihtiyacını karşılamayan bir hizmet sunumunda ısrarcı olunmaması, değişkenliklere uyum sağlanması gerekmektedir.

---

[163] Hizmet Kalitesi Yönetmeliği'nin eklerinde yer verilen "EK-4 Son Kullanıcılara Hizmet Veren İşletmeciler" başlıklı tabloda ilgili kriter yer almaktadır.
[164] Sancakdar, *İdare Hukuku*, 560-561.
[165] Vivian Witkind Davis, David Landsbergen, Raymond W. Lawton, Larry Blank, Nancy Zearfoss, John Hoag, *Telecommunications Service Quality,* (Ohio: The National Regulatory Research Institute, 1996), 28, https://ipu.msu.edu/wp-content/uploads/2016/12/Davis-Telecom-Service-Quality-96-11-Mar-96.pdf , Erişim Tarihi: 12 Nisan 2022.

Ayrıca teknolojik gelişmelerin takibi ve ülke içerisinde uygulanması bakımından hem üretim hem de hukuki altyapının eş zamanlı şekilde hazırlanması gerekmektedir. Aksi takdirde, teknolojik gelişme sebebiyle ortaya çıkan hukuki uyuşmazlıklara gelişen teknolojiyle uyumlu olmayan bir mevzuat ile cevap verilmek zorunda kalınmakta gerçek anlamda hukuken koruma sağlanamamaktadır. Örneğin, Avrupa Birliği'nde 1996 yılında çıkan direktifle kişisel verilerin korunması konusu ele alınmışken ülkemizde bunun uygulanabilirliği ancak 2016 yılında yayımlanan KVKK ile olmuş, bu zaman kadar kişisel verilerin korunması konusunda genel nitelikte olan Medeni Kanun hükümlerine başvurulmak zorunda kalınmıştır.[166]

2.7. SÜREKLİLİK İLKESİ

Süreklilik kelimesi, zaman bakımından süreklilik ve içerik bakımından devamlı olma, bir başka deyişle istikrar anlamlarında kullanılır. Süreklilik taşıyan kamu hizmeti, günün her saatinde bireylere aynı oranda hizmet verilmesi anlamına gelmemektedir. Söz konusu faaliyetler, ihtiyaca göre şekillenerek orantılı şekilde gerçekleşmelidir.[167] Örneğin, elektronik haberleşme hizmetleri kapsamında abonelere çağrı merkezi hizmeti sunulması gerekliliği her işletmeci için mevcutken yalnızca 200.000'i aşkın abonesi olan işletmeciler için söz konusu çağrı merkezi hizmetinin 7 gün 24 saat sunulması gerekliliği bulunmaktadır.[168] Çünkü gece saatlerinde büyük oranda abonelerin hizmet kullanımı azaldığından bu saatlerde abonelerin bir problemle karşılaşma ihtimalleri ve karşılaşılan aksaklıktan etkilenen abone sayısının daha az olacağı malumdur. Bu sebeple abone sayısı az olan işletmecilerin de 7 gün 24 saat aktif olan bir çağrı merkezini bulundurmalarını beklemek yerinde bir uygulama olmayacağından yalnızca çok sayıda abonesi bulunan işletmecilere bu yükümlülük getirilmiştir. Bu durum, elektronik haberleşme sektöründe süreklilik ilkesinin ihlal edildiği anlamına gelmemekte, aksine ihtiyaca ve hizmetin içeriğine göre belirlenen bir süreklilik anlayışının benimsendiğini göstermektedir.

---

[166] Merve Ayşegül Kulular İbrahim, *Modern Teknolojinin Hukuki Temelleri: Telgraf Örneği*, (Ankara: Adalet Yayınevi, 2021), 150-151.

[167] Sancakdar, *İdare Hukuku*, 560.

[168] Elektronik Haberleşme Sektöründe Hizmet Kalitesi Yönetmeliği Ek-4'ün Uygulamasına İlişkin Tebliğ'in (R.G. 17.03.2012, S. 28236) 9/1 maddesi uyarınca, çağrı merkezine bir ay içerisinde üç yüz binin üzerinde çağrı gelmekte olan ya da 200.000'in üzerinde abonesi olan işletmeciler, bu Tebliğe uygun olarak hizmet kalitesi ölçümlerini yaparak BTK'ya bildirmekle yükümlü kılınmış olup; bu işletmeciler, Sabit Telefon Hizmetine İlişkin Hizmet Kalitesi Tebliği'nin 7/6 maddesinde belirtildiği üzere, kullanıcılarının arıza bildirimini 7 gün 24 saat boyunca almakla yükümlüdür.

Süreklilik ilkesine 5369 sayılı Evrensel Hizmet Kanunu'nun 3. maddesinde yer verilmiştir. Buna göre, evrensel hizmetin sunumu ve bu hizmete ulaşılmasında süreklilik esas olarak kabul edilmiştir.

EHK'da da süreklilik konusuna değinilerek 4. maddede belirtilen ilkelerden birisi de elektronik haberleşme hizmetinin nitelik ve nicelik olarak sürekli olmasıdır. Bunun yanı sıra aynı Kanun'un 34. maddesinde, elektronik haberleşme hizmetinin yetkili merciler tarafından verilen bir karar olmadıkça kesintiye uğratılmadan sürekli şekilde verilmesi gerektiği belirtilmektedir. Bu hüküm doğrultusunda sunulan elektronik haberleşme hizmetinin hangi hallerde kısıtlanabileceği veya durdurulabileceğine ilişkin Tüketici Hakları Yönetmeliği'nde hüküm bulunmaktadır. İlgili Yönetmeliğin 17. maddesi bu hali düzenlemiştir. Ödenmemiş faturaya dayanarak hizmetin kısıtlanması veya durdurulmasının ancak abonenin önceden bilgilendirilmesiyle olabileceği, hukuka aykırı veya hileli bir faaliyetin bulunduğu şüphesiyle kısıtlama ve durdurma eylemi gerçekleştirilecekse yine abonenin ancak bilgilendirilerek ilgili aksiyonun alınabileceğine yer verilmiştir. Söz konusu durumda bireyin hizmete ulaşımı engellendiğinden; hizmeti kısıtlama veya durdurma gibi kararlar ancak kuvvetli şüphenin varlığı veya tüketicinin korunmasına ilişkin hallerde işletmeci tarafından gerçekleştirilebilir şeklinde bir düzenleme bulunmaktayken Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nde Değişiklik Yapılmasına Dair Yönetmelik'in[169] (Değişik Tüketici Hakları Yönetmeliği) 31 Aralık 2022 tarihinde yürürlüğe giren 10. maddesiyle, Tüketici Hakları Yönetmeliği'nin 17. maddesinin ilk üç fıkrasında önemli değişiklikler yapılmıştır. Bunlardan en önemlisi hukuka aykırı veya hileli durumun varlığına dair kuvvetli şüphenin söz konusu olması halinde işletmeciye verilen abonenin hizmetlerinin kısıtlanması veya durdurulmasına yönelik yetkinin kaldırılmış olmasıdır. Değişik Tüketici Hakları Yönetmeliği ile 17. maddede artık yalnızca ödenmeyen fatura olması halinde veya hizmetin mutat kullanım düzeyinin aşılması halinde tüketicinin korunması amacıyla hizmetlerin kısıtlanabileceği veya durdurulabileceğine hükmolunmuştur. İlgili değişiklik ile elektronik haberleşme hizmetlerinin mücbir sebepler dışında kesinti olmadan sürekli şekilde sunulmasına verilen hassasiyetin arttığı gözlenmektedir.

Ayrıca elektronik haberleşme faaliyetlerinin kamu hizmeti niteliğinde olması sebebiyle sürekli şekilde ulaşılabilir olması, dolayısıyla kesintisiz şekilde işletmeciler

[169] R.G. 18.01.2022, S. 31723.

tarafından sunulabilir olması gerekmektedir. Örneğin, işletmeci olabilecek şirketler için Yetkilendirme Yönetmeliği'nde sayılan çok sayıda şartın varlığı ile elektronik haberleşme sektöründe faaliyet gösterebilmek isteyen her şirket yetkilendirilmemekte, yalnızca belirli kriterde olanlara izin verilmektedir. Bu hizmetlerden faydalanan tüketicinin mağduriyet yaşamaması için ticari varlığı ve faaliyeti hukuka uygun olan şirketler vasıtasıyla ilgili hizmetlerin sunulabilir olması hali önemsenmektedir. Böylece aboneler bir problemle karşılaştıklarında karşılarında bir muhatap bulabilmekte ve hizmetin sunumunu kesintisiz şekilde almaya devam edebilmektedir.

Aynı şekilde, işletmecinin Kurum'un belirlediği yükümlülükleri yerine getirmemesi sebebiyle daha fazla müşteri mağduriyetinin yaşanmaması ve tüketici menfaatinin korunması amacıyla işletmecinin yetkilendirmesine son vermesi durumunda işletmeciye abonelerinin başka işletmecilere taşınması için bilgilendirme yapması ve söz konusu telefon veya internet hizmetlerinin taşıma süreçlerinin tamamlanabilmesi için üç aylık süre tanınmaktadır.[170] Bu sayede, abonelerin almakta olduğu hizmetlerden bir anda mahrum kalmaları önlenmek istenmektedir.

[170] 27.12.2016 tarih ve 2016/DK-YED/516 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/ehsiyy-gecici-8-maddenin-ucuncu-fikrasinin-yurutulmesi.pdf , Erişim Tarihi: 13 Nisan 2022.

BÖLÜM 2

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLENMESİ İÇİN ABONEDEN ALINAN VE ELEKTRONİK HABERLEŞME HİZMETİNİN KULLANIMIYLA ORTAYA ÇIKAN KİŞİSEL VERİLER

1. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİ VE KİŞİSEL VERİ İŞLEME KAVRAMLARI

1.1. KİŞİSEL VERİ

Ticari işletmeler arasında rekabeti artırıcı en önemli kaynak olarak sermaye ve emeğin önüne geçen veri,[171] anlamlı bir bilgi olarak tanımlanmadan önce işlenmesi gereken temel düzeydeki gözlem ya da ölçüme dayalı her türlü değer olarak tanımlanabilmektedir.[172] Bir başka tanıma göre ise bilişim sisteminin işlem gerçekleştirebildiği her türlü işarete veri denilmektedir.[173] Bilgi ise işleme sürecine tabi tutulan verinin anlamlı hale gelen versiyonu olarak adlandırılmaktadır.[174]

Kişisel veri olan bilgiden söz edilebilmesi için öncelikle bir bilginin mevcudiyeti gerekmektedir.[175] 95/46/EC sayılı Direktif'in 2/a maddesinde kişisel veri, kimliği belirli veya belirlenebilir olan gerçek kişiye ait herhangi bir bilgi olarak tanımlanmıştır.

[171] Ertuğrul Aktan, "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu," Ankara Üniversitesi Bilgi Yönetimi Dergisi 1, no.1 (2018): 2.
[172] Korcan Doğan, Sacit Arslantekin, "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum," Ankara Üniversitesi Dil Tarih Coğrafya Fakültesi Dergisi 56, no.1 (2016): 16.
[173] Mesut Orta, *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)*, (Ankara: Yetkin Yayınları, 2015), 39-40.
[174] Aktan, "Büyük Veri," 2.
[175] Süleyman Yılmaz, Gökçe Filiz Çavuşoğlu, *Kişisel Verileri Koruma Hukuku*, (Ankara: Yetkin Yayınları, 2020), 37.

GDPR'ın 4. maddesinde ve 6698 sayılı KVKK'nın 3/1-(d) maddesinde de benzer kişisel veri tanımına yer verilmiştir.

Bilginin niteliği onun kişisel veri olma haline etki etmemektedir. Kişisel veri olan bilgi, yanlış da olsa nesnel bir doğruluğa dayanmasa da ilgili kişiyi belirli kılabilecek niteliğe sahipse kişisel veri olarak tanımlanmaktadır.[176] Bununla birlikte, veri tek başına doğrudan ilgili kişiyi tanımlamasa da anlamlı şekilde bir bireyle ilişkilendirilebilir olması, kişisel veri olarak adlandırılabilmesi için yeterli sayılmaktadır. Veri, kişisel veri olma özelliğini ancak çeşitli anonimleştirme yöntemleriyle ilgili kişi ile olan bağlantısı giderildiğinde yitirmektedir.[177]

Her geçen gün daha fazla şirket, mal ve hizmetlerini pazarlamak, satmak, dağıtmak gibi amaçlarla internet ve diğer iletişim ağlarını kullanmaktadır. Söz konusu faaliyetleri yerine getirirken şirketler; mal ve hizmet sunumu için müşteri verilerini toplama ve saklama, çevrimiçi reklamlar yapma veya potansiyel müşterilere e-posta vasıtasıyla reklam gönderme, çerezler yoluyla müşterilere ait bazı temel bilgileri kaydetme gibi amaçlarla kişisel verileri farklı yöntemlerle işleyebilmektedir. Telekomünikasyon şirketleri ise her gün sayısız kullanıcının sesini ve verilerini iletişim ağları üzerinden ileterek diğer mal ve hizmetleri sunan şirketlerin de verilerinin taşınmasına ve işlenmesine aracılık etmektedir. Böylelikle telekomünikasyon şirketleri, daha fazla kişisel veriyle muhatap olduğu gerçekliğinden hareketle veri koruma düzenlemelerinden ilk sırada etkilenmektedir.[178]

Elektronik haberleşme sektöründe kişisel verilerin işlenmesine yönelik düzenleme olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'te (Kişisel Verilerin İşlenmesi Yönetmeliği) veri kavramına 4/1-(l) maddesinde yer verilerek verinin kişisel veri, trafik verisi ve konum verisinden oluştuğu belirtilmiştir. Kişisel veri ise KVKK'daki ile aynı olacak şekilde tanımlanarak bir kimseyi belirli veya belirlenebilir kılan veri olarak tanımlanmıştır.

Anayasa Mahkemesi bir kararında, kişiye ait internet verileri, IMEI bilgileri, log kayıtları ve açık Wi-Fi noktasını kullandığı tarihe ilişkin verilerin, belirli bir kişiye ait bilgi olarak değerlendirilebileceğinden kişisel veri kapsamında olduğunu ele almıştır. Bu

[176] Yılmaz, *Kişisel Verileri Koruma Hukuku*, 37.
[177] Lothar Determann, *Kişisel Verilerin Korunması Uygulama Kılavuzu Şirketlerin Uluslararası Mevzuata Uyumu*, (İstanbul: On İki Levha Yayıncılık, 2020), XXVI-XXVII.
[178] Christopher Kuner, *European Data Privacy Law and Online Business*, (New York: Oxford University Press, 2003), 2.

doğrultuda ilgili kararda, kişisel verilerin hukuka uygun işlenip işlenmediği hakkında bilgi edinmenin özel hayatın gizliliği kapsamında olduğu ve kişisel verilerin korunmasını talep etme hakkı kapsamında değerlendirilmesi gerektiğine yer verilmiştir.[179]

Elektronik haberleşme sektörünün aktörleri niteliğindeki telefon ve telefonla ilgili hizmetler sunan telekomünikasyon şebekesi operatörleri ve internet servis sağlayıcıları (ISS), büyük veri analitiğinin başlıca adayları hatta halihazırda birincil kullanıcılarıdır. Bu aktörler, faaliyetlerinin devamına yönelik olarak toplanan çok sayıda abone bilgisini içeren veriye sahip olmaktadır. Abonelerden katma değer elde etmek için söz konusu veriler, sürekli olarak yeniden değerlendirilebilmektedir.[180]

Aboneden alınan kişisel verilerin tek bir amaçla alınıp depolanması yerine, veriler işletmeciler tarafından sürekli olarak yeniden değerlendirmeye tabi tutularak profilleme teknikleriyle aboneye özel pazarlama faaliyetlerinde bulunulmaktadır. Verilerin uzun süreler saklanması yükümlülüğü, işletmecilerin kendileri açısından avantajlı hale getirilmeye çalışılmaktadır. Bu aşamada, verinin hangi amaçlarla kullanıldığı ve saklandığı, veri sahibinin rızası dahilinde işlenip işlenmediği ve benzeri konular önem arz ederek işleme faaliyetinin hukuka uygunluğunu doğrudan etkilemektedir.

1.2. KİŞİSEL VERİ İŞLEME

6698 sayılı KVKK'nın 3/1-(e) maddesinde, kişisel verilerin işlenmesi şu şekilde tanımlanmaktadır. Buna göre kişisel verilerin işlenmesi, *"kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"*dir.

Buradan hareketle, veri sorumlusunun sorumlu olduğu alanın kapsamının çok geniş olduğu açıkça görülebilmektedir. İlgili hükümde, verinin elde edilerek veri kaydının yapıldığı andan itibaren başlayan kişisel veri işleme sürecinde, verinin değiştirme,

---

[179] AYM, 2018/6161 Başvuru numaralı 28.06.2022 tarihli Karar; https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161 , Erişim Tarihi: 21 Aralık 2022.

[180] Vagelis Papakonstantinou, Paul De Hert, "Big Data Analytics in Electronic Communications: A Reality in Need of Granular Regulation (Even if This Includes An Interim Period of No Regulation at All)," *Cyber and Data Security Lab Working Paper*, no.1 (2019): 5, http://dx.doi.org/10.2139/ssrn.3535701 , Erişim Tarihi: 15 Mayıs 2022.

düzenleme, sınıflandırma ve aktarımının yapıldığı aşama da dahil olmak üzere işleme sürecinin devam ettiğinden bahsedilmekte "gibi" sözcüğüne yer verilerek de işleme fiilinin kapsamının daha da genişletilebileceği belirtilmektedir.[181]

Kişisel verilerin çokça işlendiği bir sektör olan telekomünikasyon sektöründe, "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik,"[182] kişisel verilerin korunmasına dair oluşturulan ilk düzenleme olarak dikkat çekmektedir.

İlgili Yönetmeliğin yayım tarihi, 6698 sayılı KVKK'dan çok daha önce olduğundan; ifadeler ve açıklamalar bakımından düzenlemelerin birbiriyle uyumlu olmadığı görülmektedir. Örneğin, ilgili Yönetmeliğin kişisel verilerin işlenmesi tanımının yapıldığı 3. maddesinde; otomatik olsun ya da olmasın kişisel verilere yapılan tüm işlemler, kişisel veri işleme faaliyeti olarak tanımlanmışken KVKK'ya uygun şekilde yayımlanan kişisel verilerin korunmasına yönelik yeni düzenlemelerde ise kişisel verilerin işlenmesi, kısmen veya tamamen otomatik yollarla ya da bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi anlamına gelmektedir. Bu doğrultuda, herhangi düzenli kayıt sisteminin parçası olmayan, diğer bir ifadeyle bir sistematik çerçevesinde düzenli şekilde yapılmayan kişisel veri işleme faaliyetinin gerçekleştirilmesinin önüne geçilmek istenmiştir. Otomatik işlemeye örnek olarak bilgisayar ortamında kişisel verilerin çeşitli şekillerde sınıflandırılması verilebilirken; otomatik olmayan işlemeye örnek ise noterlerin harf veya tarihe göre belgeleri sınıflandırarak oluşturdukları arşiv kayıtları gösterilebilir. Bir başka deyişle, KVKK'dan önce yayımlanan ilgili Yönetmeliğin aksine, günümüzde herhangi bir kayıt sisteminin parçası olmadan sıradan bir veri işleme faaliyeti, hukuka uygun kişisel veri işleme anlamına gelmemektedir.

Ülkemizin 1981 yılında imzalayarak taraf olduğu 108 sayılı Sözleşme'nin, 3/1 maddesinde kamu ve özel sektördeki kişisel verilerin işleme faaliyetlerinin otomatik yollarla gerçekleştirilmesi gerektiği belirtilmiş olsa da 108 sayılı Sözleşme'nin 3/2-(c) maddesinde ise devletlerin dilerlerse otomatik olmayan, diğer bir ifadeyle kişisel verilerin manuel işleme faaliyetine tabi tutulduğu veriler konusunda da ilgili Sözleşme'yi

[181] Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*, (İstanbul: On İki Levha Yayıncılık, 2019), 46.
[182] R.G. 06.02.2004, S. 25365.

uygulayabileceği belirtilmiştir.[183] Ülkemizde, özellikle kamu kurumlarında ilgili kişilerin kişisel verilerinin çoğunluğunun manuel şekilde muhafaza ediliyor olması, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla manuel sistemin uygulandığı veri kayıt sistemleri için de kişisel verilerin korunması hükümlerinin uygulanması gerekliliğine neden olmuştur. Nitekim 95/46/EC sayılı Direktif'te de yalnızca otomatik veri işleme faaliyetine yer verilmişken GDPR 4/2 maddesinde "otomatik yöntemlerle olsun ya da olmasın" ifadesine yer vererek otomatik olmayan yöntemlerle veri işleme faaliyetlerinin de işleme olarak kabul edileceği belirtilmiştir.

5809 sayılı EHK'nın 12/2 maddesinde işletmecilere, sektörün ihtiyaçları, teknolojinin gelişimi, uluslararası düzenlemeler gibi nedenlerle kişisel veriler ve gizliliğinin korunması konusunda mevzuat doğrultusunda bazı yükümlülükler getirilebileceği belirtilmiştir. Bu doğrultuda, "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik"[184] yayımlanarak ilgili Yönetmeliğin yerine Avrupa Birliği'ndeki gelişmelerle uyum sağlanabilmesi amacıyla ise güncel düzenlemeleri içeren Kişisel Verilerin İşlenmesi Yönetmeliği yayımlanmıştır.

Elektronik haberleşme sektöründe işletmecinin, aboneliğin yetkilisine ilişkin kişisel verileri veya aboneliğin kullanımından kaynaklı verileri işlemesi yönünden veri sorumlusu olması; abone tarafından hizmetlerin kullanılması dolayısıyla işletmeciye aktardığı abonede bulunan başkalarına ait kişisel verilerin, örneğin abonenin toplu kısa mesaj gönderdiği telefon numaralarının işletmeci sistemlerine kaydedilmesi neticesinde işletmecinin bu verileri kullanarak iletinin alıcıya ulaştırılması gibi hizmetleri sağlaması sebebiyle de veri işleyen konumunda olması söz konusudur.

[183] 108 sayılı Sözleşme, 6669 sayılı Kanun ile uygun bulunup; 18 Şubat 2016 tarihli 29628 sayılı Resmi Gazete'de yayımlanarak; 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanarak iç hukukumuzda yerini almıştır.
[184] R.G. 24.07.2012, S. 28363.

2. KİŞİSEL VERİLERİN KORUNMASI MEVZUATININ GELİŞME SÜRECİ

Haberleşme verilerinin gizliliğinin korunması gerekliliğinin ardındaki neden, gerçek kişilerin kişisel deneyimleri, duyguları, cinsel ve siyasi tercihleri gibi hassas nitelikteki verilerinin korunarak mevcut teknolojiler ile davranışların ve düşüncelerin gözlenebildiği büyük miktardaki meta verinin kolayca ve zahmetsiz şekilde toplanma kolaylığı, nesnelerin interneti ile sürekli olarak artış gösteren veri seli, zararsız olarak düşünülen veri parçalarının kişisel veri olan özel bilgileri ortaya çıkarması, mahremiyet ihlallerine sebep olarak, her daim güncellenmesi gereken düzenlemeler yapılmasını gerektirmektedir.[185]

OECD, ekonomik anlamda ilerleme sağlayabilmek adına kişisel verilerin korunmasına ilişkin uluslararası platformda düzenlemeler yapan öncü kuruluşlardan olmuştur. Bu çerçevede OECD'nin 1980 yılında kabul ettiği "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler Hakkındaki Konsey Tavsiyesi"[186] (OECD Rehber İlkeler) ile kişisel verilerin korunmasına dair asgari gerekliliklerin sağlanması ve üye devletlerin söz konusu ilkeleri iç hukuklarına uyarlamaları yönünde önemli bir aşama kaydedilmiştir.[187]

Veri güvenliği, açıklık gibi hususlarda düzenlemeler içeren bu ilkeler, kişisel verilerin korunması ve denetiminin yapılmasına ilişkin milletlerarası bir çözüm arayışı içerisinde olunduğunun ve kapsamlı olarak ülkelerin bu konuya ilişkin uzlaşma sağladığının ilk göstergesi olarak dikkat çekmektedir. Ayrıca her ne kadar Rehber İlkeler tavsiye niteliğinde olup bağlayıcılık teşkil etmese de konuya ilişkin ulusal ve uluslararası düzenlemelerin yapılması ve söz konusu düzenlemelerin muhtevasının oluşturulmasında

---

[185] Elena Gil González, Paul De Hert, Vagelis Papakonstantinou, "The Proposed Eprivacy Regulation: The Commission's and the Parliament's Drafts At A Crossroads?" *Brussels Privacy Hub Working Paper* 6, no.20 (2020): 9, https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL6-N20.pdf , Erişim Tarihi: 15 Mayıs 2022.

[186] OECD Rehber İlkeler, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm , Erişim Tarihi: 15 Mayıs 2022.

[187] Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku*, (İstanbul: Hukuk Akademisi Yayıncılık, 2020), 86-87; Elif Küzeci, *Kişisel Verilerin Korunması*, (İstanbul: On İki Levha Yayıncılık, 2021), 131-132.

etkin rol oynamıştır. Ülkemizde de 6698 sayılı KVKK gerekçesinde ilgili Rehber İlkelere yer verilerek iç hukukumuzda konuya ilişkin düzenleme yapılmıştır.[188]

1945 yılında kurulan Birleşmiş Milletler (BM) tarafından 1948 yılında kabul edilen BM Evrensel İnsan Hakları Bildirisi'nin 12. maddesi, kişilerin özel hayata ve haberleşmeye yönelik saldırılara maruz kalmaması gerektiği ve hukuk nezdinde korunma hakkının mevcut olduğuna vurgu yapmaktadır. BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17. maddesinde de benzer şekilde düzenleme yapılarak kişisel verilerin korunması hakkının söz konusu Sözleşme'de düzenlenen özel yaşamın gizliliği hakkı çerçevesinde değerlendirildiği BM İnsan Hakları Komitesi'nce kabul edilmiştir.[189]

BM, 1990 yılında yayınladığı "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler" özel hayatın gizliliği hakkından ayrı olarak, kişisel verilerin korunması hakkına dair doğrudan yapılan ilk düzenleme mahiyetindedir. Kanuna uygun, dürüst yollarla verinin toplanması ve işlenmesi ilkesi, verinin doğruluğu ilkesi gibi hususlarda düzenlemeler yapılmış, OECD Rehber İlkelere nazaran daha sınırlayıcı alanda etkin olmuştur.[190]

Avrupa Konseyi tarafından 1981 yılında kabul edilen 108 sayılı "Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme"[191], sadece Avrupa Konseyi üyesi devletlerin değil, söz konusu sözleşmenin taraflarından olan ülkelerin de imzalanmasına imkan vermesi ve kişisel verilerin korunmasına dair bağlayıcı nitelikte olan tek uluslararası düzenleme olması hasebiyle önem teşkil etmektedir. Sözleşmenin amacı, kişisel verilerin otomatik işlenmesi halinde dahi özel hayatın gizliliğinin korunmasını sağlamak olup bilhassa özel sektörde kişisel verilerin bilgisayar aracılığıyla işlenmesi halinde Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) gerçek kişiler yönünden gerekli korumayı sağlaması konusunda bazı endişeler olması sebebiyle 108 sayılı Sözleşme ile bu endişelerin giderilmesi hedeflenmiştir. Bu doğrultuda sadece otomatik ve kısmen otomatik şekilde işlenen veriler 108 sayılı Sözleşme kapsamında değerlendirilmektedir.[192]

---

[188] Küzeci, *Kişisel Verilerin Korunması*, 131-132.
[189] Küzeci, *Kişisel Verilerin Korunması*, 134-135.
[190] Küzeci, *Kişisel Verilerin Korunması*, 136-137.
[191] European Treaty Series - No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, https://rm.coe.int/1680078b37 , Erişim Tarihi: 17 Mayıs 2022.
[192] Küzeci, *Kişisel Verilerin Korunması*, 144-146.

108 sayılı Sözleşme'nin, bilişim teknolojilerindeki gelişmeler karşısında revize edilme ihtiyacının ortaya çıkması nedeniyle Sözleşme 108+[193], 2018 yılında Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmiştir. Bu metinde güncel konulara yer verilmesi, halihazırda 108 sayılı Sözleşmede yer alan bazı düzenlemelerin detaylandırılması ve GDPR ile benzer tarihli olması sebebiyle mevcut kişisel veri işleme süreçlerinin daha sağlıklı ilerleyeceğinden söz edilebilir.[194]

Türk hukukunda, 108 sayılı Sözleşme'nin imzalanması ile tam anlamıyla kişisel veri kavramıyla tanışılmıştır. Kişisel veri kavramı, 2010 yılında gerçekleşen referandum süreci sonrasında başlı başına bağımsız bir hak niteliğine bürünerek öncesindeki özel hayatın gizliliği hakkı çerçevesine dahil olmaktan ayrıştırılmıştır.

2016 yılında yürürlüğe giren 6698 sayılı Kanun, 95/46/EC sayılı Veri Koruma Direktifi'nin uyarlanmış hali niteliğindedir. 14 Nisan 2016'da Avrupa Parlamentosu tarafından onaylanan 2016/679 sayılı "Genel Veri Koruma Tüzüğü (General Data Protection Regulation - GDPR)"[195] ile kişisel verilerin korunmasına ve mahremiyetin sağlanmasına yönelik AB'de kapsamlı değişiklikler yapılmıştır.

GDPR, 95/46/EC sayılı Direktif'in iki temel eksikliğini gidermek üzere tasarlanmıştır. Birincisi, teknik ilerlemeler veri işlemeyi 1995 yılında beklenenin çok ötesine taşıyarak, kişisel verilerin etkilenmesine yönelik yeni tehditler oluştururken aynı zamanda verilerden değer elde etmek için yeni fırsatlar da ortaya çıkarmıştır. Bu sebeple AB'de 95/46/EC sayılı Direktif'in bazı önemli güncellemelere ihtiyacı olduğu kabullenilmiştir. İkinci olarak, AB üye devletleri, 95/46/EC sayılı Direktif'in yetkilerini kendi ulusal yasalarına biraz daha farklı bir şekilde aktarmakla kalmanın yanında, aynı zamanda ulusal yasaları uygulama ve yürütme biçimleri konusunda da oldukça farklılaşmaya başlamıştır. ABAD, veri koruma meseleleriyle ilgili kararlarında, 95/46/EC sayılı Direktif'in yetkilerinin nasıl yorumlanacağı ve uygulanacağı konusunda rehberlik sunmasına rağmen, bunun üye devletlerin mevzuat birliği sağlanarak her ülkede geçerli yeni düzenlemeler ile giderilebileceği ön plana çıkmıştır.[196]

---

[193] Convention 108 + Convention for the Protection of Individuals with regard to the Processing of Personal Data, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf , Erişim Tarihi: 17 Mayıs 2022.
[194] Küzeci, *Kişisel Verilerin Korunması*, 149-151.
[195] GDPR, https://gdpr-info.eu/ , Erişim Tarihi: 17 Mayıs 2022.
[196] Viktor Mayer-Schönberger, Yann Padova, "Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation," *The Columbia Science & Technology Law Review* 17, no.2 (2016): 323-324, https://journals.library.columbia.edu/index.php/stlr/article/view/4007/1769 , Erişim Tarihi: 17 Mayıs 2022.

AB'ye üye ülkeler arasında kişisel verilerin korunması ve bu hususta ortak bir metin oluşturularak üye devletlerin iç hukuklarında yeknesaklığın sağlanması amacıyla hazırlanan GDPR, 4 Mayıs 2016 tarihinde yayımlanarak 24 Mayıs 2016'da yürürlüğe girmiştir. Söz konusu metnin, uygulanmaya başlama tarihi ise 25 Mayıs 2018'dir. Söz konusu metnin 94. maddesinde de belirtildiği üzere, 95/46/EC sayılı Direktif mülga olmuştur.[197]

GDPR, AB'de ikamet edenlerin kişisel bilgilerini işleyen bütün veri sorumlusu ve işleyenlerin, kişisel verileri kendilerine emanet edilen kişilerin hak ve özgürlüklerini korumalarını ve uygulamalarını zorunlu kılmaktadır. Ayrıca veri işleme sistemleri ve hizmetlerinin devam eden gizliliğini, bütünlüğünü, kullanılabilirliğini sağlamak adına uygun teknik ve organizasyonel önlemler alınması gerektiğine ilişkin düzenlemelere yer vermektedir.[198]

6698 sayılı KVKK, 7 Nisan 2016 tarihinde yürürlüğe girdiğinden 4 Mayıs 2016 tarihinde AB'de GDPR'nin kabul edilmesiyle birlikte söz konusu Tüzüğe ilişkin değişikliklerin mevzuatımıza tam olarak uyarlanmadığı söylenebilir.

3. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE AÇIK RIZA

Kişisel verileri işlemenin hukuka uygun olabilmesi için ya ilgili kişinin rızasının bulunması gerekmekte ya da GDPR, AB düzenlemesi veya üye devletlerin kendi hukukundaki diğer düzenlemeler doğrultusunda meşru temelde işlenmesi gerekmektedir.[199] Diğer bir deyişle kural, kişisel verilerin işlenmemesi, istisnası ise işlenmesi halidir.[200] Kişisel verilerin işlenmesi halinde kural, ilgili kişinin açık rızasının bulunmasıdır. Onay, her türlü kişisel veri işleme faaliyetini meşrulaştırır.[201]

Elektronik haberleşme sektöründe çok sayıda veri işlenmesi hali, genellikle abonenin açık rızası koşuluna bağlanmış olsa da elektronik haberleşme hizmeti sunan

[197] GDPR Article 94, https://gdpr-info.eu/art-94-gdpr/ , Erişim Tarihi: 17 Mayıs 2022.
[198] IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide*, (Cambridge: IT Governance Publishing, 2020), 12.
[199] Paul Lambert, *Understanding the New European Data Protection Rules*, (Boca Raton: CRC Press - Taylor & Francis, 2017), Chapter 4, Need For Updating Data Protection, 10.
[200] Dülger, *KVK Hukuku*, 220.
[201] Daniel J. Solove, "Introduction: Privacy Self-Management and The Consent Dilemma," *Harvard Law Review* 126, (2013): 1880.

işletmecinin kişisel veri işlemeye yönelik çoğu faaliyeti kanuni yükümlülükten kaynaklanmaktadır.

3.1. AÇIK RIZA KAVRAMININ İNCELENMESİ

Kişisel veri işleme faaliyetinin hukuka uygunluk nedenlerinden biri olarak kabul edilen açık rıza ile veri sorumluları, rıza gösterilen konular çerçevesinde verileri kontrol edebilme hakkına sahip olmaktadır.[202]

İlgili kişilerden kişisel verilerinin işlenmesine ilişkin bildirimde bulunularak rızalarının istenmesi, verilerinin işlenmesinin sonucuna kendilerinin karar vermesini sağlar. Gizlilik düzenlemesine ilişkin bu yaklaşım, gizlilik özyönetimi olarak adlandırılmaktadır. Gizlilik özyönetiminin temeli rızaya dayanır. Bu durum, kişisel veri işleme faaliyetinin iyi veya kötü şeklinde adlandırılmasının aksine kişilerin işleme faaliyetine rıza gösterip göstermediğine odaklanmayı sağlamaktadır.[203]

3.1.1. AB Düzenlemeleri ve KVKK'da Açık Rıza ve Rıza Kavramlarının Kullanılması

95/46/EC sayılı Direktif'in 2/(h) maddesinde belirtilen rıza kavramı, veri sahibinin bilgilendirildikten sonra kişisel verisinin işlenebilmesi için özgür şekilde vermiş olduğu rıza anlamında kullanılmaktadır. İlgili Direktif'in 7/(a) maddesinde ise rızanın açık, kesin ve belirli şekilde ortaya konulması gerektiğine yer verilmiştir. Özel nitelikli kişisel verilerin korunmasına yönelik düzenlenen Direktif'in 8/(a) maddesinde ise açık rıza ifadesi kullanılmıştır.

GDPR'ın 4/11 maddesinde rıza, ilgili kişinin beyanıyla veya açık bir davranışıyla kişisel verilerinin işlenmesine özgürce rıza gösterdiğine ilişkin özel, bilinçli ve açık belirti olarak ifade edilmiştir.

95/46/EC sayılı Direktif ve GDPR'da yer yer rıza ve açık rıza kavramları kullanılmıştır. KVKK'da ise hem genel nitelikli hem de özel nitelikli kişisel verilerin hukuka uygun şekilde işlenebilmesi amacıyla ilgili kişinin açık rızası arandığı; bu bakımdan 95/46/EC sayılı Direktif ve GDPR'dan ayrıldığını düşünen bir görüşe göre,

[202] Serdar Çelikel, "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve GDPR'la Karşılaştırmalı Olarak İncelenmesi," *Uyuşmazlık Mahkemesi Dergisi* 9, no.17 (2021): 161.
[203] Solove, "The Consent Dilemma,"1880.

Anayasa 20/3 maddesinde belirtildiği üzere, kişisel veriler ilgili kişinin açık rızası dahilinde işlenebilecek olup; KVKK'nın 3. maddesinde yapılan tanım da açık rıza kapsamında düzenlenmiştir. İlgili madde uyarınca açık rıza, bilgilendirmeye dayalı olarak özgür şekilde spesifik olarak bir konuya özgülenerek verilen rızadır ve GDPR ve 95/46/EC sayılı Direktif'in aksine KVKK metninin tamamında açık rıza kavramına yer verilmiştir. Bu sebeple de KVKK'nın AB düzenleme ve uygulamalarına nazaran daha korumacı bir yaklaşımda olduğu düşünülmektedir.[204]

Diğer taraftan, GDPR ve ilgili Direktif'teki rıza kavramlarının da KVKK'da değinilen açık rıza kavramıyla aynı nitelikli olduğunun belirtildiği bir başka görüşe göre ise GDPR'da yer verilen rıza (consent) ve açık rıza (explicit consent) kavramları aslında aynı durumu nitelemektedir. Direktif'in 2/(h) maddesi ve 7/(a) maddesinde belirtilen rıza kavramıyla KVKK'daki tanım örtüşmektedir. Bununla birlikte, Avrupa Veri Koruma Kurulu'nun (European Data Protection Board - EDPB) 05/2020 sayılı Rehberi'nde[205] GDPR'daki rıza kavramıyla Direktif'teki rıza kavramlarının aynı nitelikte olduğu açıklanmıştır. Nitekim KVKK gerekçesinde[206] de açık rıza tanımının düzenlenmesi aşamasında Direktif'in esas alındığına yer verilmiştir. GDPR'ın 4/11 maddesinde yapılan rıza tanımı ile KVKK'da yapılan tanımın uyuştuğu açık olduğundan ve GDPR'da hukuka uygunluk nedeni olarak rızanın öngörüldüğü hallerde özel nitelikli kişisel veriler ve genel nitelikli kişisel veriler için aranan rıza kavramı arasında yalnızca ifade bakımından farklılık olduğu, rızanın niteliği bakımından ise hiçbir farkın olmadığı düşünülmektedir.[207]

GDPR ve Direktif'te ara ara yalnızca rıza kavramı kullanılsa da bahsi geçen tanımlar dikkate alındığında rıza için aranan koşulların aynı olduğu görüldüğünden KVKK'nın AB düzenlemelerine nazaran daha fazla koruma sağladığı düşüncesinin doğru bir yaklaşım olamayacağı düşünülmektedir.

---

[204] Bahri Öztürk, Elif Altınok Çalışkan, "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu," *Fasikül Hukuk Dergisi* 10, no.100 (2018): 292-293; KVK Kurumu, Açık Rıza Rehberi, 1-4, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf , Erişim Tarihi: 22 Mayıs 2022.

[205] EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Erişim Tarihi: 22 Mayıs 2022.

[206] KVKK Tasarısı (1/541), https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf , Erişim Tarihi: 23 Mayıs 2022.

[207] Çelikel, "Açık Rıza," 167-169.

3.1.2. Örtülü Rıza ve Açık Rıza Kavramları

AB düzenlemeleri ve KVKK uyarınca, rızanın sarih, olumlu ve herhangi bir belirsizlik içermeyecek şekilde olması gerekmektedir. İlgili kişinin önceden işaretlenmiş olan kutucuğu kaldırmayarak zımni rıza verdiğinin düşünülmesinin yanı sıra herhangi olumlu bir eylem gerçekleştirmemiş olması sebebiyle de alınan rıza, belirsizliğe yol açmayacak şekilde verilmediğinden geçerli olmamaktadır.[208] Bu sebeple veri sorumlularının, ilgili kişilerin kutucuğu işaretlemesi, tıklaması gibi aktif bir davranışta bulunmalarını gerektirecek şekilde beyanlarını almayı sağlayan bir sistem kurması daha uygun olacaktır.[209] Ayrıca rızayı alan ve veren taraf arasında herhangi bir uyuşmazlık söz konusu olduğunda ispat yükünün veri sorumlusunda olması[210] da rızanın sarih bir şekilde aktif bir davranışla verilmesinin önemini artırmaktadır.

GDPR'da açık rıza tanımı yapılmamış olmasına rağmen söz konusu düzenlemenin Giriş Bölümü'nde bulunan 32. paragrafında belirtildiği üzere, susma yoluyla rıza verilmesi ya da belirsiz ifade ve yoruma dayanarak rıza verildiği sonucuna ulaşılması hali, geçerli rıza beyanı olarak kabul edilmeyerek örtülü-zımni rızanın geçerli olmadığı ve GDPR'ın genelinde bahsedilen rıza kavramının açık rızayı karşıladığı dolaylı şekilde anlaşılmaktadır.[211]

KVK Kurulu Amazon Türkiye kararında, Amazon Türkiye'nin üyelik aşamasında kullanıcılara gösterdiği Gizlilik Bildirimi'nin kullanıcının üyelik sürecine devam etmesiyle rıza vermiş sayılması halini, diğer bir ifadeyle kullanıcılardan alınan zımni rıza beyanını hukuka aykırı olarak değerlendirmiş olup; kişisel verilerin aktarımı, çerezlerin işlenmesi gibi işleme faaliyetleri için de rızanın yine bu bildirim yoluyla tek seferde alınması halini battaniye rıza[212] olarak nitelendirerek; rızanın her işleme faaliyeti için ayrı

---

[208] Determann, *KVK Uygulama Kılavuzu*, 98.
[209] Lambert, *Data Protection Rules*, Chapter 4, 9; Determann, *KVK Uygulama Kılavuzu*, 98.
[210] EDPB, Guidelines 05/2020 on Consent, 11.
[211] Salih Polater, "Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri," *Kişisel Verileri Koruma Dergisi* 1, no.1 (2019): 8.
[212] Rızanın yeterince belirli bir konuya özgü olmasını sağlamak ile rızayı kısa ve anlaşılır kılmak arasında bir çatışma vardır. Aynı zamanda hem kısa hem de birçok bilgiyi içerebilen rıza metni hazırlanması güçtür. (Information Commissioner's Office (ICO), How should we obtain, record and manage consent?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/ , Erişim Tarihi: 24 Mayıs 2022.) Bu durumda alıcının rızasını almak isteyenler genellikle sınırları fazla belli olmayan ve kapsamı daha geniş nitelikte olacak şekilde battaniye rıza şeklinde rıza alma yoluna gitmektedir. Fakat bu şekilde alınan rızalar hukuka uygun kabul edilmemekte, geçersiz sayılmaktadır. (KVK Kurumu, "Açık Rıza Alırken Dikkat Edilecek Hususlar," https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar , Erişim Tarihi: 24 Mayıs 2022.)

ayrı alınmamış olması sebebiyle genel anlamda alınan rızaların KVKK'ya uygun alınan rıza olarak kabul edilemeyeceğine değinmiştir. Ayrıca Kurul tarafından, Amazon Türkiye'nin kullanıcıyı Gizlilik Bildirimi ile yalnızca üye olmaya ilişkin hususlarda bilgilendirmesi ve sadece üye olmayla ilgili şartları kabul etmesine yönelik rıza alması gerektiği, verilen bu onayın ticari elektronik ileti gönderimi yanında çerezlerin işlenmesi gibi başka amaçlar için de verildiği anlamına gelmeyeceği, aksi halin dürüstlük kuralına aykırılık teşkil edeceği bildirilmiştir.[213]

3.2. HUKUKA UYGUNLUK NEDENİ OLARAK AÇIK RIZA

İç hukukumuzda, KVKK'nın 5/2 madde hükmüne göre açık rıza bulunmadan verilerin işlenebileceği haller; kanunlarda açık şekilde belirtilmiş olması, fiili imkansızlık nedeniyle ilgili kişinin rızasını açıklayamayacak durumda olması halinde veya hukuken geçerli rıza veremeyecek olan kimsenin ya da bir başka kişinin beden bütünlüğünün korunması için işlemenin zaruri olması, bir sözleşmenin kuruluşu veya yerine getirilmesiyle ilgili olması halinde sözleşmenin taraflarının kişisel verilerinin işlenmesinin mecburi olması, veri sorumlusunun tabi olduğu mevzuata dair mükellefiyeti, ilgili kişi tarafından herkesçe bilinir hale getirmek, veri işlemenin ilgili kişiye bir hakkın tanınması için zorunluluk teşkil etmesi ve veri sorumlusunun hukuka uygun menfaatinin korunması amacıyla ilgili kişinin temel hak ve hürriyetlerine zarar vermeyecek şekilde işlenmesinden ibarettir.

Her ne kadar söz konusu istisnai hallerde veri sorumlusunun işleme faaliyeti hukuka uygun kabul edilerek ilgili kişinin ayrıca açık rızasının alınmasına gerek olmasa da bu durum veri sorumlusunu işleme faaliyetleri hakkında ilgili kişiyi bilgilendirme yükümlülüğünden kurtarmamaktadır.[214]

Kişisel verilerin hukuka uygun şekilde işlenmesi ve özellikle Anayasa ile koruma altına alınan kişisel verilerin korunması hakkı bağlamında verisi işlenen ilgili kişiler bakımından hukuki teminat ihtiyacı bulunmaktadır. Söz konusu korumanın sağlanması esnasında gerçekleştirilen engellemelerin veri sorumlusunun gerçekleştireceği faaliyette aksamaya neden olmaması da bir o kadar önem arz etmektedir. Kişisel veri işleme

[213] KVK Kurulu, 27.02.2020 tarih ve 2020/173 sayılı Amazon Turkey Perakende Hizmetleri Limited Şirketi Kararı, https://www.kvkk.gov.tr/Icerik/6739/2020-173 , Erişim Tarihi: 24 Mayıs 2022.
[214] Jakub Misek, "Consent to Personal Data Processing the Panacea or the Dead End?," *Masaryk University Journal of Law and Technology* 8, no.1 (2014): 81.

faaliyetine izin verilmemesi, kamu hizmetlerinin de yerine getirilmesine engel teşkil edebilmektedir. Bu sebeple yapılacak olan hukuki düzenlemelerin her zaman bu sınırı koruyabilecek düzeyde hazırlanması gerekmektedir.[215] Nitekim elektronik haberleşme hizmeti de kamu hizmeti niteliğinde olduğundan bu sektöre ilişkin yapılacak olan hukuki düzenlemelerin haberleşme hizmetinin sunumu engellenmeyecek şekilde yapılması önem teşkil etmektedir.

Kişisel verilerin korunmasına ilişkin düzenlemelerde ilgili kişinin açık rızasının alınması öncelenmiş olsa da söz konusu istisnai durumların varlığı halinde ilgili kişinin açık rızası aranmadan işleme faaliyeti gerçekleştirilebilmektedir. Açık rıza beyanının da aynı istisnai haller gibi hukuka uygunluk nedenlerinden birisi olduğu unutularak; yasal mevzuattaki yükümlülüğü sebebiyle kişisel veri işleme faaliyeti gerçekleştirmek zorunda olan veri sorumluları da yanılgıya düşerek ilgili kişiden açık rıza almaya çalışmaktadır. Bu durumda, ilgili kişi tarafından açık rızasının geri alınması halinde söz konusu kişisel verisinin işlenmesinin durdurulacağı zannedilmektedir. Halbuki aslında veri sorumlusu tarafından hukuki yükümlülüğünün yerine getirilmesi amacıyla işlemeye devam edilecektir. Diğer bir deyişle farklı bir hukuki işlemle işleme faaliyeti sürdürülecektir.[216] Dolayısıyla kişisel veri işleme faaliyetini gerçekleştirmeden önce ilgili kişilerin işleme faaliyetine yönelik bilgilendirilmesi konusunda veri sorumlularına büyük sorumluluk düşmektedir.

Her sektörde olduğu gibi elektronik haberleşme sektöründeki işletmeci olan veri sorumlularının, kişisel verileri işlemeye dair hukuka uygunluk nedenlerinin farkında olması çok önemlidir. Örneğin, navigasyon hizmeti sunan bir mobil uygulama yazılımcısı tarafından sunulan temel hizmetin navigasyon hizmeti olması sebebiyle ve bir kişinin bu hizmetten yararlanabilmesi için konum verilerine hizmeti sunan tarafından erişilmek zorunda olduğu açık olduğundan; veri sorumlusu olan hizmet sunanın ilgili kişinin açık rızasını almasına gerek yoktur. Fakat temel navigasyon hizmetinin yanında kişiye şehirdeki tiyatrolarda sahnelenen oyunların saatleri hakkında bilgi vermesi gibi bir katma değerli hizmetin sunulmak istenmesi halinde ise ilgili kişinin söz konusu tiyatroya yakınlığının uygulama tarafından tespit edilerek kendisine oyun saatleri hakkında anlık

[215] Adnan Küçük, "1982 Anayasası'ndaki Temel Hak ve Hürriyetlerin Sınırlanması Rejimi Bağlamında Kişisel Verilerin Korunması Hakkının Sınırlanmasının Anayasaya Uygunluğu," iç. *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, ed. Bayram Doğan (Ankara: Adalet Yayınevi, 2022), 39.
[216] Misek, "Consent Personal Data," 79-80.

bilgi verilmesi, kişinin hareketlerinin sürekli izlenmesini gerektirdiğinden; ilgili kişinin açık rızasının alınması gerekmektedir.[217]

3.3. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE AÇIK RIZANIN GEÇERLİLİK KOŞULLARI

KVKK, GDPR ve 95/46/EC sayılı Direktif'te yapılan tanımlar doğrultusunda açık rızanın geçerli sayılabilmesinin koşullarının; ilgili rızanın belirli bir kişisel veriye yönelik olarak verilmiş olması, özgür iradeyle açıklanmış olması ve bilgilendirmeye dayalı olarak verilmesi sayılabilir.[218]

3.3.1. Açık Rızanın Belirli Bir Konuya Özgülenerek Verilmiş Olması

Açık rızanın geçerli bir irade beyanı olarak kabul edilebilmesinin ilk şartı olan rızanın belirli bir konuya özgülenmiş şekilde verilmesi, ilgili kişinin genel anlamda tüm kişisel verilerinin işlenmesini kabul etmesinin geçerli bir rıza beyanı olmayacağı anlamına gelmektedir.[219] Diğer bir deyişle açık rızanın, veri sorumlusu tarafından verilerin hangi konularda işleneceğine dair yapılan açıklaması doğrultusunda, ilgili kişi tarafından kendisine bildirilmiş olan verilerinin yine sadece bildirilen konularda işlenmesine rıza gösterilmiş olması halinde geçerli bir rızadan bahsedilebilecektir.[220] Bu doğrultuda, ilgili kişinin rızasının alınmak istendiği konunun sınırlı ve kapsamının belli olmasının yanı sıra rızanın açık bir şekilde alınması gerekmektedir.[221] Bahsi geçen kriterler, OECD ilkelerinden olan açıklık, kapsamının sınırlı olması ve belirli amaç doğrultusunda kişisel verilerin işlenmesi ilkelerinin bir yansımasıdır.

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(a) maddesinde de ilgili kişinin açık rızasının belirli bir konuya yönelik olarak işlem öncesinde alınması gerektiğine değinilmiş, belirli bir konuya özgülenmeyen genel nitelikte alınan rızalar geçerli sayılmamıştır.

---

[217] Misek, "Consent Personal Data," 80-81.
[218] Öztürk, "KVKK Hakkında Değerlendirme," 293.
[219] Dülger, *KVK Hukuku*, 224-225; KVK Kurumu, Açık Rıza Rehberi, 5.
[220] Sinem Göçmen Uyarer, *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*, (Ankara, Seçkin Yayıncılık, 2020), 111-112.
[221] KVK Kurumu, Açık Rıza Rehberi, 5-6.

3.3.2. Açık Rızanın Özgür İradeyle Verilmiş Olması

Rızanın, ilgili kişinin özgür iradesinin yansıması olması gerekmektedir. Başka bir deyişle, ilgili kişinin iradesini etkileyecek ya da bozacak herhangi bir dışsal etken bulunmaması gerekmektedir.[222] Rızayı veren taraf ile alan taraf arasında kamu kurumu ve birey arasında olduğu gibi açık bir dengesizliğin olduğu hallerde, rızanın hukuka uygunluk nedeni olarak anılmasında kesinlik bulunmamakta olup; bunun gibi hallerde rızanın serbestçe verilmesi olası değildir.[223] Aynı şekilde, işçi-işveren arasındaki gibi bir ilişkinin söz konusu olduğu durumlarda rızanın serbest irade ürünü olduğu sorgulanmaktadır. Örneğin, ilgili kişinin işten çıkartılma gibi çeşitli kaygılarla rıza verirken ilgili kişiye rızasını geri alma hakkı ve benzeri güvencelerin sağlanmasının rızanın geçerliliğini artıracağı açıktır.[224] Ayrıca ilgili kişiye rızayı geri alma hakkının tanınmamasının rızanın geçersiz sayılacağı anlamına gelmesinin yanı sıra ilgili kişinin kişisel verisinin işlenmesine rıza göstermediği hallerde hizmete erişememe, sözleşmenin kurulamaması gibi bir yaptırım öngörülmesi de rızanın geçerliliğini etkilemektedir.[225] Bununla birlikte, açık rızayı verenin her zaman geri alabilmesi durumu, bir başka deyişle irade açıklaması üzerinde serbest şekilde tasarruf edebilmek, veri sorumluları tarafından ilgili kişiye verilen rızayı geri alabilmeleri hakkını da sunmayı gerektirir. Bu bağlamda, hukuka uygunluk nedeni olan açık rızanın kişisel verilerin gelecekte nasıl kullanılacağını belirleyebilmeye yönelik olarak verildiği söylenebilir.[226]

Elektronik haberleşme sektöründe işletmeci tarafından önceden hazırlanan abonelik sözleşmesi, abone olmak isteyen kişiye imzalatılmakta ve abone ancak hizmete işletmeci tarafından verilmesi halinde ulaşabildiği için, abone ve işletmeci arasında da benzer ilişkinin söz konusu olduğu söylenebilir. Bu doğrultuda, Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(b) maddesinde belirtildiği üzere açık rızanın, aboneliğin kuruluşu, cihaz temini ve temel düzeydeki elektronik haberleşme hizmetlerinin sunumu için ön şart olarak belirlenemeyeceği hüküm altına alınmış olup; yalnızca ilgili kişinin çeşitli hediye SMS ve benzeri faydalar sağlanarak açık rıza vermeye teşvik edilebileceği düzenlenmiştir.

---

[222] Küzeci, *Kişisel Verilerin Korunması*, 266.
[223] Lambert, *Data Protection Rules*, Chapter 4, 10.
[224] Küzeci, *Kişisel Verilerin Korunması*, 266-267.
[225] Lambert, *Data Protection Rules*, Chapter 4, 10; Küzeci, *Kişisel Verilerin Korunması*, 268.
[226] Çelikel, "Açık Rıza," 167; Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-," *Kişisel Verileri Koruma Dergisi* 1, no.2 (2019):44-45.

Bireylerin kendi mahremiyetlerini korumak adına alabilecekleri bazı tedbirler söz konusudur. Teknolojik aletlerin kullanımı ya da bu cihazlar kullanılarak elde edilen veri toplama uygulamaları konusunda yeterli bilgi sahibi olmamak, verilerin elde edilmesi ve kullanılmasıyla sonuçlanan işlemlerde kültürel ya da ekonomik baskılardan kaçınamama durumu çoğu zaman bilinçsiz şekilde verilen rıza beyanlarına sebep olmaktadır.[227] Örneğin; bilmediği bir dilin konuşulduğu ülkede, haberleşme hizmetinden yararlanmak adına bir telekom operatörünün hattını kullanma talebi olan kişinin doldurduğu formun içeriğine yeterince dikkat etmeden, kullanmak istediği hatta bir an önce kavuşabilmek motivasyonuyla hareket etmesi çoğu zaman mahremiyetinin ihlali ile sonuçlanabilmektedir.

Benzer şekilde, elektronik haberleşme sektöründeki işletmeciler tarafından çeşitli amaçlarla kişisel verilerin işlenmesine abone tarafından onay verilmesi halinde kullanılan tarifeye indirim yansıtılacağı gibi fayda sağlanması durumu, ekonomik baskı olarak nitelendirilebilir. Bu durumun, abone veya kullanıcının motivasyonunu etkileyeceği açık olduğundan, her ne kadar Kişisel Verilerin İşlenmesi Yönetmeliği ile meşru kılınmışsa da ilgili kişinin özgür iradesini değiştirebileceğinden; rızanın geçerliliğini doğrudan etkilediği açıktır.

3.3.3. Açık Rızanın Bilgilendirmeye Dayalı Olarak Verilmesi

Açık rızanın geçerliliğini etkileyen son şart ise ilgili kişinin rızasının alınmak istendiği konu hakkında bilgilendirilmiş, aydınlatılmış olmasıdır. Açık rıza alınması aşamasında yapılacak olan bilgilendirmenin içeriğinde; veri sorumlusunun kimliği, rızanın istendiği işleme konularından her birinin amacı, hangi verilerin toplanacağı ve kullanılacağı, rızanın geri alınmasına ilişkin hak tanınması, veriler otomatik karar vermek için kullanılacaksa buna dair bilgilendirme ve verilerin yurtdışına aktarımı durumunda yeterlilik kararı ve gereken önlemlerin olmaması durumunda oluşabilecek risklere ilişkin bilginin yer alması gerekmektedir.[228]

Güç dengesizliğinin söz konusu olduğu taraflar arasında rıza beyanı alınmak istendiği durumlarda, bilgi ve güç bakımından daha savunmasız konumda olan tarafa

---

[227] Anita L. Allen "An Ethical Duty to Protect One's Own Information Privacy?," *Alabama Law Review*, no.64 (2013): 865.

[228] Article 29 Çalışma Grubu, Guidelines on Consent Under Regulation 2016/679, (2018): 13, https://ec.europa.eu/newsroom/article29/items/623051 , Erişim Tarihi: 28 Mayıs 2022.

bilgilendirme metninin çok sayıda belge ya da uzun sayfalar halinde sunulması durumunda, bilgi almak isteyen tarafın bu sayfalar arasında asıl ihtiyacı olanı bulması ve kendisine sunulan seçenekleri anlayabilmesi zor olduğundan; bireyin gerçekten bilgilendirilip bilgilendirilmediği muğlaktır. Dolayısıyla eksik bilgilendirme sebebiyle verilen rızanın geçerliliği de sorgulanmalıdır.[229]

Bu doğrultuda, Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(c) maddesinde, abone veya kullanıcıdan açık rıza beyanı almadan önce işlenecek olan kişisel, trafik ve konum verilerinin amacı, türü, işleme süresi gibi konularla ilgili bilgilendirme yapılması gerektiğine yer verilerek; ilgili bilgilendirmenin yazılı şekilde yapılması halinde ise aynı Tüketici Hakları Yönetmeliği'nin 7/3 maddesinde belirtilen abonelik sözleşmelerinde olduğu gibi on iki puntoyla yazılması gerektiği belirtilmiştir.

Elektronik haberleşme sektöründe abonelerin veya kullanıcıların diğer sektörlere nazaran daha fazla türde ve sayıda kişisel verisinin işlenmesi sebebiyle, abonelerin kişisel verilerinin işlenmesine rıza göstermelerinin üzerinden vakit geçtikten sonra unutulma ihtimaline karşı, işletmeci tarafından işlenen kişisel verileri hakkında hatırlatma amacıyla abonelere bilgilendirme mesajı gönderilmesiyle ilgili Kişisel Verilerin İşlenmesi Yönetmeliği'nin 13/2 maddesinde, her yılın Temmuz, Ağustos ve Eylül aylarını kapsayan üçüncü çeyreği içerisinde işletmeciler tarafından abonelere veya kullanıcılara GSM numaralarına, GSM numara bilgisi olmayanlara ise e-posta ya da arama yoluyla daha önce vermiş oldukları açık rızaları doğrultusunda kişisel verilerinin işlendiği hakkında kısa mesaj ile bilgilendirme yapılması öngörülmüştür. Söz konusu bilgilendirme yükümlülüğünü yerine getirmeyen işletmecilerin ise abone veya kullanıcılardan aldıkları açık rıza beyanları kapsamında hukuka uygun hale gelen kişisel verileri işleme faaliyetlerini ilgili bilgilendirmeyi yapana kadar durdurması gerekmektedir.

Bir BTK kurul kararında,[230] GSM işletmecilerinin kullanıcılarından tarife ve kampanya değişiklikleri, kişisel verilerin işlenmesine ilişkin hususlar, faturalı-faturasız hat geçiş işlemleri gibi abone açısından hukuki veya ekonomik anlamda sonuçları olabilecek konular hakkında açık rızanın alınması gerektiği hallerde açık rıza, mobil veya

[229] Orla Lynskey, *The Foundations of EU Data Protection Law*, (Oxford: Oxford University Press, 2015), 189.

[230] 24.03.2020 tarih ve 2020/DK-THD/084 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/tuketici-sikayetleri-anlik-bildirimler-pop-up-push-notification-vb-ile-alinan-onay-riza/84-2020-web.pdf , Erişim Tarihi: 29 Mayıs 2022.

SIM uygulaması ya da internet sitesi üzerinden pop-up[231], push notification[232] ve benzeri şekilde alındığında; işletmeci tarafından mevzuata uygun bilgilendirme yükümlülüğünün yerine getirilmesi, aboneye SMS veya anlık ekranda belirecek şekilde gönderilen tek kullanımlık şifrenin abone tarafından bildirim ekranına girilmesi yoluyla doğrulanması, gönderilen bu tek kullanımlık şifreyle ilgili mevzuatta yapılması gereken bilgilendirme ve işlemin adına yer verilmesi gerektiği vurgulanmıştır. Ayrıca rızanın alındığı bildirim ekranında aboneye ret imkanı sunularak; abone tarafından onay verilmesi halinde ise ilgili işlemin yerine getirildiği hakkında ayrıca bir bilgilendirme SMS'i gönderilmesinin zaruri olduğu belirtilmiştir.

Elektronik haberleşme sektöründe belirtilen şartlara ek olarak; abone veya kullanıcıdan açık rıza alınması gereken hallerde, rızanın Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(ç) maddesinde belirtildiği üzere, işletmeci tarafından rızanın alındığı konuya özgü yapılan bilgilendirmenin akabinde, abone veya kullanıcıdan olumlu irade beyanının yalnızca yazılı şekilde veya elektronik ortamda alınabileceğinin belirtilmesi sebebiyle, sözle verilen onayların kabul edilemeyeceği anlaşılmaktadır. Ayrıca rızanın konuya özgü olarak verilmiş olması gerektiği, abone olmak için veya daha sonrasında bir hizmetin kabulüne yönelik verilen rızalarla birleştirilemeyeceği, bununla birlikte rızanın, pazarlama maksadı taşıyan ticari elektronik iletilerin gönderilmesine veya başka bir işleme yönelik verilen rızalarla da beraber alınamayacağı hüküm altına alınmıştır.

---

[231] Pop-up (açılır pencereler), yeni bir reklamcılık ve tanıtım yöntemi olarak, özel bir ürün ya da hizmetin tanıtımını yapmak amacıyla bir internet sitesinde başlatılmaktadır. Açılır pencereler butonlardan farklı olarak bağımsız nitelikte; genellikle tarayıcı penceresinin bir karesini kaplayarak ortaya çıkmaktadır. Esasen, ziyaretçiyi internet ana sayfasından uzaklaştırmadan onların dikkatini çekmek için tasarlanmıştır. Böylece ziyaretçiler, bağımsız bir form veya "banner" ile pop-up ile etkileşim kurabilirken; aynı zamanda etkileşimde bulunabilecekleri veya alışveriş yapabilecekleri internet ana sayfasında kalmaktadır. Ayrıca söz konusu açılır pencereler, potansiyel müşterilerin kişisel müşteri bilgilerini toplama yeteneğine sahiptir. (Jesus Mena, Data Mining Your Website, (Boston: Digital Press Butterworth-Heinemann, 1999), 128.)

[232] Push notifications (anlık bildirimler), ürün kullanıcılarının karşısına çıktığında, kullanıcıyı belirli bir ekrana, internet sayfasına ya da başka bir konuma kısa mesajlar aracılığıyla da gönderebilen gerçek zamanlı bildirimler olarak tanımlanmaktadır. Anlık bildirimlerin amacı, kullanıcıların önemli ya da zamana duyarlı bilgilerden haberdar olmasını sağlamaktır. Söz konusu bildirimler, işletim sistemine ve kullanıcıların etkinleştirdiği bildirim ayarlarına bağlı olarak, kullanıcıların cihaz kilit ekranlarında ya da cihazın bildirim merkezi bölümünde görülmektedir. (Countly, Push Notifications: A Review of Best Practices for Mobile Product Managers, Count.ly. https://count.ly/resources/white-papers/countly_push-notifications-a-review-of-best-practices-for-mobile-product-managers.pdf , Erişim Tarihi: 29 Mayıs 2022.)

3.4. OPT-IN (ÖNCEDEN İZİN ALINARAK) ve OPT-OUT (ÖNCEDEN İZİN ALINMAKSIZIN) GÖNDERİLEN İLETİLER

İnternetin ticari olarak yönlendirme yapabilmeye müsait bir bilgi ve iletişim aracı olması nedeniyle, bireylerin ve şirketlerin, mallarını ve hizmetlerini tanıtmak amacıyla internet aracılığıyla gönderilen elektronik postalardan yararlanıyor olmaları şaşırtıcı değildir. Bu çerçevede reklam ve tanıtım amacıyla elektronik postaların kullanılması şirketler yönünden cazip gelse de istenmeyen reklam (spam)[233] içeriklerinin sayısının her geçen gün artış göstermesi ve milyonları bulması internet ağında kesintilerin oluşmasına sebep olabilmektedir. Ayrıca kullanıcılar, istenmeyen elektronik postaları indirmek, gözden geçirmek, silmek ve yanıtlamak için gereksiz zaman harcamaktadır. İnternet servis sağlayıcıları ise istenmeyen elektronik posta hacmiyle başa çıkabilmek adına, yeni teknolojiler kullanmak zorunda kaldığından, ticari olarak maliyetlerinin artmasını gerekçe göstererek abonelerine ve kullanıcılarına oluşan yüksek ücretleri yansıtmak mecburiyetinde kalmaktadır.[234]

İlgili kişiden rıza beyanları alınma zamanına göre; ileti gönderilmeden önce alınması (opt-in) sistemine göre ve ileti gönderildikten sonra ret seçeneğinin sunulması (opt-out) sistemine göre alınanlar olarak ikiye ayrılmaktadır. Pazarlama yöntemlerinde yaşanan teknolojik gelişmeler doğrultusunda artış yaşanan ve tüketicileri rahatsız edici boyuta ulaşan ileti gönderimlerinin ilk olarak opt-out sisteme göre yapıldığı söylenebilmektedir. Diğer bir deyişle ileti öncelikle alıcıya gönderilmekteydi ve alıcı o şirketten reklam içerikli ileti almak istemediğini belirtmediği sürece de iletiler kendisine gönderilmeye devam edilmekteydi. Alıcıların bu noktada rızalarını susarak, örtülü şekilde verdiği düşünülmekteydi. Ancak iletilerin fazlaca gönderilmesi sebebiyle onayların acele verilmesi, ileti gönderimi için yapılan veri işleme faaliyetinin başka bir hukuka uygunluk sebebine dayanmasına rağmen veri sorumluları tarafından alıcılardan bilinçsizce açık rıza

---

[233] Spam kelimesi, iki avukatın internet üzerinden Usenet (User's Network) olarak adlandırılan haber grubuna bir reklam göndermesiyle, Nisan 1994'te Phoenix-Arizona'da ortaya çıkmıştır. Bu reklam iletisi, yaklaşık yirmi milyon kişiye ulaşarak, iletiye verilen cevapların çok olması nedeniyle internet servis sağlayıcıların sistemlerine zarar vermesiyle sonuçlandı. Söz konusu reklam, avukatların yeni müvekkiller bulmalarını sağlamasa da pazarlama tekniği, para kazanma planları, sağlık ya da kilo verme ve benzeri konulara ilişkin çeşitli ürünler satmayı hedefleyen şirketler arasında hızla yayılarak kullanılmaya başlanmıştır. (Elizabeth A. Alongi, "Has The U.S. Canned Spam?," *Arizona Law Review* 46, no.2 (2004): 263.)

[234] John Magee, "The Law Regulating Unsolicited Commercial E-Mail: An International Perspective," *Santa Clara High Technology Law Journal* 19, no.2 (2003): 380.

alınmak istenmesi ve benzeri çeşitli zararların ortaya çıkması, tüm dünyada opt-out sistemin uygulanabilirliğinin sorgulanmasına yol açmıştır. Bu nedenle opt-out sisteme karşı opt-in sistem geliştirilerek uygulanmaya başlamıştır.

Uluslararası düzenlemeler veya devletlerin hukuk sistemleri tarafından meşru görüldüğü sürece iletilerin opt-out şekilde gönderilmesi de hukuka uygundur. Lakin opt-in rıza beyanının ilgili kişiyi veri işleme konusunda daha fazla bilgilendirdiği açıktır. Bu durum, devletleri genel olarak opt-in sistemi benimsemeye yöneltse de gereksiz yere rıza beyanı talep etme durumunun veri sorumluları açısından maliyet teşkil etmesi doğrultusunda veri işlemekten vazgeçerek veri işlemenin faydalarından uzak kalmaya neden olmaktadır.[235] Bununla birlikte, ilgili kişiler bakımından ise sürekli şekilde kendilerinden rıza istenmesi sebebiyle içeriğe dikkat etmeden bilinçsizce verilen rıza beyanları nedeniyle[236] kişisel verilerin korunmasına aykırılık teşkil eden uygulamalarla karşı karşıya kalmalarına sebebiyet verebilmektedir.

Elektronik Haberleşme Direktifi'ne getirilen değişikliklerle, ileti alanların spam (istenmeyen) ileti gönderen e-posta ve diğer hizmet sağlayıcılarına karşı itiraz süreci başlatabilmelerine imkan sağlanmasının kişilerin mahremiyetinin korunmasının yanı sıra çok sayıda iletinin gönderilememesinden kaynaklı ekonomik bir zarar da ortaya çıkardığı yadsınamaz bir gerçekliktir. Bahsi geçen bu ekonomik zararın başında elektronik iletişim sağlayan hizmet sağlayıcıların istenmeyen ticari iletişimleri (spam) önlemek için yatırım yapma yükümlülüğü gelmektedir. Ayrıca üye devletlerin, istenmeyen iletileri göndererek ihlale sebep olan hizmet sağlayıcılara karşı özel önlem alma amacıyla düzenlemeler yayımlama ve cezalandırma mekanizmalarını da kurmaları gerekmektedir.[237] Bu sebeple hem veri sorumlusu hem de ilgili kişilere rıza beyanı alma ve verme konusunda vazife düşmektedir.

3.4.1. ABD'de Opt-In ve Opt-Out Uygulaması

Kişisel veri işlemeyi her zaman olumsuz anlamda bir faaliyet olarak adlandırmak doğru olmayacaktır. Şirketlerin müşterilerinden kişisel veri işleme faaliyetleri için olumlu onay almaya çalışması, bazen daha maliyetli olmakta ve sosyal açıdan faydalı kullanımları engelleyebilmektedir. Bu doğrultuda, rıza beyanını almaya çalışmanın

[235] Solove, "The Consent Dilemma," 1899.
[236] Misek, "Consent Personal Data," 80.
[237] Kosta, *Data Protection Law*, 377-378.

işleyişi hantal hale getirdiği ve maliyetli olduğu düşünüldüğünde; daha az veri işlemek her zaman doğru mudur ya da veri işleme faaliyetinin faydaları, kişisel verileri korumanın maliyetine göre daha az olsa bile yine de mahremiyeti korumak öncelenmeli midir, şeklindeki bazı sorular akla gelmektedir.[238]

Telefon numaraları, en çok işlenen kişisel verilerdendir. Amerika Birleşik Devletleri'nde (ABD) 1980'li yılların sonlarına doğru telefon yoluyla ürün pazarlama artmaya başlamış; tüketiciler agresif şekilde istenmeyen tele pazarlama aramalarına maruz kalmışlardır.[239] Bu durum, tüketicilerin sürekli şekilde rahatsız edilmelerinin yanı sıra istenmeyen fakslar sebebiyle alıcıların faks makinelerini o sırada kullanamamalarına ek olarak kağıt, mürekkep ve faks makinelerinin yıpranma maliyetlerinin artmasına sebep olmuştur. Yaşanan maddi zararların yanı sıra alıcı kendisine gelen faks mesajını yazdırmadan silse, diğer bir ifadeyle maddi zararı oluşmasa dahi, mesajın reklam mesajı olduğunu anlamak ve silmek için zaman harcanması ve gelen kutusunun istenmeyen mesajlarla dolmasına sebep olunması hali de alıcı için bir kayıp olarak değerlendirilmektedir.[240]

Artan tele pazarlama şirketlerinin suiistimallerinin önlenebilmesi amacıyla ABD'de 1991 yılında Telefon Tüketici Koruma Yasası (Telephone Consumer Protection Act - TCPA) düzenlenmiştir. İlgili düzenleme ile telefon ve faks yoluyla istenmeyen reklam içerikli çağrıların gönderilmesine kısıtlama getirilerek; teknolojik gelişmelerin artmasıyla birlikte kötüye kullanım amaçlı tele pazarlama iletilerinin bireyin rızası olmadan gönderilemeyeceği düzenlenmiştir.[241] Buna göre, acil çağrılar dışında ancak bireyin önceden alınan açık rızası olması halinde arama gerçekleştirilebileceği düzenlenmiştir.[242]

TCPA'nın asıl amacı, teknolojinin istismar edilmeye müsait ve potansiyel olarak tehlikeli addedilebilecek kullanımlarının önüne geçebilmek ve özellikle iletilen mesajların içeriğine odaklanmak yerine istenmeyen faks gönderimi gibi belirli

[238] Solove, "The Consent Dilemma," 1899.
[239] Rebecca I. Yergin, "Consent in The Age of Facebook: Applying The Telephone Consumer Protection Act to Text Messages from Social Media Platforms," *Columbia Law Review Online* 116, (2016): 83.
[240] J. Gregory Sidak, "Does The Telephone Consumer Protection Act Violate Due Process As Applied?," *Florida Law Review* 68, (2016): 1407.
[241] Spencer Weber Waller, Daniel B. Heidtke, Jessica Stewart, "The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology," *Loyola Consumer Law Review* 26, (2014): 347; Yergin, "Consent in Facebook," 81, 83.
[242] Yergin, "Consent in Facebook," 83.

teknolojileri tamamen yasaklayarak; kötüye kullanımların engellenmesini sağlamaktır.[243] Bu doğrultuda, iletiler alıcılara gönderilmeden önce rızalarının alınması hem iletilerin rahatsız ediciliğinden uzaklaşılmasına hem de iletinin gönderildiği telefon numarasının alıcının rızası dahilinde ileti gönderecek tarafla paylaşılmış olmasıyla kişisel verilerin korunmasına katkıda bulunulmuş olur.

3.4.2. Opt-In ve Opt-Out Uygulamasına İlişkin AB Düzenlemeleri

Elektronik Haberleşme Direktifi'nin 13. maddesi, doğrudan pazarlama hakkında istenmeyen iletişimleri düzenler. Söz konusu Direktif'in kapsamında ve hükümlerinde elektronik iletişim hizmeti sağlayıcılarının dahil edildiği belirtilse de ilgili 13. maddenin istenmeyen iletiler gönderen herhangi bir kuruluş için de geçerli olduğu söylenebilir.[244] İlgili hükmün 1. fıkrasında bahsi geçen faks, otomatik çağrı sistemleri gibi belirtilen sistem ve tekniklerin doğrudan pazarlama amaçları için kullanımına ancak ilgili kullanıcıların önceden onayı alındıktan sonra izin verileceği belirtilmektedir. Diğer bir ifadeyle, otomatik arama veya iletişim sistemleri, faks, e-posta, SMS, MMS veya benzeri yöntemlerle doğrudan pazarlama mesajlarının gönderilmesi için genel bir opt-in kuralı ortaya koymaktadır. Article 29 Çalışma Grubu, bir örnek ile konuya açıklık getirerek; varsayılan olarak istenmeyen iletilerin gönderilmesine izin veren bir internet sitesine önceden işaretlenmiş kutucukların yerleştirilmesi suretiyle alıcının eylemsizliği doğrultusunda sonuçlanacak rızayı açıkça ilgili onay kavramından hariç tutmaktadır.[245]

Neredeyse tüm dünyada ileti gönderilmeden önce alıcının rızasının alınmış olmasına yönelik bir sistem olan opt-in sistem tercih edilmeye ve mevzuat da bu doğrultuda hazırlanmaya başlamıştır. Fakat her ne kadar yeni opt-in sistem ile kullanıcılar açısından daha iyi koruma sağlanıyor gibi görünse de açık rıza almaya fazlaca yer verilmesi nedeniyle, verilerin işlenmesi hususu veri sorumlusunun kanuni yükümlülüğü olsa bile alıcıdan gereksiz yere açık rıza alınmaya çalışılmaktadır. Dolayısıyla bu durum ilgili kişilerden gereğinden fazla rıza talep edilmesine ve rıza kurumunun değerinin düşürülmesine sebep olmaktadır.[246] Böylece ilgili kişiler tarafından bilinçsizce verilen

[243] Waller, "The Telephone Consumer," 347.
[244] Eleni Kosta, *Consent in European Data Protection Law*, (Leiden-Boston: Martinus Nijhoff Publishers, 2013), 349.
[245] Kosta, *Data Protection Law*, 358.
[246] Misek, "Consent Personal Data," 80.

rızalara sebebiyle gerçekten önemli olan konular hakkında da acele kararlar verilebilmektedir.

95/46/EC sayılı Direktif'in 14. maddesinde, pazarlama konusunda opt-out sistemin benimsendiği görülmektedir. 2002/58/EC sayılı Elektronik Haberleşme Direktifi'nde ise bunun aksine opt-in sistem benimsenerek; e-posta, otomatik arama sistemleri ve faks yoluyla yapılacak olan pazarlama faaliyetlerinde ileti gönderilmeden önce ilgili kişinin rıza vermiş olması koşulu aranmaktadır; fakat diğer yollarla yapılan pazarlama faaliyetlerinde üye devletler opt-in veya opt-out sistemi benimsemekte özgürdür.[247]

95/46/EC sayılı Veri Koruma Direktifi kişisel verilerin meşru şekilde işlenmesinin nasıl olabileceğine değinirken Elektronik Haberleşme Direktifi ise genellikle bireyin kişisel verilerinin korunmasının ihlal edilebileceği haller olsa bile onayı alındığı vakit kişisel verilerin işlenmesine izin verecek hükümler içermektedir. Bu durum, rıza alınması yoluyla kişisel verilerin korunmasına zarar veren faaliyetlerin meşrulaştırılmasına yol açmakta olup; bireyin kendi rızasının olması haliyle gerekçelendirilmektedir.[248]

GDPR'nin 4/11 maddesinde belirtildiği üzere ise rızanın ancak ilgili kişinin verilerinin işlenmesini onayladığına ilişkin beyanı veya olumlu eylemi ile belirttiği takdirde geçerli olabileceğine değinilerek opt-in sistemin benimsendiği anlaşılmaktadır.[249] İlgili hükümde bireyin sözlü beyanı veya veri sorumlusu tarafından yapılan bilgilendirmenin akabinde kişisel verisini vermesi davranışı da geçerli rıza beyanı olarak kabul edilmektedir. Buna karşılık, GDPR'ın 7. maddesinde belirtilen veri sorumlusunun almış olduğu rıza beyanını ispatla yükümlü olduğu hüküm dikkate alındığında ise söz konusu olumlu davranışın veya sözlü olarak açıklanan beyanın ispatının zor olacağı malumdur. Bu sebeple veri sorumluları genellikle ispatı daha kolay olabilecek yöntemlerle rıza beyanı almayı tercih etmektedir.[250]

Opt-in rıza beyanı, kişisel verisi işlenerek ileti gönderilmek istenen ilgili kişinin ileti almayı kabul ettiğini gösteren olumlu bir davranışı gerektirmektedir. Buna karşılık opt-out rıza beyanında, ilgili kişinin susmasından veya istemediğine ilişkin herhangi bir davranışının olmayışından onay verdiği düşünülerek pazarlama içerikli iletiler

[247] Küzeci, *Kişisel Verilerin Korunması*, 271.
[248] Kosta, *Data Protection Law*, 378.
[249] Küzeci, *Kişisel Verilerin Korunması*, 271.
[250] Ozan Selek, "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 21, no.2 (2019): 929.

gönderilmektedir. Bu halde kişi, ileti almak istemediğine veya kişisel verisinin işlenmesine rızası olmadığını beyan edebilmek için veri sorumlusuna ayrıca bir bildirimde bulunacaktır. Dolayısıyla ilgili kişinin kişisel verilerinin korunması bakımından opt-out uygulaması, opt-in şekilde rıza beyanı alınması sistemine göre daha az koruma sağlamaktadır.[251] Bu sebeple bireylerin varsayılan ayarları değiştirmeye yönelik taleplerinin düşük oranda olması, rıza beyanlarını yönetebilme imkanı sunulmasının önemli olduğu gerçeğini değiştirmemektedir. Bu yöntemin açık şekilde sunulabilmesinin en kolay yolu da opt-in sistemin benimsenmesidir.[252]

3.5. TÜRKİYE'DE OPT-IN SİSTEMİN UYGULANMASI VE İLETİ YÖNETİM SİSTEMİ (İYS)

3.5.1. Ticari Elektronik İleti Kavramı

Elektronik ticaretin artmasıyla birlikte, mal satışı veya üretimi yapan esnaf veya tacirlerin kendilerinden uzakta olan alıcılara da ulaşabilmesi kolaylaşmıştır. Ürünlerin pazarlanma ihtiyacı da aynı doğrultuda artış göstermiştir. Tele pazarlama yöntemi ile başlayan pazarlama serüveni, teknolojinin gelişmesiyle ve AB mevzuatında konuyla ilgili yapılan düzenlemeler doğrultusunda elektronik ortamda gönderilen ticari elektronik iletilere dönüşmüştür.

Ticari elektronik ileti, mal ya da hizmetlerin ticari anlamda pazarlanması veya tanıtılması amacıyla elektronik ortamda elektronik bir adrese gönderilen iletidir.[253] 6563 sayılı Elektronik Ticaretin Düzenlemesi Hakkında Kanun'un[254] 2/1-(c) maddesinde ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in[255] (Ticari Elektronik İleti Yönetmeliği) 4/1-(o) maddesinde ise ticari elektronik ileti, ticari amaçlı elektronik bir ortamda gönderimi sağlanan veri, ses ve görüntülerin bulunduğu ileti şeklinde tanımlanmıştır. Söz konusu maddelerde yer verildiği üzere bu iletiler faks, telefon, e-posta, SMS gibi araç veya sistemler yoluyla gönderilebilmektedir.

---

[251] Küzeci, *Kişisel Verilerin Korunması*, 270-271.
[252] Lynskey, *Data Protection Law*, 187.
[253] Commercial Electronic Mail Message, https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-941144812-289124299&term_occur=2&term_src=title:15:chapter:103:section:7702 . Erişim Tarihi: 1 Haziran 2022.
[254] R.G. 05.11.2014, S. 29166.
[255] R.G. 15.07.2015, S. 29417.

3.5.2. Ticari Elektronik İletilere Opt-In Sistemin Uygulanması ve İleti Yönetim Sisteminin Ortaya Çıkışı

Ticari elektronik iletiler, başlangıçta herkese gönderilmekteyken; tüketicilerin sürekli reklam mesajlarına maruz kalması hem rahatsız olmalarına hem de kişisel verilerinin kendi rızalarının olmadığı kişilerin eline geçtiği düşüncesiyle ileti almak istememelerine sebep olmuştur. Bunun akabinde, neredeyse dünyanın her yerinde bu soruna çözüm arayışları başlamış ve bu konuda düzenleme yapılma ihtiyacı hissedilmiştir.

Yapılan düzenlemeler çerçevesinde genellikle, e-posta yoluyla ticari elektronik ileti gönderiminde her iletinin içeriğinde alıcıya ücretsiz ve kolay şekilde, en azından aynı iletişim yöntemi ile ileti almayı reddetme imkanı sunulması gerektiği kabul edilmektedir. SMS yoluyla gönderilen ticari elektronik iletilerde ise reddetme imkanının SMS'i gönderen hizmet sağlayıcıya tahsis edilen numaraya alıcının ileti almak istemediğine ilişkin beyanını göndermesi yoluyla sunulması yeterli olarak kabul edilmektedir.[256]

Opt-out sistem ile ileti gönderildikten sonra alıcının onayı bulunmaması halinde bir daha ileti gönderilmemesi yönteminin denenmesinin ardından; ilk iletinin rıza dışı gönderilmesinin sebebinin ne olduğu sorusunun akla gelmesiyle birlikte; uygun olan yöntemin opt-in sistem olabileceği düşünülmüştür. Opt-in, diğer bir deyişle kişinin rızası olmadan ileti gönderilememesi yöntemiyle birlikte tüketiciler bir nebze nefes alsa da ilgili yöntemin tacirler açısından problemler teşkil ettiği hususlara bu çalışmanın önceki bölümlerinde yer verilmiştir.

Sonuç olarak, opt-in sistemin temelinde, ileti gönderilmeden önce alıcıya ileti almak isteyip istemediğinin sorulması bulunmaktadır. Nitekim bu irade beyanının da ileti gönderilerek değil, kişiden bizzat alınması gerekmektedir. Genel olarak opt-in sistemi benimseyen ülkelerin hukuk kurallarına göre, ancak olumlu irade beyanını ileti gönderene daha önceden bildiren alıcılara gönderilen iletiler hukuka uygun kabul edilmektedir. Bu noktada iletinin hukuka uygun olup olmamasının da alıcılara istenmeyen iletilerin gönderilmesine engel olamadığı anlaşıldıktan sonra devletler bu irade beyanlarının yönetilebildiği sistemlerin kurulması gerektiği kanaatine varmışlardır. Bu doğrultuda ülkemizde de 7061 sayılı Kanun[257] ile 6563 sayılı Kanun'da yapılan değişiklik ile 11.

[256] Kosta, *Data Protection Law*, 373.
[257] R.G. 05.12.2017, S. 30261.

maddeye 4. fıkra hükmü eklenerek tüketicilere ileti onayı verme ve reddetme imkanının tanınacağı bir sistem kurulması kararlaştırılmıştır. Böylece İleti Yönetim Sistemi oluşturulmuştur.

Ticari Elektronik İleti Yönetmeliği'nin 4/1-(ö) maddesinde ileti yönetim sistemi, hizmet sağlayıcıların ileti onayı alabilmesi ve tüketicilerin reddetme hakkını kullanabileceği, aynı zamanda şikâyet süreçlerinin de yürütülebileceği bir sistem olarak tanımlanmaktadır.

3.5.3. Elektronik Haberleşme Sektöründeki İşletmecilerin Ticari Elektronik İleti Yönetmeliği ve İleti Yönetim Sistemindeki Konumu

Ticari Elektronik İleti Yönetmeliği'nin 2/2-(a) maddesinde, 5809 sayılı EHK kapsamında faaliyet gösteren işletmecilerin, kendi abonelerine veya kullanıcılarına hizmetlerini pazarlama veya şirketini tanıtma amaçlı göndermiş oldukları iletilerin ilgili Yönetmelik kapsamında olmadığı belirtilmiştir. Söz konusu hüküm doğrultusunda, elektronik haberleşme sektörü işletmecilerinin abonelerine göndermiş oldukları iletiler, tür olarak ticari elektronik ileti olsa da bu işletmeciler tarafından abone veya kullanıcılarına gönderildiği için Yönetmelik kapsamı dışında tutulmakta; bu sebeple de ilgili Yönetmelik'te bahsi geçen bir ticari iletinin taşıması gereken unsurları taşıyıp taşımadığı, alıcının önceden onayının alınıp alınmadığı gibi hususlara aykırılık teşkil etse dahi elektronik haberleşme sektöründeki işletmeciler hakkında idari soruşturma başlatılamamaktadır.

Ticari Elektronik İleti Yönetmeliği'nin 11. maddesinde aracı hizmet sağlayıcıların yükümlülüklerine yer verilmiştir. İlgili hüküm doğrultusunda aracı hizmet sağlayıcı, hizmet sağlayıcının kendi yükümlülüklerini yerine getirebilmesi için gereken teknik imkanı sağlamakla yükümlendirilmiştir. İletinin içeriğinin hukuka uygun şekilde düzenlenip düzenlenmediğinin kontrolünü yapma görevi bulunmamaktadır. Hizmet sağlayıcı, kendisi iletiyi gönderebileceği gibi aracı hizmet sağlayıcı vasıtasıyla da iletinin gönderimini sağlayabilir. Fakat bu durumda aracı hizmet sağlayıcı, ticari elektronik ileti gönderimi için hizmet sağlayıcı adına alıcılardan onay alamaz. İlgili hükmün devamında, aracı hizmet sağlayıcıların sistemlerini İYS'ye uyumlaştırmaları gerektiğine yer verilerek aracı hizmet sağlayıcının abonesi olan ve ticari elektronik ileti göndermek isteyen hizmet sağlayıcılardan İYS'ye kaydolmayanların iletilerini gönderemeyecekleri belirtilmiştir. Bu kontrolün akabinde, İYS'ye kayıtlı olan hizmet sağlayıcı ileti göndermek istediğini

aracı hizmet sağlayıcıya ilettiği takdirde ise aracı hizmet sağlayıcı gönderimi başlatmak zorundadır. Gönderim aşamasında aracı hizmet sağlayıcıya düşen bir diğer görev, alıcıların İYS'ye kayıtlı onaylarının bulunup bulunmadığının kontrolüdür. Alıcıların, ileti göndermek isteyen hizmet sağlayıcıya daha önceden vermiş olduğu ve İYS'ye kaydedilmiş onayı bulunmadığında, ilgili alıcıya söz konusu iletinin gönderilmemesi konusunda aracı hizmet sağlayıcı yükümlü kılınmıştır. Fakat alıcının onayının gerekmediği hallerden olan ilgili Yönetmeliğin 6. maddesinin 1., 2. ve 4. fıkralarında yer verilen, alıcının kendisinin iletişim bilgilerini verdiği ve hizmet sağlayıcının sunduğu hizmet veya mala ilişkin kullanım, değişiklik veya bakım durumlarıyla ilgili ileti gönderilmesi halinde, devam etmekte olan üyeliğe ilişkin borç bilgilendirmesi yapılması, teslimat gibi durumlar veya sermaye piyasası mevzuatına dayanarak yapılan aracılık yapan şirketlerin kendi müşterilerine göndermek istedikleri bilgilendirme iletilerinin varlığı halinde; aracı hizmet sağlayıcı tarafından hizmet sağlayıcıdan söz konusu hallerin varlığı sebebiyle alıcının onayını almadığına ilişkin beyan alınması gerekmektedir. Bunun yanı sıra aboneliği kapanan-fesholan alıcıların numaraları da İYS'ye yine aracı hizmet sağlayıcılar tarafından bildirilmektedir.[258]

Elektronik haberleşme sektöründeki işletmecilerin, Ticari Elektronik İleti Yönetmeliği kapsamındaki yeri aslında belirsizdir. Şöyle ki; aracı hizmet sağlayıcılar, 6563 sayılı Kanun'un 2/1-(d) ve ilgili Yönetmeliğin 4/1-(b) maddelerinde başkalarının ticaret yapması için elektronik ticaret ortamını sağlayan kişiler olarak tanımlanmıştır. İlgili tanım incelendiğinde, aracı hizmet sağlayıcının e-ticaret sayfasını hazırlayan yazılım firması olduğu akla gelmekte olup; söz konusu Yönetmeliğin 11. maddesinde aracı hizmet sağlayıcılara verilen yükümlülüklerin kapsamı düşünüldüğünde; aracı hizmet sağlayıcının elektronik haberleşme sektöründeki işletmecilerden başkasının olamayacağı anlaşılmaktadır. Anayasa'nın 22. maddesinde yer verilen haberleşmenin gizliliği ilkesi ve elektronik haberleşme mevzuatının genel hükümleri doğrultusunda, elektronik haberleşme sektöründeki işletmecilerin asıl görevinin gönderen ve alıcı arasındaki haberleşmeyi sağlamak olduğu anlaşılmaktadır. Diğer bir deyişle, 6563 sayılı Kanun ve Ticari Elektronik İleti Yönetmeliği'nde yer verilen tanımın kapsamının çok

[258] Ticari Elektronik İleti Yönetmeliği'nin 17/A maddesinde belirtildiği üzere, e-posta şeklinde gönderilecek ticari elektronik iletilerde ise aracı hizmet sağlayıcılar, İYS üzerinden hizmet sağlayıcının İYS'ye kayıt durumunu veya alıcının onayını sorgulama gibi İYS üzerinden yapması gereken hususları yerine getirmekle yükümlü kılınmamıştır.

daha geniş olduğu[259], ticaretin yapılmasına ortam sağlayan şirketlerden bahsedildiği fark edilmektedir.[260]

3.5.4. Ticari Elektronik İleti ve İleti Yönetim Sistemi'nin KVKK Bağlamında İncelenmesi

KVKK'nın 2016 yılında, 6563 sayılı Kanun'un ise 2014 yılında yayımlandığı ve ticari elektronik iletilerin alıcılara gönderilebilmesi için çokça kişisel veri işlendiği düşünüldüğünde; kişisel verilerin korunması konusunda 6563 sayılı Kanun'un 10. maddesinde yer alan özel nitelikli hükmün mü yoksa daha genel nitelikte hükümler içeren KVKK'nın mı uygulanacağı belirsizlik teşkil etmekteydi. 2014 yılından 2016 yılına kadar ticari elektronik iletilere ilişkin kişisel verilerin korunması konusunda başka hüküm bulunmadığından; konuyla ilgili kanun olan 6563 sayılı Kanun hükümleri uygulanmıştır.

6563 sayılı Kanun'un 10. madde hükmü ile ileti göndermek isteyen hizmet sağlayıcılar ve gönderim konusunda hizmet sağlayıcıya ortam sağlayan aracı hizmet sağlayıcının ticari elektronik iletilerin gönderimi çerçevesinde edindikleri kişisel verilerin saklanmasından sorumlu olduklarının belirtilmesinin yanı sıra kişisel veri sahibinin onayı olmadığı sürece üçüncü kişilerle paylaşılamayacağına ve alınan onayın belirtilen amacın dışında başka bir amaç için kullanılamayacağına yer verilmiştir.

2016 yılından sonra ise ticari elektronik iletilere uygulanacak kişisel verilerin korunması konusunda uygulanacak hüküm olaya göre farklılık gösterebileceğinden; yeri geldiğinde KVKK, yeri geldiğinde ise 6563 sayılı Kanun'un 10. madde hükmü uygulama alanı bulmuştur. 6563 sayılı Kanun'da alıcıdan alınacak onaya ilişkin 6. maddede belirtildiği üzere onay, yazılı şekilde ya da elektronik iletişim aracı vasıtasıyla alınabilmekte olup; 11/4 maddesinde belirtildiği üzere, alıcılardan alınan onayların İYS'ye kaydedilmediği sürece geçersiz kabul edileceğine yer verilmiştir. KVKK'da ise rızanın yalnızca açık şekilde alınması gerektiği düşünüldüğünde; 6563 sayılı Kanun'da rızaya ilişkin daha ayrıntılı düzenlemeler yer alması sebebiyle, ticari elektronik ileti onayı alınması konusunda daha özel nitelikteki 6563 sayılı Kanun hükümleri uygulanabilecektir. Bunun yanı sıra rıza-onay kavramının ne demek olduğuna ise

[259] Ticari Elektronik İleti Yönetmelik hükümlerinin işleyişinin devamlılığı için, uygulamada elektronik haberleşme sektöründeki işletmecilerin aracı hizmet sağlayıcı olduğu düşünüldüğünden; bu çalışmada da ticari elektronik iletiler bakımından işletmecilerin rolü aracı hizmet sağlayıcı olarak anılacaktır.
[260] Mahmut Furkan Balaban, "İleti Yönetim Sisteminin Kurulması ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in Değerlendirilmesi," *Bilişim Hukuku Dergisi* 2, no.2 (2020): 204-205.

yalnızca KVKK'da yer verildiği düşünüldüğünde; her iki kanunun da yerine göre birlikte veya ayrı ayrı uygulanabilir olduğu görülecektir.[261]

Söz konusu uygulama belirsizliğinin ortadan kaldırılabilmesi amacıyla, 7416 sayılı Kanun'un[262] 4. maddesi ile getirilen düzenlemenin 1 Ocak 2023 tarihinde yürürlüğe girmesiyle, ilgili 6563 sayılı Kanun'un 10. maddesi tamamen yürürlükten kaldırılmıştır. Böylece artık kişisel verilerin korunması konusunda 6563 sayılı Kanun'un mu yoksa 6698 sayılı KVKK'nın mı uygulanacağına dair tartışmaya konu olabilecek hüküm bulunmamakta olup; yalnızca KVKK uygulanmaya devam edecektir.

İleti Yönetim Sistemi A.Ş.'nin, kişisel verilerin korunması bağlamında rolü incelendiğinde; KVKK'nın 12/2 maddesinde belirtilen, veri sorumlusunun işlemekte olduğu verilerin kendi adına başka bir kişi tarafından işlenmesi halinde; verilerin saklanması, işlenmesi ve verilere erişilmesi konularında işleyen kişinin de veri sorumlusuyla birlikte sorumluluğunun olduğuna ilişkin hüküm doğrultusunda değerlendirilme yapılması gerekmektedir. Ticari elektronik ileti gönderebilmek için telefon numarası verileri bakımından hizmet sağlayıcının veri sorumlusu, aracı hizmet sağlayıcının ise ilgili iletileri göndermekle görevli olmaktan kaynaklı veri işleyen olduğu göz önünde bulundurulduğunda; aracı hizmet sağlayıcıların ileti gönderimi esnasında alıcıların onayının bulunup bulunmadığını sorgulama amacıyla telefon numaralarını ileti yönetim sistemi üzerinden sorgulamasına yönelik işleme faaliyetinde, özel hukuk tüzel kişisi olan İleti Yönetim Sistemi A.Ş.'nin de ileti gönderimine konu olan telefon numaralarını saklamakla yükümlü olması sebebiyle hizmet sağlayıcısıyla müştereken sorumluluğunun bulunduğu açıktır.[263]

[261] Balaban, "İleti Yönetim Sistemi," 211-212; Polater, "Hukuka Uygunluk Sebepleri," 5; Çekin, *KVK Hukuku*, 218-219; Mehmet Bedii Kaya, *Elektronik Ticaret Hukuku Ticari Elektronik İletiler*, (İstanbul: On İki Levha Yayıncılık, 2020): 159.
[262] R.G. 7.7.2022, S. 31889.
[263] Balaban, "İleti Yönetim Sistemi," 213.

4. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERE İLİŞKİN AYDINLATMA METNİ SUNULMASI

4.1. AYDINLATMA METNİNİN ŞEFFAFLIK İLKESİYLE İLİŞKİSİ

Aboneye veya kullanıcıya sunulan aydınlatma metni, esasen şeffaflık ilkesinin yerine getirilmesi amacını taşımaktadır. Şeffaflık ilkesi, veri sahiplerinin kişisel verilerinin hukuka uygun olarak işlenmesi ve söz konusu verilerin nasıl işlendiği konusunda bilgilendirilmelerini içerir. Bu doğrultuda, verilerin işleme süreçlerinde şeffaflığın sağlandığı bir mekanizma ile veri işlendiği konusunda veri sahibinin bir endişe taşımaması gerekir.[264]

GDPR'da kişisel verilerin şeffaflık ilkesi çerçevesinde işlenmesi hususuna, genel ilkelerden bahsedilen 5/1 maddesindeki *"Kişisel veriler: (a) veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir ('hukuka uygunluk, adalet ve şeffaflık');"* hükmü ile değinilmiştir. Bu ilke, iç hukukumuza KVKK'nın 4/2-(a) maddesiyle getirilmiş olup; ilgili hükümde belirtildiği üzere, kişisel verilerin hukuka ve dürüstlük kurallarına uygun şekilde işlenmesi gerekmektedir.

Kişisel verilerin hukuka uygun şekilde işlenmesi, kişisel verilerin korunması hukuku mevzuatının yanı sıra genel hukuk kurallarına ilişkin ulusal ve uluslararası kurallara da uygun olma anlamına gelmektedir. 4721 sayılı Türk Medeni Kanunu'nun (TMK)[265] 2. maddesi olan dürüstlük kuralıyla, diğer hukuk kurallarının bireylere yüklediği yükümlülüklerin bu kural çerçevesinde yerine getirilmesi; aksi haldeki davranışların hakkın kötüye kullanılması anlamına geleceği vurgusu yapılmaktadır. Genel nitelikte yapılan bu tanımın kişisel verilerin işlenmesi konusuna yansıması, veri sorumluları ve veri işleyenlerin kişisel verileri işleme sürecindeki yükümlülüklerini yerine getirirken dürüstlük kuralına uygun hareket etmeleri şeklinde olmaktadır.[266] Kişisel verisi işlenen ilgili kişinin makul beklentileri ve menfaatleri doğrultusunda veri

[264] Dayana Spagnuelo, Ana Ferreira, Gabriele Lenzini, "Transparency Enhancing Tools and the GDPR: Do They Match?," iç. *Information Systems Security and Privacy ICISSP 2019*, ed. Paolo Mori, Steven Furnell, Olivier Camp, Communications in Computer and Information Science 1221, (Prague: Springer Cham, 2020), 162-163.
[265] R.G. 08.12.2001, S. 24607.
[266] Göçmen Uyarer, *KVKK*, 123.

sorumlusunun ilgili kişiyi bilgilendirerek işleme faaliyetini gerçekleştirmesi gerekmektedir.[267]

4.2. AYDINLATMA METNİYLE BİLGİLENDİRME YÜKÜMLÜLÜĞÜNÜN YERİNE GETİRİLMESİ

KVKK'nın 10. maddesinde, veri sorumlusu veya veri işleyenin kişisel verisini işlediği ilgili kişileri, veri sorumlusunun veya temsilcisinin kimlik bilgisi, kişisel verileri hangi amaçla işledikleri, kimlere hangi amaçlarla aktardıkları, kişisel verileri veri sahiplerinden toplamalarındaki hukuki sebep ve yöntemleri ve ilgili kişinin sahip olduğu haklar bakımından bilgi vermekle yükümlü olduğu düzenlenmiştir.

Elektronik haberleşme sektöründeki işletmecilerin bilgilendirme yükümlülüğü ile ilgili, Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(c) maddesinde abone veya kullanıcıdan açık rıza alınmadan önce işletmecinin işleyeceği kişisel verilerin neler olduğu, hangi trafik ve konum verilerinin işleneceği, işleme faaliyetinin amacı, kapsamı ve süresi konusunda abone veya kullanıcının açık ve anlaşılır bir şekilde bilgilendirilmesi gerektiği hüküm altına alınmıştır. Ayrıca ilgili hükümde söz konusu bilgilendirmenin yazılı olması durumunda metnin en az on iki punto ile yazılması gerektiği belirtilmiştir. Ayrıca aynı Yönetmeliği'nin 9. maddesinde ise KVKK'nın 10. maddesinde belirtilen haller haricinde, konum ve trafik verisini işleyen işletmeciler, işleme faaliyetine ilişkin veri türü, amaç ve işleme süresi konusunda abone veya kullanıcıları bilgilendirmekle yükümlü kılınmıştır.

Aydınlatma yükümlülüğü, veri sorumlusu için bir yükümlülük iken; veri sahibi için bir hak olduğu söylenebilir.[268] Veri sorumlusunun aydınlatma yükümlülüğüne ilişkin düzenlemenin detayları KVK Kurulu tarafından yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de[269] (Aydınlatma Yükümlülüğüne İlişkin Tebliğ) düzenlenmiştir.

---

[267] KVK Kurumu, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler , 2, Erişim Tarihi: 18 Haziran 2022.

[268] KVK Kurumu, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, Nisan 2019, 3, 6, https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi , Erişim Tarihi: 18 Haziran 2022.

[269] R.G. 10.03.2018, S. 30356.

4.2.1. Aydınlatma Metninin İçeriği

Aydınlatma Yükümlülüğüne İlişkin Tebliğ'in 5. maddesi elektronik haberleşme sektörü açısından değerlendirildiğinde; öncelikle işletmecilerin, hizmet verdikleri abonelere ve henüz hizmet vermeseler dahi abone adaylarına, sundukları hizmetler gereğince aboneye daha iyi hizmet verebilmek amacıyla işledikleri veya kanunen işlemekle yükümlü oldukları kişisel verilerin hangi amaçlarla ve ne kadar süre işlendiği, kimlere aktarıldığı hususlarının ayrıntılarından aydınlatma metinlerinde bahsetmeleri gerektiği anlaşılmaktadır. Abone veya abone adayına yapılan bu bilgilendirme, kimi zaman işletmecinin abone merkezlerine gelmiş olan kişilere sözlü olarak veya yazılı metinlerle kimi zaman ise işletmecinin internet sayfası üzerinde yapılan veya çağrı merkezini arayan kişilere dinletilen bilgilendirme metinleri yoluyla yapılabilmektedir. Ayrıca kişisel verinin işlendiği her durum için ilgili kişinin bilgilendirilmesi koşulunun yanı sıra işleme amacının değişmesi halinde ise aydınlatma metinlerinin güncellenmesi ve aynı işletmeci de olsa kişisel veriyi işleyen birimlerin işleme amaçlarının farklı olması halinde birim bazında aydınlatma yükümlülüğünün yerine getiriliyor olması koşulları göz önünde bulundurulduğunda; elektronik haberleşme sektöründeki işletmeciler açısından kişisel verinin işlenmesi kadar abone veya abone olmak isteyen abone adayını bilgilendirmek açısından aydınlatma metinleriyle tam ve doğru bilgilendirme yapılması da bir o kadar önem teşkil etmektedir.

4.2.2. VERBİS Kayıtlarıyla Uyumlu Olma Zorunluluğu

Aydınlatma Yükümlülüğüne İlişkin Tebliğ'in 5. madde hükmünün devamı elektronik haberleşme sektörü bakımından incelendiğinde, Veri Sorumluları Sicil Bilgi Sistemi'ne (VERBİS)[270] kayıt yükümlülüğü olan elektronik haberleşme sektöründeki işletmecilerin işlemekte olduğu kişisel verilere ilişkin VERBİS'te yayımladığı bilgilerle, yukarıda ayrıntılarından bahsedilen kanallarla yapmış olduğu bilgilendirmenin birbiriyle uyumlu olması gerektiği anlaşılmaktadır. Bununla birlikte, işletmecinin işlemekte olduğu kişisel veriler hakkında yaptığı bu bilgilendirme, ilgili kişinin talebi olmasa da yapılmak

[270] VERBİS, KVKK'nın 16. maddesinde belirtildiği üzere, veri sorumlusu olan gerçek veya tüzel kişilerin kişisel verileri işlemeden önce ilgili sisteme kaydolarak; işledikleri kişisel verileri hangi amaçlarla ve hangi sürelerde işledikleri, kimlere aktardıklarına ilişkin ayrıntılı bilgilendirmeyi yaptıkları kayıt sistemidir. KVK Kurumu, Sorularla VERBİS, https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf , 4, Erişim Tarihi: 20 Haziran 2022.

zorundadır. İşletmecinin yapmış olduğu bilgilendirmenin ispat yükü de yine veri sorumlusu olan işletmecinin kendisindedir.

4.2.3. Bilgilendirmenin Açıklığı

Aydınlatma Yükümlülüğüne İlişkin Tebliğ'in 5. maddesinin elektronik haberleşme sektörü açısından nasıl uygulanacağına ilişkin söz konusu hüküm incelenmeye devam edildiğinde; işletmecinin KVKK'nın 5/2 maddesinde sayılan haller haricinde abonenin kişisel verisini işlemeden önce açık rızasını alması gerektiği durumlarda, aboneden açık rıza alınmasının yanı sıra aydınlatma yükümlülüğünün ayrıca yerine getirilmesi gerekmekle birlikte, aydınlatma yükümlülüğünün yerine getirilmiş olmasının, açık rıza alındığı anlamına gelmediği anlaşılmaktadır. Nitekim Kişisel Verileri Koruma Kurulu Amazon Türkiye kararında[271], Amazon'a üye olurken kullanıcılara onaylatılan Gizlilik Bildirimi ile birlikte yalnızca bilgilendirme yükümlülüğünün yerine getirilmiş sayılacağı, bu bilgilendirmenin Amazon'un açık rıza almasına ilişkin yükümlülüğünü ortadan kaldırmayacağı belirtilmektedir.

4.2.4. Tam ve Doğru Bilgilendirme

Şeffaflık ilkesinin bir gereği olarak aydınlatma yükümlülüğünü yerine getirmesi gereken elektronik haberleşme sektöründe faaliyet gösteren işletmecinin, abonelerin kişisel verilerini işleme amaçlarının belirli, açık ve meşru olması, muğlak ifadelere yer verilmemiş olması, bildirimin dilinin anlaşılır, sade ve açık olması gerektiği, Aydınlatma Yükümlülüğüne İlişkin Tebliğ'in 5. maddesi elektronik haberleşme sektörüne göre incelendiğinde görülmektedir. Bununla birlikte, elektronik haberleşme sektöründeki ilgili kişi olan abone adayı veya abonenin kişisel verilerinin işletmeci tarafından KVKK'nın 5. ve 6. maddelerinden hangisine dayanılarak işlendiği hakkındaki hukuki sebepler aydınlatma metninde açıkça belirtilmelidir.

4.2.5. Kişisel Verilerin Aktarılması Konusunda Bilgilendirme Yapılması

Aydınlatma Yükümlülüğüne İlişkin Tebliğ'in 5. maddesi kapsamında ilgili kişiyi bilgilendirmek gereken bir başka husus da kişisel verilerin kimlere aktarıldığıdır. Bu sebeple işletmeciler, veri sahibi abone adayı veya abonelerin kişisel verilerini

[271] KVK Kurulu, Amazon Turkey Kararı.

aktardıkları, sunulan ürün ve hizmetlerin aboneye ulaştırılabilmesi amacıyla çalışma yapılan iş ortakları veya tedarikçiler, abone tarafından acil yardım çağrısı yapılması halinde konum tespiti yapacak olan yetkili merciler, kişisel verilerini talep edebilmesi için yetkilendirilmiş olan kamu kurum ve kuruluşları, mobil hat kullanarak hizmet alan abonelerin bankacılık işlemleri sırasında işlem güvenliğinin sağlanabilmesi ve kimlik doğrulama amaçlarıyla ilgili kurum ve kuruluşlara bilgi aktarımı yapılabilmektedir. Buna ilişkin bilgilendirmelere, sicile kayıt yükümlülüğü olan işletmeciler açısından her ne kadar VERBİS'te yer verilse de işletmecilerin kendi internet sayfalarında da VERBİS'teki bilgilendirmeye uygun olacak şekilde aydınlatma metinleri bulunmaktadır.[272] Ayrıca ilgili tebliğin 5.maddesinin (i) bendi uyarınca işletmeciler, yayımladığı aydınlatma metinlerinde işlemekte oldukları kişisel verileri otomatik veya bir veri kayıt sistemine dahil edilmek suretiyle hangi otomatik olmayan yoldan edinildiğini açıkça belirtmelidir. İlgili hükmün son bendi gereğince ise; ilgili kişilerin beklentileri doğrultusunda ve yanıltıcı ifadelerden uzak olacak şekilde tam ve doğru bilgilendirme yapılmalı, yanlış bilgilendirme yapılmamalıdır.

4.2.6. Abonelik Tesisinden Sonra Abonenin Bilgilendirilmeye Devam Edilmesi

Yalnızca abonelik başlatılmadan önce değil, abonelik başlatıldıktan sonra da abone, işletmeci tarafından hangi kişisel verilerinin işlendiğini sorgulayabilmektedir. Bu tür durumlarda abone, genellikle işletmecinin internet sayfasında bulunan aydınlatma metnine yönlendirilmektedir. Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin aydınlatma metinlerinde genel olarak; aboneliğin oluşturulabilmesi amacıyla alınan kişisel verilerin yanı sıra aboneliğin kullanımına bağlı olarak ortaya çıkan kişisel verilerin hangi metot, amaç ve sürelerde işlendiği, kişisel verileri işlemeye dayanak gösterilen hukuki sebepler, aktarılan alıcı grupları diğer bir deyişle kimlerle paylaşıldığı hususlarının ayrıntıları yer almaktadır. Ayrıca KVKK'nın 11. maddesi

[272] Türk Telekomünikasyon A.Ş., Aydınlatma Metni - Kişisel Verilerin Aktarılması, https://bireysel.turktelekom.com.tr/mobil/sayfalar/gizlilik-ve-guvenlik.aspx ; Netgsm A.Ş., Aydınlatma Metni - Kişisel Verilerinizin Aktarıldığı Taraflar ve Aktarım Amaçları, https://www.netgsm.com.tr/gizlilik-ve-guvenlik/ ; Vodafone Telekomünikasyon A.Ş. Aydınlatma Metni - Kişisel Verilerin Aktarıldığı Alıcı Grupları, https://www.vodafone.com.tr/VodafoneHakkinda/gizlilik-ve-guvenlik-politikalari , Erişim Tarihi: 25 Haziran 2022.

uyarınca, ilgili kişinin haklarını kullanabileceği ve daha detaylı bilgi alabileceği kanallar hakkında da bilgilendirme yapılmaktadır.[273]

5. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ÇEREZ POLİTİKASI

5.1. ÇEREZ KAVRAMI VE TÜRLERİ

5.1.1. Çerez Kavramı

Bireyler verilerinin nasıl kullanıldığını bilme ve bu verilere ilişkin karar verme hakkına sahip olup; mahremiyetlerini ilgilendiren süreçleri kendileri yönetmek istemektedir. Aksi halde kendilerini özgürlükleri kısıtlanmış ve savunmasız hissetmeleri söz konusudur. Kimileri sosyal medya hesaplarını yalnızca tanıdığı kişilerin görebileceği şekilde kullanırken; kimileri de paylaşımlarının herkes tarafından görülebilir olmasını tercih etmektedir. Sosyal medya hesaplarının gizliliği hakkında herkes az da olsa bilgi sahibi olup; bu hesaplarını yönetmek için vakit ayırsa da ziyaret ettikleri internet sayfalarında kendileri hakkında hangi verilerin işlendiğini inceleme ve yönetme zahmetinde bulunmamaktadır.[274]

Çerezler, internet sitelerinde gezinen kullanıcıların cihazlarına internet sitesi operatörleri tarafından aktarılan, Hiper Metin Transfer Protokolü - Hyper Text Transfer Protocol (HTTP)'nin bir bölümü olan, boyutları küçük metin şeklindeki dosyalar olarak adlandırılır. Bir başka deyişle, kullanıcılar web sitelerinde bir sayfayı ziyaret ettiğinde, terminal cihazlarına yerleştirilen metin halindeki bilgiler vasıtasıyla kullanıcının tanınabilir olmasını sağlayan bilgilere çerez adı verilir.[275] Diğer bir tanıma göre ise çerez, bir internet sunucusu tarafından bir internet tarayıcısında saklanmak üzere gönderilen küçük bilgi parçasıdır.[276]

---

[273] Turkcell İletişim Hizmetleri A.Ş., Aydınlatma Metni - Kişisel Verilerin Aktarılması, https://www.turkcell.com.tr/tr/gizlilik-ve-guvenlik?page=kisisel-verilerin-korunmasi , Erişim Tarihi: 25 Haziran 2022.

[274] Solove, "The Consent Dilemma," 1900.

[275] KVK Kurumu, Çerez Uygulamaları Hakkında Rehber, Haziran 2022, 8, https://www.kvkk.gov.tr/Icerik/7353/Cerez-Uygulamalari-Hakkinda-Rehber , Erişim Tarihi: 3 Temmuz 2022.

[276] Brian Pennington, "New Technology Briefing: Cookies-Are They a Tool for Web Marketers or a Breach of Privacy?," *Interactive Marketing* 2, no.3 (2001): 251.

Kullanıcının bir internet sitesine girebilmek için kullandığı tarayıcı, sunucuya talebi iletmesinin akabinde kullanıcının talep ettiği bilgilere ek olarak kullanıcının bilgileri de söz konusu web tarayıcısına gönderilmektedir. Söz konusu web tarayıcı, kullanıcının geçmiş eylemlerinin yanı sıra aynı web tarayıcısında ziyaret edilen diğer internet sayfalarındaki davranışları birleştirerek; kullanıcı hakkında bilgi edinilmesini sağlamaktadır. Böylece çerezler vasıtasıyla kullanıcıların tercihleri tespit edilerek depolanmaktadır.[277] Bilgisayar kullanıcılarının cihazlarında çeşitli türde veriler depolanması, esasen kullanıcı açısından bir risk teşkil etmez. Buradaki temel risk, çerezler vasıtasıyla elde edilen verilerin bilgisayar kullanıcısına zarar verecek şekilde kullanılma riskidir. Çerezler aracılığıyla yapılan izleme faaliyetleri ile elde edilen kişisel veriler, kullanıcıların gizliliklerinin ihlal edilmesine sebep olabilir. Bir kişinin kimliğiyle ilişkilendirilebilecek verilerin kişisel veri olduğundan hareketle, kullanıcıların bilinçli ya da bilinçsiz olarak kişisel verilerinin işlendiğinin farkında olması gerekir.[278]

Hayatın her alanında olan teknoloji ve haberleşme ihtiyacı düşünüldüğünde, bireylerin bunlardan yararlanabilmek adına kişisel verilerin işlenmesi konusunda veri paylaşımında bulunduğu telekom operatörleri, internet servis sağlayıcıları, bulut hizmet sağlayıcıları ve uygulama geliştiricileri ile pazarlık yapma ihtimali sınırlıdır. Bir başka deyişle, bireylerin veri gizliliğini koruması daha zordur. Bu sebeple bireylerin kişisel verilerinin korunması gerekliliği bakış açısına sahip olanlar ile pazarlamadan yana olan bakış açılarının çatıştığı söylenebilir.[279] Ayrıca tüm bu işleme faaliyetleri esnasında veri sahibinin rızasına dayanılması durumu, kendi başına bireyin özel hayatının korunmayacağını göstermektedir. Bu doğrultuda yalnızca alınan rızaya güvenmeyerek, bireyin mahremiyetini ihlal eden tüm eylemleri meşru kılmak için de alınan rıza tek başına yeterli olarak değerlendirilmemelidir.[280]

Günümüzde ticari kazanç elde etmek isteyen pek çok şirket, fiziki olarak yaptıkları ticaretin maliyetlerinin her geçen gün artması ve yapılan ticaretin odağında internetin olmasıyla birlikte internet ortamında aktif olma yoluna gitmektedir. İnternet

---

[277] Hüseyin Can Aksoy, Mesut Halıcıoğlu, "AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme," *Kişisel Verileri Koruma Dergisi,* no.3 (2021): 63.

[278] Ognjen Pantelic, Kristina Jovic, Stefan Krstovic, *"Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations," Sustainability* 14, no.9 (2022): 2, https://doi.org/10.3390/su14095015 , Erişim Tarihi: 5 Temmuz 2022.

[279] Allen, "Information Privacy," 865-866.

[280] Kosta, *Data Protection Law*, 322.

ortamında aktifleşmek ise çoğu zaman çerezler vasıtasıyla kullanıcıların alışkanlıklarının takip edilerek; kullanıcı verilerini toplamak suretiyle gerçekleşmektedir. Çerezler ile profilleme yapan şirketler, kullanıcıya özel reklamlar yaparak ticari kazanç elde ederken; kullanıcıların gizlilik teşkil eden verilerinin mahremiyetini ticari kazançları uğruna yok saymaktadır. Söz konusu şirketler dijitalleşmenin ve ticaretin geleceğinin kullanıcılara özgü kişiselleştirme ile mümkün olacağı fikrini ön plana çıkararak; profilleme faaliyetlerini her geçen gün geliştirmektedir.[281]

Özetle; bir internet sitesi, kullanıcıların bilgilerini kişiselleştirerek ve internet sitesinin içeriğini güncel tutarak daha hızlı ve kullanışlı bir şekilde çevrimiçi satışlar yapabilmek için çerez kullanmak ister.[282] Bununla birlikte, bir internet sitesinden çevrimiçi alışveriş yapılabilmesi için sepete atılan ürünlerin internet sitesi tarafından hatırlanması da yine çerezler vasıtasıyla gerçekleştirilebilmektedir.[283] Diğer bir deyişle, bahsi geçen çerezlerin olmaması ya da kullanılmaması halinde çevrimiçi alışveriş olarak adlandırılan bir kavramdan söz edilemeyecektir.

Çerezlerin internet siteleri tarafından kullanılmak istenmesinin bir diğer sebebi de internet sitesinde en fazla ve en az ziyaret edilen sayfalar hakkında bilgi alınabilmesine olanak sağlamasıdır. İnternet sitesinin gerçekte aldığı trafik ve benzeri istatistiki bilgiler, sitede geliştirme yapılacağı zaman kullanıcıya uygun şekilde düzenleme yapılabilmesi açısından önem arz etmektedir.[284]

İnternet siteleri, kullanıcılara hitap eden en uygun içeriği sunmak adına kullanıcı deneyimlerini kişiselleştirme konusuna yoğunlaşmaktadır. Veriler, çerezler tarafından kendiliğinden toplanmaz. Kullanıcılardan gelen kişisel veriler, çeşitli izleme yollarıyla toplanarak, ayrıştırılır.[285] Kullanıcının tercihleri daha sonra hatırlanarak alışveriş dosyası gibi bir çerez dosyasında saklanarak, ileriki ziyaretlerde kullanıcıya özel ürünler gösterilmektedir.[286]

---

[281] Adeyemi Aladeokin, Pavol Zavarsky, Neelam Memon, "Analysis and Compliance Evaluation of Cookies-Setting Websites with Privacy Protection Laws," *2017 Twelfth International Conference on Digital Information Management (ICDIM)*, (2017), 121, https://ieeexplore.ieee.org/document/8244646 , Erişim Tarihi: 3 Temmuz 2022.
[282] David Whalen, "The Unofficial Cookie FAQ Versiyon 2.6," cookiecentral.com, Son Güncelleme: 8 Haziran 2002, http://www.cookiecentral.com/faq/ , Erişim Tarihi: 4 Temmuz 2022.
[283] Pennington, "Cookies," 252.
[284] Pennington, "Cookies," 253.
[285] Pantelic, "Cookies Implementation Analysis," 1-2.
[286] Pennington, "Cookies," 253.

5.1.2. Çerez Türleri

Tek başına bir anlam ifade etmese de kullanıcıyı belirlenebilir kılma özelliği sebebiyle kişisel veri niteliğinde olabilen çerezler, çeşitli yönlerden gruplandırılabilir. Kullanım sürelerine, kaynağına ve kullanım amaçlarına göre üç ayrı başlık altında incelenebilir.[287]

5.1.2.1.Kullanım Sürelerine Göre Çerezler

Bu tür çerezler, oturum ve kalıcı çerezler şeklinde ikiye ayrılmaktadır. Oturum çerezleri, kullanıcı internet sitesinde gezinirken toplanabilen, siteden çıkış yaptığında ise kullanıcının cihazında depolanmadan silinen geçici süreli çerezlerdir.[288]

Montulli'nin 1998 yılında patentini aldığı kalıcı çerez terimi[289] ise internet sayfasını ziyaret eden kullanıcı, siteden çıkış yapsa bile silinmeyen, cihazında depolanmaya devam eden çerez anlamına gelmektedir. Bu çerez türünün amaçlarından bir tanesi, kullanıcının cihazına yerleştirilerek veri depolamayı hızlandırmaktır. Bu durum, internet sitesindeki gezinti sırasında hem operatöre hem de kullanıcıya daha iyi bir deneyim yaşatmayı amaçlamaktadır. Depolanan kullanıcının verileri ve davranışları, kullanıcının internet sitesinde ileride oluşabilecek aktivitelerini yönlendirmeye yarayacaktır.[290] Her ne kadar, bir internet sitesinde kullanıcı giriş sayfasına kaydedilen kimlik doğrulama bilgilerinden, kullanıcının ilgi alanlarına yönelik yapmış olduğu tercihlere kadar çeşitli verilerden oluşan kalıcı çerezlerin depolanması kullanım kolaylığı sağlasa da bu kalıcı çerezlerin kullanıcının kişisel verilerini içermesi sebebiyle verilerin gizliliği yönünden risk teşkil ettiği göz ardı edilmemelidir.[291]

5.1.2.2.Kaynağına Göre Çerezler

Bu tür çerezler, birinci taraf ve üçüncü taraf çerezler şeklinde iki başlıkta incelenmektedir. Birinci taraf çerezler, herhangi başka bir aracı olmadan ziyaret edilen

---

[287] Aksoy, "Çerezler," 63-64.
[288] Başak Doğan, Tuğçe Bozkurt, "Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle," blog.lexpera.com.tr, Son Güncelleme: 10 Eylül 2020, https://blog.lexpera.com.tr/kisisel-verilerin-korunmasi-cercevesinde-cerezler-turleri-kullanimlari-ve-uygulama-ornekleriyle/ , Erişim Tarihi: 5 Temmuz 2022; Pantelic, "Cookies Implementation Analysis," 4; Aksoy, "Çerezler," 64; KVK Kurumu, Çerez Rehberi, 8.
[289] Hal Berghel, "Toxic Cookies," *Computer* 46, no.9 (2013): 104, http://ww.berghel.net/col-edit/out-of-band/sept-13/oob_9-13.pdf , Erişim Tarihi: 5 Temmuz 2022.
[290] Pantelic, "Cookies Implementation Analysis," 4.
[291] KVK Kurumu, Çerez Rehberi, 9; Aksoy, "Çerezler," 64.

internet sitesinin kendisi tarafından kullanıcının cihazına yerleştirilen çerezlerdir.[292] Kullanıcı bilgileri, kullanıcının hangi reklamlara tıkladığı ve hangi sayfada ne kadar süre harcadığına ilişkin bilgilere dair oluşturulanlar, birinci taraf çerezler kapsamındadır.[293]

Kişinin ziyaret ettiği internet sayfası dışında farklı bir tarafın oluşturduğu çerezler, üçüncü taraf çerezlerdir.[294] Üçüncü taraf çerezlerin, birinci taraf çerezlerden iki yönden farklı olduğu söylenebilir. Bunlardan birincisi, bir internet sitesinin isteğine yanıt olarak yerleştirilmeyerek; üçüncü taraf sunucunun birinci taraf olan internet sitesinde bulunan reklamlar, resimler ya da komut dosyaları vasıtasıyla yerleştirilmeleridir. Kullanıcının cihazına yapılan bu yerleştirme, kullanıcının kendi aktivitesi doğrultusunda gerçekleşmez. İkinci fark ise üçüncü taraf çerezlerin farklı internet sayfalarında kullanılması sebebiyle birinci taraf çerezlerden daha kalıcı olmasıdır.[295]

Örneğin, internet tabanlı reklamcılık hizmetleri konusunda uzmanlaşan New York merkezli DoubleClick şirketi, çerezler vasıtasıyla reklamları hedefleme, sıklığını düzenleme ve pazar taleplerine ulaşmak için ayrıntılı analizler yapmaktadır. Kullanıcı bir internet sitesini ziyaret ettiğinde, bu internet sitesi arka planda DoubleClick'e de bağlanıp kullanıcının cihazına daha önceden çerez yerleştirilip yerleştirilmediğini sorgulamakta olup; aksi halde çerezlerden biri kullanıcıya iletilmektedir. Bunun akabinde, kullanıcı internet sitesinde gezinirken DoubleClick tarafından internet sitesinin kullanıcıya gösterdiği reklamlara tıklama gibi çeşitli bilgiler kaydedilmeye başlanmaktadır. Kullanıcı her yeni sayfaya geçtiğinde bu veriler de DoubleClick'e aktarılmaya devam edilmektedir. Böylece kullanıcının hangi sayfaları ziyaret ettiği ve bu sayfada ne kadar süre kaldığı, hangi reklamlara tıkladığı gibi veriler doğrultusunda kullanıcıya ait profil oluşturulmaktadır. Kullanıcı, aynı internet sitesini yeniden ziyaret ettiğinde DoubleClick tarafından kullanıcı tanınarak; aynı reklamlar yerine kullanıcının profiline uygun reklamlar gösterilmektedir. Söz konusu süreç uzun gibi görünse de esasında yaklaşık

---

[292] KVK Kurumu, Çerez Rehberi, 12.
[293] Jo Pierson, Rob Heyman, "Social Media and Cookies: Challenges for Online Privacy," *Info* 13 no.6 (2011): 34, https://www.emerald.com/insight/content/doi/10.1108/14636691111174243/full/html , Erişim Tarihi: 7 Temmuz 2022.
[294] Ginevra Bianco, "An Empirical Analysis Of Consumer Response To Google's Decision Of Phasing Out Third Party Cookies," *Luiss Guido Carli University Department of Economics and Finance Course of Marketing*, (2020): 5, https://www.researchgate.net/publication/345253989_An_empirical_analysis_of_consumer_response_to_Google's_decision_of_phasing_out_third_party_cookies/link/5fa191f0299bf1b53e5d1a98/download , Erişim Tarihi: 10 Temmuz 2022.
[295] Pierson, "Social Media Cookies," 35.

yirmi milisaniyeden daha kısa bir sürede gerçekleşmektedir.[296] Bahsi geçen örnekteki çerez türü, üçüncü taraf çerez kategorisine dahil edilebilir.

5.1.2.3.Kullanım Amaçlarına Göre Çerezler

Bu çerezler; zorunlu, performans, fonksiyonel, pazarlama ve flash çerezler olmak üzere beşe ayrılmaktadır.[297]

Zorunlu çerezler, internet sitesinin çalışabilmesi ve temel işlevlerini yerine getirebilmesi için mutlak surette etkinleştirilmesi gereken çerezlerdir. Bu çerezler olmadan internet sitesinden gerektiği şekilde faydalanılamayacaktır.[298] Genellikle birinci taraf çerezlerden oluşan zorunlu çerezler, kullanıcıların kişisel bilgilerini de içerebileceğinden pazarlama amacıyla kullanılması kullanıcılar açısından yüksek risk teşkil etmektedir.[299]

Performans çerezleri, internet sitesi tarafından genellikle kullanıcı dostu bir yapı oluşturulabilmek amacıyla kullanıcıların hangi sayfada ne kadar vakit harcadığı, reklamlara olan ilgileri gibi hususlara ilişkin istatistiki bilgilerin depolandığı verilerdir.[300]

Fonksiyonel çerezler, kullanıcıya internet sitesine sonraki girişlerinde daha işlevsel bir kullanım sağlamak amacıyla kullanıcıların tercihlerini hatırlayarak kişiselleştirilmiş bir deneyim sunmaya yönelik oluşturulan çerezlerdir.[301] İnternet sitesinde zorunlu çerezler dışında kalan işlevlerden faydalanabilmeye yönelik oluşturulur. Bilgi toplumu hizmeti[302] olduğu açıkça belli olmayan hallerde bu tür çerezlerin kullanılabilmesi, kullanıcının rızasını gerektirmektedir.[303]

---

[296] Pennington, "Cookies," 251-252.
[297] OneTrust LLC, "The Ultimate Cookie Handbook For Privacy Professionals," onetrust.com, Kasım 2020: 6-7, https://www.dataguidance.com/sites/default/files/20201228-onetrust-cookieconsent-handbook-digital.pdf , Erişim Tarihi: 10 Temmuz 2022.
[298] OneTrust LLC, "Cookie Handbook," 7.
[299] KVK Kurumu, Çerez Rehberi, 10, 49.
[300] Aksoy, "Çerezler," 64.
[301] OneTrust LLC, "Cookie Handbook," 7.
[302] Bilgi toplumu hizmetleri, genellikle bir ücret karşılığında, kullanıcının talebi doğrultusunda, elektronik araçlar vasıtasıyla uzaktan sağlanan hizmetlerdir. Bir hizmetin bilgi toplumu hizmeti olarak adlandırılabilmesi için temelde üç şart aranmaktadır. Bunlar, hizmetin uzaktan sağlanması, elektronik araçlar kullanılması ve talebin kullanıcıdan gelmesidir. Ücret kriteri ise son kullanıcıdan alınmasa bile reklamlar vasıtasıyla reklam verenden ücret alınarak hizmetin finanse edilmesiyle sağlanmaktadır. Bilgi toplumu hizmetlerine örnek olarak; ürün satış platformları-internet siteleri, çevrimiçi oyunlar, internet tabanlı sesli telefon hizmetleri, sosyal medya platformları gösterilebilmektedir. (Information Commissioner's Office (ICO), What do you mean by an 'information society service'? https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/ , Erişim Tarihi: 12 Temmuz 2022.)
[303] KVK Kurumu, Çerez Rehberi, 10.

Pazarlama çerezleri, internette kullanıcıların davranışlarının takip edilerek; herkese aynı reklamın yapılması yerine kullanıcının kendisine özgü reklamların gösterilmesini temel alan çerezlerdir. Kişiye özgü reklamcılık, genele hitap eden reklamlara nazaran amaca ve alıcıya daha kısa sürede ulaşılabilmesi sebebiyle reklam verenler tarafından öncelikli tercih edilmektedir.[304] Bunlar genellikle üçüncü taraf çerezlerden oluşmaktadır.[305]

Flash çerezler ise Adobe Flash geliştiricileri tarafından kullanıcıların cihazlarına veri depolamak için kullanılan, tüm HTTP çerezlerine göre tamamen ortadan kaldırılması daha zor olan, silinse bile yeniden ortaya çıkabilen dosyalar olup; kullanıcılar tarafından silinmesi zor olduğu için reklam verenler tarafından sıkça tercih edilen çerezlerdir. Flash çerezler, HTTP çerezlerden farklı olarak bir cihazdaki tüm tarayıcıların erişebileceği şekilde düzenlenmekte olup; kullanıcı tarayıcısını değiştirse bile izlenmeye devam edilebilmesini sağlar.[306] Flash çerezlerin HTTP çerezlerinden bir başka farkı ise flash çerezler 100 kilobayt bilgi depolayabilirken; HTTP çerezleri yalnızca 4 kilobayt bilgi depolayabilirler.[307] Bu çerezler, silinen HTTP çerezlerini yeniden aktif hale getirmek için kullanılabilmektedir.[308] İnternet siteleri tarafından çerezlere ilişkin yapılan bilgilendirmelerde genellikle flash çerezlere dair fazla bilgi yer almamakta ve çoğu zaman kullanıcılardan bu çerezlerin etkinliğine ilişkin rızaları da alınmamaktadır. HTTP çerezlerini silmek, kullanıcının ziyaret ettiği internet sayfalarını gösteren geçmişini temizlemek, önbelleği silmek ya da tarayıcı içerisindeki özel verilerin belirli aralıklarla silinmesi seçeneğinin aktif olması dahi flash çerezlerin varlığını etkilemez.[309]

5.1.3. ÇEREZLER VASITASIYLA DAVRANIŞSAL PAZARLAMA YAPILMASI

Gelişen teknolojinin reklamcılık sektörüne getirdiği yeniliklere kadar, ürün veya hizmetler pazarlanırken alıcıların profilleri bilinmemekteydi. Bu durum, ürünün hitap

---

[304] KVK Kurumu, Çerez Rehberi, 11.
[305] OneTrust LLC, "Cookie Handbook," 7.
[306] Mika D Ayenson, Dietrich James Wambach, Ashkan Soltani, Nathan Good, Chris Jay Hoofnagle, "Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning," srrn.com, (2011): 2, http://dx.doi.org/10.2139/ssrn.1898390, 2, Erişim Tarihi: 12 Temmuz 2022.
[307] Ayenson, "Flash Cookies," 2.
[308] OneTrust LLC, "Cookie Handbook," 7.
[309] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle, "Flash Cookies and Privacy," ssrn.com, (2009): 1, http://dx.doi.org/10.2139/ssrn.1446862 , Erişim Tarihi: 12 Temmuz 2022.

ettiği kitlenin yanı sıra ürünle aslında ilgilenmeyen kimselere de pazarlanmasına böylece hem zaman hem de maddi kayba neden olmaktaydı. İnternet sitelerinin kullanıcılarının kendilerini daha sonra tekrar ziyaret etmeleri amacıyla kullanıcı dostu site hazırlama ihtiyacının çerezlerle karşılanabileceği fikri daha da öteye taşınarak; kullanıcılardan toplanan kişisel verilerin pazarlama amacıyla kullanılması halinde ürünün hizmet ettiği asıl kitleye daha kısa sürede ulaşılabileceği fark edildi. Bir kullanıcının internet sitesinde hangi sayfalarda gezindiği, hangi ürünlere göz attığı bilgisi, üçüncü taraf çerezleriyle toplanılarak; pazarlama amacıyla internet üzerinden satış yapanlarla paylaşılmaya, böylece kullanıcıya daha önce arattığı ve muhtemelen hala satın almamış olduğu ürünün çeşitli versiyonlarına dair ürünler gösterilmeye başlandı.[310]

Davranışsal pazarlama olarak da anılan bu pazarlama türünde, tarayıcılar veya kullanıcıyı takip amacı olan internet siteleri, kullanıcıların cihazlarına kimlik numarasına benzer bir değer atayarak kullanıcıyı izlemeye yönelik bir çerez tanımlayabilir. Kullanıcıya özgü atanan bu kimlik numaralarına çerez vasıtası ile erişilerek; farklı internet sitelerindeki ziyaretleri takip edilebilmektedir.[311] Kullanıcının ziyaret ettiği internet sayfaları ve tıkladığı reklamların takibiyle birlikte kullanıcı profili oluşturularak kullanıcıya daha sonra gösterilecek reklamların belirlenmesi ve bir reklamın aynı kullanıcıya tekrar gösterilmemesi için çerezler kullanılır.[312]

Çevrimiçi yapılan kullanıcı takipleri vasıtasıyla, kullanıcılara ait özel nitelikli kişisel veriler ve onları tanımlayan diğer veriler aktarılarak, reklam verenlerin kullanıcılara yönelik çıkarımda bulunmaları sağlanır. Söz konusu takibi sağlayan çerezler, sunulan ücretsiz teklifleri kabul eden kullanıcıların cihazlarına yerleştirilmek suretiyle de gerçekleşebilmektedir.[313] Pazarlama çerezleri ile kullanıcıların internetteki davranışları takip edilerek profilleme yapılmakta olup; bu profilleme vasıtasıyla kullanıcılar kendilerine özgü reklamlara maruz bırakılmaktadır.[314] Böylece reklam verenler, geleneksel pazarlamaya nazaran daha hızlı ve daha az maliyetle alıcıya ulaşabilmektedir.

---

[310] Chris Jay Hoofnagle, Ashkan Soltani, Nathan Good, Dietrich James Wambach, Mika D Ayenson, "Behavioral Advertising: The Offer You Cannot Refuse," *Harvard Law & Policy Review*, no.6 (2012): 274-275, https://ssrn.com/abstract=2137601 , Erişim Tarihi: 14 Temmuz 2022.
[311] Hoofnagle, "Behavioral Advertising," 276.
[312] Pennington, "Cookies," 251.
[313] Hoofnagle, "Behavioral Advertising," 276.
[314] KVK Kurumu, Çerez Rehberi, 11.

5.2. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE ÇEREZ DÜZENLEMELERİ

5.2.1. AB Hukukunda Çerez Düzenlemeleri

Kişisel verilerin işlenmesi ve serbest dolaşımına ilişkin yayımlanan 95/46/EC sayılı Direktif'in ardından telekomünikasyon sektöründe kişisel verilerin işlemesine ilişkin mahremiyet hakkını ve serbest dolaşımı sağlamak adına, 95/46/EC sayılı Direktif'i özelleştirme ve tamamlamak amacıyla[315] 97/66/EC sayılı Telekomünikasyon Sektöründe Gizliliğin Korunması Direktifi[316] yayınlanmıştır.

Elektronik haberleşme sektörü, ilk düzenlemelerin yer aldığı 1997 yılından itibaren söz konusu özel koruma mevzuatından yararlanmaktayken;[317] bu düzenlemelerin akabinde, 2002 yılında elektronik haberleşme sektörüne ilişkin daha özel mahiyette hükümlere yer verilen 2002/58/EC sayılı Elektronik Haberleşme Direktifi yayımlanmıştır.[318] Telekomünikasyon sektörü, AB hukukunda sektöre özel veri koruma mevzuatı düzenlenen tek sektör olma ayrıcalığına sahiptir.[319]

Elektronik Haberleşme Direktifi'nin 1/1 maddesinde belirtildiği üzere Direktif'in amacı, elektronik haberleşme sektöründe işlenen kişisel verilerin gizliliğinin sağlanması ve işleme süreçlerine yönelik hususların belirlenmesidir. Diğer bir deyişle ilgili Direktif, elektronik haberleşme sektörüne yönelik olarak hazırlanmıştır.[320] Ayrıca Elektronik Haberleşme Direktifi'nin 1/2 maddesi uyarınca, gerçek kişilerle birlikte tüzel kişilerin de korunması hedeflenmektedir. Direktif'in 3/1 maddesi ise bu Direktif'in kamuya açık elektronik haberleşme hizmetlerinin sağlanması adına işlenen kişisel veriler için geçerlilik teşkil edeceğini belirtmektedir.

Çerezler vasıtasıyla kişinin kimlik bilgilerinin ayrıntılarına kadar öğrenilebilmesi ve profilleme yöntemleri sayesinde tüketicilerin yönlendirilmesi nedeniyle işlenen kişisel verilerin artış göstererek bu konuda bir düzenleme yapılarak kullanıcılara yönelik hukuki koruma sağlanması ihtiyacı doğmuştur.

---

[315] Vagelis Papakonstantinou, Paul De Hert, "The Amended EU Law on ePrivacy and Electronic Communications After Its 2011 Implementation: New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights," *Journal of Computer Information Law* 29, (2011): 40, https://repository.law.uic.edu/jitpl/vol29/iss1/2/ , Erişim Tarihi: 17 Temmuz 2022.
[316] Directive 1997/66/EC, *EUR-Lex*, Erişim Tarihi: 17 Temmuz 2022.
[317] Papakonstantinou, "ePrivacy 2011 Implementation," 29.
[318] Küzeci, *Kişisel Verilerin Korunması*, 212-213.
[319] Papakonstantinou, "ePrivacy 2011 Implementation," 29.
[320] Papakonstantinou, "ePrivacy 2011 Implementation," 30.

Casus yazılımlara karşı güçlendirilmiş koruma sağlayan firmaların yanı sıra internet servis sağlayıcıları ve benzeri istenmeyen iletilerden etkilenenlerin bu iletileri gönderenlere karşı başlattıkları yasal takiplerin artmasıyla birlikte, kişisel verilerin korunması ve veri ihlallerine karşı zorunlu bildirimlerin, diğer bir deyişle yalnızca onay veren abonelere ileti gönderilebilmesi[321] gibi ihtiyaçların doğması ve telekomünikasyon kavramının yalnızca sesin kablolar üzerinden iletilmesinden İnternet Üzerinden Ses İletimi Protokolü (Voice Over Internet Protocol - VoIP)[322] vasıtasıyla internet üzerinden iletişime geçilerek internetin tamamlayıcı ve hatta ikame bir rol üstlenmesi göz önünde bulundurulmuştur.[323] Bu doğrultuda, 2002 yılında yayımlanan Direktif'te değişiklikler yapılarak 2009 yılında 2009/136/EC sayılı Direktif yayımlanmıştır. Böylece ilgili düzenleme, 1997 yılındaki düzenlemenin yerini almıştır.[324]

Elektronik Haberleşme Direktifi'ne 2009 yılında yapılan değişiklik ile çerezlere ilişkin hüküm getirilmiştir. 2009/136/EC sayılı Direktif'in 5/3 maddesi uyarınca; terminal cihazlarda veri depolanması veya depolanan bu verilere erişilebilmesinin hukuka uygunluğu, verisi işlenen abone veya kullanıcının işleme amaçları hakkında bilgilendirilerek açık rızalarının alınmış olması koşuluna bağlanmıştır. Söz konusu düzenlemenin, çerez yerleştirilmesine ilişkin hukuki dayanak olduğu söylenebilir.[325] İlgili kişiden rıza alınması ve çerezlere ilişkin önemli değerlendirmelere yer verilen AB Adalet Divanı'nın (ABAD) 2019 yılında verdiği Planet 49 kararında,[326] söz konusu madde 5/3'ün kişisel veri içermese bile tüm çerezlere uygulanması gerektiği belirtilmiştir.

95/46/EC sayılı Veri Koruma Direktifi'nin 29. maddesiyle tüm ulusal veri koruma otoritelerinin yetkililerinden oluşan Veri Koruma Çalışma Grubu (Article 29 Çalışma Grubu) kurulmuştur. Bu grup, Direktif kapsamında kabul edilen hususların nasıl

---

[321] Papakonstantinou, "ePrivacy 2011 Implementation," 43.

[322] İnternet Protokolü üzerinden sesin iletimi anlamına gelen VoIP, kullanıcıların internet bağlantıları aracılığıyla diğer kullanıcılarla konuşmasını sağlamaktadır. VoIP, arayan tarafı aranan tarafa bağlamak için genel anahtarlamalı telefon ağı yerine interneti kullanır. İnternet üzerinden telefon araması yapmak için, her ikisi de standart bir bilgisayar veya mobil cihazda bulunan bir geniş bant ağ bağlantısı, bir mikrofon ve hoparlör ve Skype gibi bir VoIP yazılımı gerekmektedir. (Misty E. Vermaat, Susan L. Sebok, Steven M. Freund, Jennifer T. Campbell, Mark Frydenberg, Discovering Computers 2018 Digital Technology, Data, and Devices-Module 2, Boston: Cengage Learning, 2018), 37.)

[323] Papakonstantinou, "ePrivacy 2011 Implementation," 49.

[324] Papakonstantinou, "ePrivacy 2011 Implementation," 30.

[325] Aksoy, "Çerezler," 64-65; Küzeci, *Kişisel Verilerin Korunması*, 215-216.

[326] Case C-673/17, 1 Ekim 2019, https://curia.europa.eu/juris/document/document.jsf;jsessionid=D6F8DD810FC121A0AD5EC1F1F93DD780?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=131346, Erişim Tarihi: 20 Temmuz 2022.

uygulanması gerektiğine ilişkin ortak bir uygulama şekli belirlemek üzere bir araya gelmiştir.[327]

Article 29 Çalışma Grubu, çerezlere ilişkin 2009/136/EC sayılı Direktif'in 5/3 maddesinde belirtilen söz konusu bilgilendirmenin, ilgili kişi internet sayfasına girdiğinde karşılaştığı ilk ekranda görünür bir şekilde yapılması gerektiğine değinmiştir. Kullanılan bütün çerezlere ilişkin bilgilendirmenin yapılmasının önemi vurgulanarak; çerezlerin listelendiği bir sayfaya yönlendirme yapılabileceği ve bu sayfada kullanım amacı ve işleme süresine ilişkin hususlara yer verilmesi gerektiğinden bahsedilmektedir. Şayet üçüncü taraf çerezler kullanılıyorsa, yapılan veri aktarımına ilişkin bilgilendirmeye de yer verilmelidir. Tüm bu bilgilendirmenin devamında ise ilgili kişiden bilgilendirme yapılan çerezlerin hepsini kabul etme, bir kısmını kabul etme ve hepsini reddetme seçeneklerinin sunulması gerekmektedir. Bu doğrultuda kullanıcıdan alınan açık rızada çerezin kullanım amacının belirtilmesi, diğer bir deyişle genel anlamda çerez kullanımına izin verilmeyecek şekilde olması ve işleme başlanmadan önce rızanın alınması gerekmekte olup; kullanıcının aktif bir davranışıyla ve özgür iradeyle rıza verilmesinin önemi vurgulanmıştır.[328]

Söz konusu hususlar değerlendirildiğinde ve Planet 49 kararında da değinildiği üzere; kullanıcının aktif davranışıyla verilmesi gereken çerezler için verilecek onayın önceden işaretli şekilde kullanıcıya sunulmaması gerektiği, internet sayfasının çalışabilmesi için gerekli olan zorunlu çerezler hariç olmak üzere sayfayı kullanabilmek için çerezlerin kabul edilmesinin şart koşulmaması gerektiği, kullanıcıya çerezlerden bazılarını kabul edip bazılarını etmeme gibi seçeneklerle çerezlerin katmanlı olarak sunulması ve kullanıcının internet sayfasını her ziyaret ettiğinde yeniden rıza alınmaması gerektiği çıkarımında bulunulabilir.[329]

Kullanıcı internet sayfasını her ziyaret ettiğinde çerezler için rıza alınması, rıza yorgunluğuna neden olmaktadır. Bu durum, kullanıcının bilgilendirmeyi okumadan hızlı bir şekilde rıza vermesiyle sonuçlanmakta olup; rızanın bireyi uyarıcı ve koruyucu olan etkisinin azalmasına sebep olmaktadır.[330] Dolayısıyla rızanın her kullanıcı için yalnızca

[327] Papakonstantinou, "ePrivacy 2011 Implementation," 35.
[328] Article 29 Çalışma Grubu, Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies, (2013): 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf , Erişim Tarihi: 21 Temmuz 2022.
[329] Aksoy, "Çerezler," 65-66.
[330] Article 29 Çalışma Grubu, Consent for Cookies, 17.

bir kez alınabilmesi daha uygun bulunmaktadır. Fakat çerezlerin kullanım amacının değişmesi veya üçüncü taraflara gönderilen çerezlerin varlığı halinde üçüncü taraflarda değişiklik olması gibi durumlarda, kullanıcıdan yeniden rıza alınması gerekliliği ortaya çıkmaktadır.[331]

Kullanıcının fazla sayıda rıza talebiyle karşı karşıya bırakılması olan rıza yorgunluğu, kullanıcı açısından iki şekilde sonuçlanabilmektedir. Kullanıcı ya tüm çerezleri reddetmekte ve bu sebeple faydalı veri işleme faaliyetleri engellenerek internet sayfasının aktif kullanımının önüne geçilmesine sebep olunmakta ya da bilinçsizce tüm çerezleri kabul eden kullanıcının aleyhine olacak şekilde agresif bir veri işleme faaliyeti başlayarak kullanıcının hukuka aykırı şekilde verileri işlenmeye başlanmaktadır.[332] Bunun önüne geçilebilmesi amacıyla Avrupa Veri Koruma Kurulu tarafından kullanıcı dostu uygulamaların artırılması önerilmektedir.[333]

5.2.2. AB Düzenlemeleri Doğrultusunda Elektronik Haberleşme Sektöründeki Kullanıcının Açık Rızasının Alınmasının Gerekmediği Durumlar

2009/136/EC sayılı Direktif ile değiştirilen 2002/58/EC sayılı Direktif'in 5/3 maddesinde açık rıza alınması gerekliliğinin yanı sıra bu yükümlülüğün istisnalarına da yer verilmiştir. Bu doğrultuda, yalnızca elektronik haberleşmenin sağlanabilmesi amacıyla çerez kullanımı gereken hallerde kullanıcıların rızalarının alınmasına gerek yoktur. Article 29 Çalışma Grubu, bu çerezleri Kriter A istisnası olarak tanımlamıştır.[334] Haberleşmenin sağlanması için zorunlu şekilde işlenen Kriter A çerezler; çağrının doğru yere ulaşmasını sağlayanlar, iletişimin içeriğini oluşturan verilerin karşılıklı olarak taşınmasını sağlayanlar ve iletişim esnasındaki veri kaybını önleme ve iletişim hatalarını belirlemeye yarayan çerez uygulamalarıdır. Bu anlamda, söz konusu üç durumdan birinin

---

[331] Information Commisioner's Office (ICO), Guidance on the Use of Cookies and Similar Technologies, (2019): 40-41, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf , Erişim Tarihi: 24 Temmuz 2022.

[332] Aksoy, "Çerezler," 73-74.

[333] European Data Protection Board (EDPB), Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021, 3, https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en , Erişim Tarihi: 24 Temmuz 2022.

[334] Article 29 Çalışma Grubu, Opinion 04/2012 on Cookie Consent Exemption, (2012): 2, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf , Erişim Tarihi: 27 Temmuz 2022.

varlığı halinde, kullanıcının rızası aranmamakta; çerez kullanımı için kullanıcıya tercihinin sorulmasına gerek bulunmamaktadır.[335]

Article 29 Çalışma Grubu tarafından Kriter B çerezler olarak adlandırılan çerezler ise ilgili kişinin talepte bulunduğu bilgi toplumu hizmetlerinin sunulması amacıyla kullanılan çerezlerdir.[336] Kriter B istisnai durumuna dahil edilerek kullanıcının rızasının alınmasına gerek olmayan çerezler için öncelikle kullanıcının bilgi toplumu hizmetini kullanmaya yönelik aktif bir davranışının olması gerekmektedir. Bu istisnanın geçerli olabilmesi için ikinci şart ise söz konusu hizmetin sağlanabilmesi için çerez kullanımının zorunlu olması, diğer bir deyişle çerez kullanılmadığı takdirde kullanıcının hizmetten faydalanamamasıdır.[337] Örneğin, gazetenin internet sitesindeki haberlerin herkes tarafından okunabilmesine karşılık yorum yazmak isteyen kullanıcıların oturum açmaları beklenmektedir. Oturum açarak gazeteyi okuyan kullanıcılara özel hizmetler sağlanmaktadır. Bu durumda ayrıcalıklı hizmetlerden faydalanma talebi kullanıcının kendisinden gelmekte ve kullanıcının aktif bir eylemiyle gerçekleşmekte olup; diğer bir ifadeyle kullanıcının kendisi oturumu açmaktadır. Oturum açılmadan da yorum yazabilme özelliği aktif olmadığından söz konusu oturum çerezleri için Kriter B sağlanmış denilebilmektedir.[338]

Bazen çerezler birden fazla amaç için kullanılmak istenmektedir. Bu durumda çerezleri Kriter A veya Kriter B istisnasına dahil ederek kullanıcının rızası alınmadan kullanabilmek için birden fazla olan amaçların hepsinin istisna kapsamına dahil olması gerekmektedir. İstisna kapsamına dahil olmayan amaç için kullanıcının ayrıca rızasının alınması gerekmektedir.[339]

Article 29 Çalışma Grubu, kullanıcıların ziyaret süreleri gibi istatistiki bilgileri gösteren analitik çerezlerin iletişim gerçekleşmesi için mecbur olmaması sebebiyle, kullanıcının internetteki davranışlarını takip ederek pazarlama ve veri analizi yapma amacıyla kullanılan sosyal takip çerezlerinin işlemenin zorunlu olması kriterini sağlamaması sebebiyle ve üçüncü taraf pazarlama çerezlerinin ise kullanıcının trafik verilerinin pazarlama amacıyla kullanılması sebebiyle, kullanıcının rızası olmadan

[335] Article 29 Çalışma Grubu, Opinion on Cookie, 3.
[336] Article 29 Çalışma Grubu, Opinion on Cookie, 2.
[337] Article 29 Çalışma Grubu, Opinion on Cookie, 3.
[338] Article 29 Çalışma Grubu, Opinion on Cookie, 4.
[339] Article 29 Çalışma Grubu, Opinion on Cookie, 6.

işlenemeyeceğini belirtmiştir. Diğer bir deyişle bu üç tür çerezin, her halükarda Kriter A ve Kriter B istisnaları kapsamına dahil edilmeyeceğine değinilmiştir.[340]

5.2.3. Türk Hukukunda Çerez Düzenlemeleri

Kişisel verilerin korunması hukukunda çerez kullanımı önemli bir yer teşkil etse de iç hukukumuzdaki temel düzenleme olan KVKK'da bu konuya dair ayrıntılı bir hüküm yer almamaktadır. Bununla birlikte ülkemizdeki çerez uygulamalarına bakıldığında, kullanıcıların açık rızalarının alınarak çerez kullanımının tek istisnası, elektronik haberleşme sektöründeki işletmecilerin haberleşmeyi sağlayabilmesi amacıyla çerezler vasıtasıyla veri işlemesi hali olarak gösterilebilir.

Ülkemizde, Elektronik Haberleşme Direktifi gibi çerezlere ilişkin ayrıntılı hükümlere yer verilen AB düzenlemelerinin aksine, çerezlere ilişkin ayrıca bir düzenleme bulunmasının yerine konuya ilişkin yalnızca EHK 51/3 maddesi uygulama alanı bulmaktadır.

EHK'nın bahsi geçen 51/3 hükmünde, işletmecilerin elektronik haberleşmeyi sağlaması dışında abone veya kullanıcıların cihazlarında bilgi saklama ve bu verilere erişilmesinin yalnızca bu kişilerin bilgilendirilmelerinin akabinde açık rızalarının alınması halinde gerçekleştirilebileceği belirtilmektedir.

2002/58/EC sayılı Direktif'te yer verilen Kriter A'da bahsedildiği üzere ve EHK'nın 51/3 maddesi doğrultusunda, BTK tarafından yetkilendirilmiş olan ve elektronik haberleşme hizmeti sunan veya elektronik haberleşme şebekesi sağlayan işletmecilerin, haberleşmenin sunulması amacıyla çerezler vasıtasıyla veri işleme faaliyeti gerçekleştirebilmesi için abonenin veya kullanıcının açık rızasını almasına gerek yoktur. Buna karşılık EHK'nın 51/3 maddesinin devamında değinildiği üzere, abonenin veya kullanıcının terminal cihazlarında bilgi saklama ve bu bilgilere erişim gibi faaliyetler için söz konusu kişilerin açık rızasının alınmış olması şartı bulunmaktadır.

EHK'nın 51/3 maddesinde belirtilen işletmeci ifadesiyle kimlerin kastedildiği incelendiğinde; söz konusu düzenleme EHK içerisinde yer aldığından ve ilgili Kanun'da ise işletmeci kavramı yalnızca elektronik haberleşme sektöründe faaliyet gösteren işletmecileri ifade ettiğinden; Google gibi bilgi toplumu servis sağlayıcılarının hüküm kapsamı dışında yer aldığı düşünülmektedir.[341]

---

[340] Article 29 Çalışma Grubu, Opinion on Cookie, 9-11.
[341] Aksoy, "Çerezler," 77.

AB düzenlemelerinde bahsi geçen Kriter B istisnasına ise Türk hukukunda henüz yer verilmemiştir.[342] KVKK'daki kullanıcının açık rızası bulunmadan kişisel veri işlemeye ilişkin istisnai hallerin EHK 51/3 hükmüne uygulanıp uygulanmayacağı hususu değerlendirildiğinde; EHK, KVKK'ya nazaran daha özel nitelikli bir düzenleme olduğundan; KVKK'daki istisnai hallerin EHK 51/3 maddesinde kullanıcının açık rızasının olmadan terminal cihazlarına[343] çerez yerleştirilebilmesi hususuna uygulanamayacağından söz edilebilir.[344] Fakat EHK kapsamına girmeyen işleme faaliyetlerinde ise Türk hukukunda çerezlere ilişkin başka bir düzenleme bulunmadığından; KVKK'daki veri işleme istisnai hallerine örneğin veri sorumlusunun meşru menfaati için işlenebilmesine dayanılabilmektedir.[345]

KVK Kurulu tarafından verilen Amazon Türkiye kararında,[346] çerezlerin işlenmesine ilişkin önemli hususlara değinilmiştir. Kullanıcılara çerezlerin işlenmesine izin vermedikleri takdirde sepete ürün eklemelerine, satın almalara ve oturum açılması gereken hizmetlerin kullanımına izin verilmeyeceği yönünde yapılan bildirimin, hizmetin sunumunun rıza koşuluna bağlandığı ve hakkın kötüye kullanımı anlamına geldiği belirtilerek; kişisel verilerin işleme amacıyla sınırlı ve ölçülü olma ilkesine aykırılık teşkil ettiği bildirilmiştir. Ayrıca Amazon Türkiye internet sitesini ziyaret eden kullanıcılardan, ürün satın alma işlemi yapmasalar bile yalnızca ziyaret etmeleri halinde bile gerekli olan hizmetlerin sağlanması, kullanıcının ilgisinin hangi kategoriler olduğunun tespiti gibi konuların takibi amacıyla fazla sayıda ve ayrıntılı kişisel verileri toplamaktadır. Söz konusu veri toplama faaliyetine ilişkin bilgilendirmenin pop-up şekilde yapılması yerine bilgilendirme metnine yerleştirilmiş olması ve bu bilgilendirmeye ulaşabilmek için site içerisinde çokça çaba sarf edilmesi halinin yalnızca ziyaret amacı olan kişiler açısından zorluk teşkil ettiği KVK Kurulu tarafından dile getirilmiştir. Dolayısıyla veri sorumlusu olan Amazon Türkiye tarafından çerezler konusunda kullanıcının aydınlatılması yükümlülüğünün Aydınlatma Yükümlülüğüne İlişkin Tebliğ'e aykırı olduğuna yer verilmiştir.

---

[342] Aksoy, "Çerezler," 76.
[343] Terminal cihaz ya da terminal ekipmanı kavramı, bir çerezin yerleştirilebildiği bir bilgisayar, mobil cihaz, akıllı televizyonlar ve nesnelerin interneti dahil olmak üzere genel anlamda bağlı cihazlar için kullanılmaktadır. (Information Commisioner's Office (ICO), Cookies, 9.)
[344] Aksoy, "Çerezler," 77-78.
[345] Aksoy, "Çerezler," 80.
[346] KVK Kurulu, 27.02.2020 tarih ve 2020/173 sayılı Amazon Turkey Perakende Hizmetleri Limited Şirketi Kararı, https://www.kvkk.gov.tr/Icerik/6739/2020-173 , Erişim Tarihi: 1 Ağustos 2022.

Kullanıcının internet sitesini ziyaretiyle birlikte çerezlerin işlenmeye başlaması halinde, kullanıcı internet sitesine girdiği anda veri sorumlusu tarafından yapılan bilgilendirme sayesinde kullanıcının ayrıca çaba sarf ederek hangi verilerinin işlendiğine ilişkin araştırma yapmasına gerek kalmamalıdır. KVK Kurulu'nun verdiği Amazon Türkiye kararı doğrultusunda ulaşılan bir diğer sonuç da çerezlerin işlenmesine yönelik verilecek olan rızaların katmanlı şekilde ve opt-in verilebilecek şekilde düzenlenmiş olması gerektiğidir. İnternet sayfasının asıl görevini yerine getirmek için zorunlu olan çerezlerin dışındaki çerezlerin işlenip işlenemeyeceği hususu kişinin rızasına bağlı olmalıdır.[347]

Amazon Türkiye kararıyla birlikte, Türk hukukunda çerezlerin işlenmesinde kişisel verilerin korunması konusuna önem verilmeye başlandığı anlaşılmıştır.[348] Nitekim 2022 yılında KVK Kurumu Çerez Rehberi'ni yayımlamıştır.

5.2.4. Elektronik Haberleşme Direktifi'nde Yapılacak Değişiklikler

GDPR, Avrupa'da veri korumaya ilişkin genel kuralları belirler; dolayısıyla elektronik haberleşme sektöründen bağımsız olarak kişisel verilerin işlenmesiyle ilgili tüm konular için geçerlidir. Teknolojik gelişmeler doğrultusunda, hizmet sağlayanlarla hizmet alanların ihtiyaçları da değişime uğradığından; Direktif'in kapsamının geleneksel telekom sağlayıcılarının yanında aynı zamanda IP üzerinden ses, metin mesajı ve e-posta sağlayıcıları gibi OTT (Over-the-Top)[349] sağlayıcıları olarak adlandırılan yeni pazar oyuncularını da kapsayacak şekilde genişletilmesi amaçlanmıştır. Bu yüzden, Elektronik Haberleşme Direktifi'nde değişiklik yapılması gerekliliği ortaya çıkmıştır.[350] Bu

---

[347] Murat Volkan Dülger, "Yurt Dışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı," ssrn.com, 9-10. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388 . Erişim Tarihi: 1 Ağustos 2022.

[348] Hüseyin Can Aksoy, Mesut Halıcıoğlu, "E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması," *Kişisel Verileri Koruma Dergisi* 2, no.2 (2020): 14.

[349] OTT, kullanıcılara televizyon, film gibi içerikler veya haberleşme hizmetlerinin internet üzerinden sunulması anlamına gelmektedir. (Telestream, What Does OTT Really Mean? https://www.telestream.net/video/solutions/what-is-ott.htm , Erişim Tarihi: 1 Ağustos 2022.)
Over-the-top (OTT) mesajlaşma uygulamaları, e-posta, Whatsapp, Facebook Messenger gibi OTT mesajlaşma servislerine erişimin kolaylaşmasını sağlayan akıllı telefon kullanımının artış göstermesi, her geçen gün kullanımı azalan geleneksel mobil mesajlaşma servislerinin kullanımını neredeyse sona erdirmiştir. Tim Dwyer, "Privacy From Your Mobile Devices? Algorithmic Accountability, Surveillance Capitalism, and the Accumulation of Personal Data," ed. Rich Ling, Leopoldina Fortunati, Gerard Goggin, Sun Sun Lim, Yuling Li, iç. *The Oxford Mobile Handbook of Mobile Communication and Society*, (Oxford: Oxford University Press, 2020), 555.

[350] González, "Proposed ePrivacy Regulation," 6.

doğrultuda ilgili Direktif'te yapılması öngörülen değişikliklerle ilgili taslak metinler yayımlanmaya başlamıştır.

Taslak halindeki Elektronik Haberleşme Direktifi, kişisel veri olarak kabul edilen elektronik haberleşme verileriyle ilgili olarak GDPR'ı detaylandırarak, onu tamamlama vazifesini üstlenmektedir. Bilhassa, istenmeyen pazarlama, çerezler ile izleme teknolojileri ve gizlilik alanları Elektronik Haberleşme Direktifi'nde spesifik olarak ele alınmaktadır. Öte yandan, Taslak Elektronik Haberleşme Direktifi'nin herhangi bir düzenleme yapmadığı konularda, GDPR doğrudan etkili hukuki metin olarak geçerli olacaktır.[351]

İlk kez 2017 yılında yayımlanan Elektronik Haberleşme Direktifi taslağını, sonuncusu 10 Şubat 2021'de yayımlanan taslak metin takip etmiştir.[352] Son taslak metinle,[353] Elektronik Haberleşme Direktifi'ndeki belirsiz hususlar ayrıntılandırılarak; çerez uygulamalarına ilişkin daha çok ve ayrıntılı istisnalar öngörülmüştür. Kriter A ve Kriter B istisnalarının yanı sıra rıza yorgunluğu gibi hususlara da yer verilmiştir.

İlgili Direktif Taslağı'nda, Kriter A istisnasına ilişkin birtakım değişiklikler öngörülmüştür. Bunlardan ilki 8/1-(da) maddesinde bahsi geçen husus, amaç bilgi toplumu hizmetleri ya da terminal cihazların güvenliğini sağlamak veya dolandırıcılığın önlenmesi olduğunda, kullanıcının rızasının alınmasına gerek olmadığıdır. Aynı maddenin (f) bendinde yer alan hüküm gereğince, acil durumlarda kullanıcının terminal cihazına yapılacak olan konum tespiti için de kullanıcının rızasına gerek duyulmamaktadır. Madde 8/1-(d)'de ise internet sayfasına giriş yapan kullanıcıların sayfada kalma veya hangi sayfaları ziyaret ettiği gibi analize veya internet sayfası açısından istatistiki bilgileri toplamaya yardımcı olan çerezler için de kullanıcının açık rızasının aranmayabileceğine yer verilmiştir. İnternet sayfası, söz konusu analizi üçüncü bir tarafa yaptırıyorsa; GDPR'nin 26. ve 28. maddelerinde belirtilen koşullar sağlanması halinde, üçüncü taraf da birinci tarafla birlikte müştereken sorumlu kabul edildiğinden; üçüncü taraf da bu açık rıza almama muafiyetinden yararlanabilecektir.

---

[351] González, "Proposed ePrivacy Regulation," 4-5.

[352] Elektronik Haberleşme Direktifi'nde yapılan değişiklikleri gösteren taslakların yayımlanma süreci, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010 , Erişim Tarihi: 1 Ağustos 2022.

[353] 10 Şubat 2021 tarihli Elektronik Haberleşme Direktifi Taslağı, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN , Erişim Tarihi: 1 Ağustos 2022.

İlgili Direktif Taslağı'nın Giriş Bölümü'ndeki 21b sayılı maddesinde açıklandığı ve 8/1-(e) maddesinde belirtildiği üzere, kullanıcının cihazında seçtiği gizlilik ayarını değiştirmesine gerek olmadığı müddetçe yazılım güncellemenin cihazın güvenliği için gerekmesi ya da güncelleme gerçekleştirilmeden önce kullanıcının güncellemeyle ilgili bilgilendirilerek bu otomatik kurulumu dilerse başka bir zamana erteleme imkanı sunulması halinde, söz konusu yazılım güncellemeleri de açık rızadan muaf tutulmuştur. Kullanıcıdan bir işlemeye ilişkin rıza alındıktan sonra işleme amacının dışına çıkılarak başka bir konuda işleme faaliyetinin gerçekleştirilmek istenmesi hali ise Taslak'ın 8/1-(g) maddesinde incelenmiştir. Bu diğer amaç için kullanıcının rızasının varlığı sorgulandıktan sonra eğer yoksa, diğer AB düzenlemelerinde veya üye devletin kendi iç hukukunda işlemeyi meşru kılan başka bir durumun varlığı sorgulanmalıdır. Bunun da yokluğu halinde, işleme amacının kullanıcıdan alınan ilk veri işleme amacıyla uyumlu olup olmadığına bakılacaktır. İki amacın birbiriyle uyumlu olduğu düşünüldüğü takdirde; amacın gerçekleştiği anda elde edilen verilerin silinmesi veya anonim hale getirilmesi, kullanıcı profili ortaya çıkarma hedefine yönelik olmaması ve şifreleme ya da takma ad gibi uygun güvenlik önlemlerinin alınmış olması halinde, söz konusu ikinci amaç için kullanıcının yeniden rızasının alınmasına gerek görülmemektedir.

Taslak Direktif metninde değişikliğiyle dikkat çeken bir diğer husus ise Kriter A istisnasına getirilen düzenlemelerdir. İnternet üzerinden sağlanan hizmetlerden OTT haberleşme hizmetleri, işlevsel olarak geleneksel iletişim araçlarına eşdeğer nitelikte olduğundan kişilerin haberleşmelerinin gizliliğini etkileme potansiyeli bulunmaktadır. Önceki yıllarda yalnızca kablolu iletişim araçları ile haberleşme yapılabiliyorken; günümüzde Skype ve benzeri hizmet sağlayıcılar vasıtasıyla internet üzerinden haberleşme hizmetlerinden faydalanılabilmektedir.[354]

2018/1972 sayılı Direktif olan Avrupa Elektronik Haberleşme Kanunu'nun[355] 2/4 maddesinde yer verilen elektronik haberleşme hizmetleri kavramı; kişilerarası iletişim hizmeti, 2015/2120 sayılı Direktif'in[356] 2/2-(2) maddesinde tanımlandığı şekliyle internet

[354] González, "Proposed ePrivacy Regulation," 7.
[355] European Electronic Communications Code, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN , Erişim Tarihi: 3 Ağustos 2022.
[356] 2015/2120 sayılı Açık İnternet Erişimi ile ilgili Önlemleri Belirleyen ve Evrensel Hizmet ve Elektronik İletişim Ağları ve Hizmetlerine İlişkin Kullanıcı Haklarına İlişkin 2002/22/EC Sayılı Direktif'i ve AB İçerisinde Genel Mobil İletişim Ağlarında Dolaşıma İlişkin 531/2012 Sayılı Direktif'te Değişiklik Yapan Direktif, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN , Erişim Tarihi: 20 Ağustos 2022.

erişim hizmeti ve makineler arası sinyallerin iletilmesini sağlayan hizmet türlerini kapsayan, elektronik iletişim ağları aracılığıyla ücret karşılığında sağlanan hizmet anlamına gelmektedir.

Elektronik Haberleşme Direktifi yalnızca telekomünikasyon şirketlerini ve internet servis sağlayıcılarını kapsamaktayken; internet üzerinden haberleşme hizmeti veya bilgi toplumu hizmeti sunanlar dahil edilmemişti.[357] İlgili Taslak metnin Giriş Bölümü'ndeki 11. maddesinde de söz konusu elektronik haberleşme servisi tanımına değinilerek; bunların dışında internet tabanlı iletişim hizmeti kullanıcılarının da etkin ve eşit bir şekilde korunabilmelerinin amaçlandığı belirtilmiştir. Böylelikle, elektronik haberleşme işletmecilerinin yanı sıra Whatsapp gibi internet tabanlı servis sağlayıcılarının da çerezlerle ilgili Direktif'e tabi olacağına ilişkin hükümler getirilmesi hedeflenmiştir.[358]

Whatsapp gibi kişiler arası iletişim hizmetleri, Netflix gibi yayın hizmetleri ve sinyal iletimi sağlayanlar, bir şirkete dışarıdaki internet vasıtasıyla erişimi sağlayan VPN'i (Virtual Private Network -Sanal Özel Ağ)[359] de kapsayacak hükümler getirilmesinin yanı sıra birbirleriyle iletişim kuran cihazların hızlı artış göstermesiyle nesnelerin interneti yaygınlaşmasına rağmen; Article 29 Çalışma Grubu, yalnızca makineler arası iletişimde kişisel verileri veya gizliliği etkileyen herhangi bir etki

[357] Meg Leta Jones, Jenny Lee, "Comparing Consent to Cookies: A Case for Protecting Non-Use," *Cornell International Law Journal* 53, no.1 (2020): 116, https://community.lawschool.cornell.edu/wp-content/uploads/2021/03/Jones-Lee-final.pdf , Erişim Tarihi: 21 Ağustos 2022; Papakonstantinou, "ePrivacy 2011 Implementation," 42-43.

[358] Aksoy, "Çerezler," 71.

[359] Şirket çalışanlarına özgülenmiş belirli kullanıcılar tarafından kullanılması için tasarlanmış parola korumalı ağ olan "intranet" kavramının ortaya çıkmasından sonra şimdilerde birçok şirket genellikle kendi sanal özel ağları olan VPN'lerini oluşturarak, uzaktan çalışan personellerinin ya da sanal ofis olarak kurdukları şirket merkezlerinin özel ağ ihtiyaçlarını karşılamaktadır. Esasen VPN, uzak internet sitelerini ya da kullanıcıları birbirlerine bağlamak amacıyla oluşturulan özel bir ağ olup; şirketin özel ağından uzak internet sitesine ve böylelikle çalışana internet üzerinden yönlendirilen sanal bağlantıları aracılığıyla ulaşma amacı ile kullanılır. Bu çerçevede iyi tasarlanmış bir VPN, coğrafi bağlantıyı genişletmek, güvenliği iyileştirmek, işletim maliyetlerini azaltmak, üretkenliği artırmak, ağ topolojisini basitleştirmek, küresel ağ oluşturma fırsatları sağlamak, uzaktan çalışma desteği sağlamak, geniş bant uyumluluğu sağlamak gibi şirketlere büyük faydalar sağlayabilir. Ayrıca iyi tasarlanmış bir VPN, güvenlik, güvenilirlik, ölçeklenebilirlik, ağ yönetimi gibi özellikleri taşımalıdır. Farklı türde VPN türleri bulunmakla birlikte, Uzaktan Erişim VPN (Remote-Access VPN) ve Siteden Siteye VPN (Site-to-Site VPN) en yaygın VPN türleridir. Örneğin; uzaktan erişimli bir VPN'e ihtiyacı olan sahada yüzlerce satış elemanı olan bir şirket özel ağı ile bir hizmet sağlayıcı aracılığıyla uzak kullanıcılar arasında, güvenli ve şifreli bağlantılar kurabilir. (Jeff Tyson, "How Virtual Private Networks Work," communicat.com.au, https://www.communicat.com.au/wp-content/uploads/2013/04/how_vpn_work.pdf , Erişim Tarihi: 23 Ağustos 2022.)

olmadığından; yalnızca makineler arası iletişimin sağlanması durumunda Elektronik Haberleşme Direktifi'nin uygulama alanı bulmayacağını belirtmiştir.[360]

6. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE İŞLENMESİ İÇİN ABONEDEN ALINAN KİŞİSEL VERİLER

Elektronik haberleşme sektörünün aktörü konumundaki şirketler, temelde üç tür veri işlemektedir. Bu veriler; abone verileri, meta veri ve iletişim içeriğine dair veriler olmak üzere üç başlıkta sınıflandırılabilir. Abone verileri, yeni bir abonelik sözleşmesinin kurulması ve sözleşmenin uygulanması sırasında abonelerden talep edilen kişisel bilgilerdir. Meta veri; aranan numaralar, ziyaret edilen internet sitelerine ilişkin URL (Uniform Resource Locator- Tek Tip Kaynak Bulucu) verileri, terminal ekipmanının bağlantı noktasına ilişkin konum verileri, tarih ve saat içeren haberleşme süreleri, ses ya da veri içeren haberleşme türü bilgisini kapsar. Bu çerçevede telekom operatörleri, aranan numara/tarih/saat/sesli aramanın süresi hakkında ayrıntılı verilere sahiptir. ISS'lerin ise baz istasyonu üçgenlemesi[361] yerine GPS[362] kullandıkları için daha iyi coğrafi konum verilerine sahip olduğu söylenebilir. İşlenen diğer veri türü olan iletişimin içeriğine dair veriler ise sesli arama içeriği, SMS metni, sesli posta mesajı ve elektronik posta içeriğinden oluşmaktadır.[363]

---

[360] González, "Proposed ePrivacy Regulation," 7-8.

[361] Baz istasyonu üçgenlemesi, telefonu açık olan kullanıcıların yaydıkları sinyallerin yoğunluğunun hesaplanmasıyla konum belirlenmesine yönelik olarak yapılan takip türüdür. Hizmet sağlayıcıya ait en az üç adet baz istasyonunun varlığı halinde, genellikle kullanıcıların konumu yaklaşık olarak tahmin edilebilir. Söz konusu belirleme, kullanıcının net konumunu göstermemekle birlikte yaklaşık 1 kilometreye kadar bulunabileceği alanı göstermektedir. Bu konum belirlemesinin gerçekleştirilebilmesi için kullanıcının telefonunun açık olmasının yanı sıra SIM kartının takılı olarak hizmet sağlayıcısına sinyal göndermesi gerekmektedir. Bu üç durumun birlikte varlığı halinde kullanıcının konumu yaklaşık olarak belirlenebilmektedir. (Surveillance Self-Defense, "Cep Telefonları: Konum Takibi," Son Güncelleme: 4 Mayıs 2021, https://ssd.eff.org/tr, https://ssd.eff.org/tr/module/cep-telefonlar%C4%B1-konum-takibi , Erişim Tarihi: 23 Ağustos 2022.)

[362] Küresel Konumlandırma Servisi (Global Positioning System-GPS), uydu ile iletişim halinde olan bir cihaz aracılığıyla kullanıcının yerini belirler. Birden fazla uydu tarafından yapılan üçgenleme, cihazı konumlandırarak, GPS'i konum bulmak için en doğru yöntem haline getirir. (Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, "Location-Sharing Technologies: Privacy Risks and Controls," TPRC 2009, (2010): 2 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997782 . Erişim Tarihi: 24 Ağustos 2022.)

[363] Papakonstantinou, "Big Data Analytics," 13.

Abonelik başvurusu kapsamında işletmecinin internet sitesi üzerinden otomatik yöntemlerle elde edilen abone adayının adı, soyadı, GSM numarası ve sabit telefon numarasından oluşan kişisel verileri, başta 5809 sayılı EHK olmak üzere işletmecilerin uymakla yükümlü olduğu mevzuat gereğince, abone adayının başvurusunun değerlendirilmesi, abonelik başvurusuyla ilgili bilgilendirme amacıyla iletişime geçilebilmesi kapsamında işlenmektedir.[364] İnternet hizmeti veren işletmeciler, bahsi geçen bu bilgilere ek olarak internet altyapısıyla ilgili incelemenin yapılabilmesi ve işletmecinin o adrese hizmet verip veremeyeceğinin tespiti için ayrıca abone adayının adres bilgisine ihtiyaç duymakta ve başvuru sürecinde abone adayından adres bilgisini de alarak işlemektedir.[365]

Abonelik başlatılması konusunda iradesini işletmeciye iletmiş olan abone adayıyla işletmeci arasında abonelik sözleşmesi imzalanmakta ve abone adayı tarafından kimlik bilgilerini içeren kimlik belgesi, adına kayıtlı fatura örneği ve benzeri evrak işletmeciye sunulmaktadır.[366] Genellikle abonelik sözleşmesinin ilk sayfasında bulunan abone bilgi formuyla da abonenin birçok kişisel verisi alınmaktadır. Abonelik başlatılması esnasında abone adayı tarafından sunulan kimlik belgesinin yanı sıra abone adayının beyanıyla doldurulabilecek bilgiler doğrultusunda abone bilgi formu tamamlanmaktadır.[367]

Elektronik haberleşme sektöründeki işletmeciler, haberleşme hizmeti vermeleri dolayısıyla normalden daha fazla veri işlemekle yükümlü olmaktadır. Diğer hizmet ve mal satışı yapan şirketler, genellikle müşterilerinin yalnızca ad, soyadı ve iletişim bilgilerini işlerken; elektronik haberleşme sektöründeki işletmeciler, bu bilgilere ek olarak, abonelerinin haberleşme hizmetleri kullanmalarından kaynaklı ortaya çıkan haberleşme trafiğine ilişkin verileri de işlemekle yükümlüdür.

---

[364] Turkcell İletişim Hizmetleri A.Ş., Ön Başvuru Formu, https://www.turkcell.com.tr/tr/form/gnc-numara-tasima-on-basvuru-formu ; Netgsm A.Ş., Ön Kayıt, https://www.netgsm.com.tr/on-kayit , Erişim Tarihi: 23 Ağustos 2022.

[365] Turknet İletişim Hizmetleri A.Ş., Başvuru Formu, https://turk.net/taahhutsuz-ozgur-iletisim-abonelik , Erişim Tarihi: 23 Ağustos 2022.

[366] Vodafone Net İletişim Hizmetleri A.Ş., Hizmetlerden Yararlanmak İçin Gerekli Evraklar, https://www.vodafone.com.tr/yardim/hizmetlerden-yararlanmak-icin-gerekli-evraklar-nelerdir-330 ; Turkcell İletişim Hizmetleri A.Ş., Abonelik İşlemleri, https://www.turkcell.com.tr/yardim/hattiniz/abonelik-islemleri/fatura-alternatifleri-nelerdir , Erişim Tarihi: 25 Ağustos 2022.

[367] Netgsm A.Ş., Bireysel Sabit Telefon Hizmetleri Abonelik Sözleşmesi, https://www.netgsm.com.tr/abonelik/sozlesme/bireyselabonelik.php , Erişim Tarihi: 25 Ağustos 2022.

İşletmeciler, abonelerin; adı, soyadı, kimlik numarası, uyruk, doğum yeri ve tarihi, pasaport numarası, kimlik belge numarası, cinsiyet, medeni hal, fotoğraf ve kurumsal abonelik ise bunlara ek olarak abonelik yetkilisine ait imza beyannamesi, imza sirküleri veya vekaletname ve benzeri belge örnekleri ve bilgilerden oluşan kimlik bilgileri; adres bilgisi, sabit telefon numarası, GSM numarası, e-posta adresi, sosyal medya hesapları ve adına kayıtlı hat numarası gibi iletişim bilgileri; tarife, paket veya abonelik kullanım bilgileri, abone veya kullanıcı numarası anlamına gelen MSISDN[368]; ses ve SMS çağrılarının tarih-saat-arama süresi bilgisi, internet üzerindeki erişimlere ilişkin sisteme bağlanma ve sistemden ayrılma tarih-saat bilgileri, trafik verileri, cihaz bilgileri, SIM kartın[369] kullanıldığı cihaza ait konum bilgileri gibi verileri işlemektedir. Bununla birlikte, işletmeci tarafından işlenen diğer veriler ise abonelik yapılma sürecinde iletilen bilgi ve belgeler ile uzaktan abonelik esnasında alınan video ve fotoğraf kayıtları, abonelik başlatılırken veya daha sonrasında seçilen güvenlik kelimeleri, çağrı merkezi standartları gereği tutulan ses kayıtları, arayan kişinin kimliğinin daha sonraki görüşmelerde tespiti amacıyla alınan ses kaydı ve abonenin satış kanallarına ilettiği taleplerden oluşan işletmeci ve diğer satış kanallarında bulunan bilgilerdir. İşletmecinin aboneye sunduğu mobil uygulamalar üzerinden alınan cihaz, konum, ağ ve şebeke kullanım verileri, işletmecinin sunduğu ürün ve hizmetlerin aboneler tarafından ne kadar ve hangilerinin kullanıldığına ilişkin alışkanlıklar, işletmecinin internet sayfası veya mobil uygulaması vasıtasıyla sunulan ürün ve hizmetlere ilişkin tanıtımlara dair abonelerin davranışları ve çerezlerden oluşan hizmetlerin ve ürünlerin kullanımına ilişkin bilgilerin de işlendiğine aydınlatma metinlerinde yer verilmektedir. Son olarak işletmeciler abonelerin geçmiş döneme ait faturalarını ödeyip ödemediklerine ilişkin

[368] Mobile Station Integrated Services Digital Network (MSISDN- Mobil İstasyon Entegre Hizmetler Dijital Ağı), bir mobil kullanıcıya atanan ITU-T Tavsiyesi E.164 numaralandırma planına göre yapılandırılmış telefon numarasıdır. Bu telefon numarası, operatörün herhangi bir abonesinin bir mobil istasyonu aramasını mümkün kılan, ülke kodu ve ulusal hedef kodundan oluşur. Bir MSISDN'nin maksimum 15 basamak uzunluğundadır. International Mobil Subscriber Identity (IMSI) ve MSISDN arasındaki temel fark, IMSI operatör tarafından bir aboneyi tanımlayan, MSISDN ise tuşlamada kullanılan numaradır. Bir başka deyişle, cep telefonu ile arama yapıldığında aranılan, cep telefonunun IMSI numarası değil, MSISDN numarasıdır. (Simbase Telecommunication, MSISDN, https://www.simbase.com/iot-glossary-dictionary/msisdn . Erişim Tarihi:26 Ağustos 2022).

[369] Cep telefonlarında kullanılan SIM (Subscriber Identity Modüle-Abone Kimlik Modülü) kartlar, kullanıcılarının hücresel ağda kimliğinin doğrulanmasının yanı sıra gerekli güvenlik koşullarını sağlayan, veri şifreleme ve şifre çözme işlemlerini gerçekleştiren güvenli bir depolama alanına sahiptir. (Garima Jain, Sanjeet Dahiya, "NFC: Advantages, Limits and Future Scope," *International Journal on Cybernetics & Informatics (IJCI)* 4, no.4 (2015): 6, https://airccse.org/journal/ijci/papers/4415ijci01.pdf , Erişim Tarihi: 28 Ağustos 2022.)

bilgi, ön ödemeli kullanıcıların harcama potansiyelleri, abonelere sunulacak hizmetler ve cihaz kampanyaları için abonenin ekonomik düzeyinin ölçülebilmesi amacıyla kredi notu bilgileri; gazi veya engellilere ait sağlık bilgileri, uzaktan abonelik esnasında alınan ses kaydına ilişkin biyometrik veriler ile görüntü kaydı ve fotoğraf çekimi sebebiyle alınan fotoğraf kaydının kimlik bilgilerindeki fotoğraf ile eşleştirilmesi sonucu elde edilen yüz tanıma bilgileri, dijital imza bilgileri ve sendika, dernek ve vakfa üyelik bilgilerinden oluşan özel nitelikli kişisel verilerden oluşan verileri işlemekte olup; internet sayfalarında ve mobil uygulamalarında yer alan aydınlatma metinlerinde bu verileri işlediklerinden bahsetmektedir.[370]

Bu doğrultuda, elektronik haberleşme sektöründe çok sayıda ve çeşitlilikte kişisel veri işlenmekte olup; çalışmanın bu bölümünde genel olarak bu sektörde işlenmekte olan kişisel verilerin neler olduğuna ilişkin ayrıntılı bilgilere yer verilecektir. Kişisel verilerin korunması hukuku ve elektronik haberleşme hukuku bağlamında gerek olmadığı sürece kişisel veri işlenmesinin önüne geçebilmek amacıyla işlemin amacına yönelik başka hangi yöntemlerin benimsenebileceğine ilişkin uygulamaya yönelik önerilerde bulunulacaktır.

6.1. ABONELİK KURULMADAN ÖNCE ABONE ADAYINDAN ALINAN KİŞİSEL VERİLER

Elektronik haberleşme sektöründeki işletmecilerden hizmet almak isteyen abone adayı, teknolojinin sunduğu imkanlar dolayısıyla internet üzerinden işletmecilerin web siteleri aracılığıyla hem hizmet alabileceği işletmecileri hem de sundukları hizmetleri inceleyebilmektedir. İnternet veya haberleşme hizmeti almak isteyen bir kişi, öncelikle elektronik haberleşme sektöründe faaliyet gösteren bir işletmeciye başvurmalıdır. Elektronik haberleşme sektöründe aboneliği başlatılmamış olan ancak abone olma iradesini işletmeciye sunmuş olan kişi olarak adlandırabileceğimiz abone adayı, internet üzerinden abonelik başvurusunda bulunmak istemesi halinde, işletmecinin internet sitesindeki başvuru formunu doldurarak abonelik sürecini başlatabilmektedir.[371] Abone

[370] Netgsm A.Ş., Aydınlatma Metni - Kişisel Verilerinizin Aktarıldığı Taraflar ve Aktarım Amaçları, https://www.netgsm.com.tr/gizlilik-ve-guvenlik/ ; Turkcell İletişim Hizmetleri A.Ş., Aydınlatma Metni - Kişisel Verileriniz Nelerdir?, https://www.turkcell.com.tr/tr/gizlilik-ve-guvenlik?page=kisisel-verilerin-korunmasi , Erişim Tarihi: 29 Ağustos 2022.

[371] Turknet İletişim Hizmetleri A.Ş. Başvuru Formu, https://turk.net/taahhutsuz-ozgur-iletisim-abonelik , Erişim Tarihi: 29 Ağustos 2022.

adayıyla iletişime geçilebilmesi için alınan bilgilerin bulunduğu arayüzde, işletmeci tarafından sunulan hizmetler kapsamında alınan kişisel verilerin hangi amaçlarla ve hangi sürelerde işlendiği ve kişisel verilerin kimlerle paylaşıldığı hakkında aydınlatma metni sunulmaktadır.[372]

Abone adayının gerekli evraklar ve abonelik süreci hakkında bilgilendirilmesi, yarım kalan abonelik süreci varsa bunun devam ettirilmesi ve abonelik sürecinde kimlik teyidinin gerçekleştirilebilmesi amacıyla işletmeci tarafından abone adayıyla iletişime geçilmesini gerektirmektedir. İletişime geçebilmek de abone adayı, ad-soyadı, iletişim bilgileri, kimlik numarası gibi temel düzeydeki kişisel verilerin işletmeci tarafından alınmış olmasını mecburi kılmaktadır.

Genellikle abonelik başlatmak isteyen abone adayı kendi rızasıyla işletmeciye başvurarak; kendisiyle iletişime geçilmesi için bilgilerini verse de işletmeci bu aşamada abone adayından ilgili kişisel verilerinin sözleşme kurulumu sürecindeki gerekli bilgileri aktarmak amacıyla işlenmesi için usulüne uygun şekilde abone adayının açık rızasını alarak hukuken kendini koruma altına almak istemektedir. Böylece işletmeci, KVKK'nın 5/1 maddesinde belirtilen ilgili kişi olan abone adayının açık rızasının bulunması sebebiyle kişisel verilerini işlemektedir.

Mal veya hizmetin satışı henüz tamamlanmamış olsa dahi hizmetten faydalanmak isteyen kişi tüketici olarak kabul edilmektedir.[373] Elektronik haberleşme sektörü açısından bu kavram düşünüldüğünde ise henüz abone olmamış abone adayının da işletmeci açısından tüketici olarak kabul edilmesi gerekmektedir. Nitekim Kişisel Verilerin İşlenmesi Yönetmeliği'nin kapsamına yer verilen 2. maddesi, işletmecilerin elektronik haberleşme hizmeti sunmak üzere elde ettikleri kişisel verilerle ilgili uygulanacak hükümleri içermektedir. Bu doğrultuda, abone adayı ile abonelik süreci tamamlanmasa bile, bahsi geçen kişisel verilerin elektronik haberleşme hizmeti sunma amacıyla abonelik sürecinin tamamlanabilmesi için işlenmiş olması sebebiyle, abonenin verilerinin işlenmesi ve saklanması konusuna gösterilen ihtimam, abone adayının verileri için de geçerli olmalıdır.

---

[372] Turkcell İletişim Hizmetleri A.Ş., Abonelik Başvurusu Aydınlatma Metni, https://www.turkcell.com.tr/tr/turkcell-abonelik-basvurusu-aydinlatma-metni , Erişim Tarihi: 29 Ağustos 2022.

[373] Açıkgöz, *Genel İşlem Koşulları*, 22.

6.2. ABONELİK TESİSİ SIRASINDA ALINAN KİŞİSEL VERİLER

Elektronik haberleşme hizmetlerinden faydalanmak isteyen abone adayının, kendisi ile iletişime geçilebilmesi için bilgilerini işletmeciyle paylaşmasından sonra abone adayının işletmecinin sunduğu hizmetlerden faydalanma talebinin devam etmesi veya abone adayının bizzat işletmeciye başvurarak hemen abone olmak istemesi halinde, abonelik evrakının tamamlanması aşamasına geçilir.

İşletmeciler, aboneye ait kişisel verilerin çoğunluğunu aboneliğin kuruluş aşamasında almaktadır. Tüketici Hakları Yönetmeliği'nin 7/5 maddesinde yer verildiği üzere; abonelik sözleşmelerinin kuruluşu aşamasında işletmeci tarafından, kişiden kimlik belgesi ya da kimlik belgesi yerine kabul edilen diğer belgelerden birinin aslının sunulması talep edilmelidir. Bu belgeler, Türkiye Cumhuriyeti kimlik numarasını veya Türkiye Cumhuriyeti tarafından verilen yabancı kimlik numarasını içeren kimlik belgesi, geçerlilik tarihi uygun olan uluslararası geçerliliği olan kimlik belgesi; kurumsal abonelik kurulmak isteniyorsa, yetkilinin kimlik belgesi veya yetkilendirildiğini gösteren resmi belge, vergi kimlik numarasını içeren resmi belge veya vergi kimlik numarası yoksa benzer nitelikteki diğer belgeler olup; işletmeci tarafından bu belgelerin aslı incelendikten sonra elektronik ortamda bir suretini alması gerekmektedir. Aynı Yönetmeliğin 7/6 maddesinde ise uzaktan abonelik yapılması halinde uygulanacak olan yöntemlere göre kimlik doğrulamanın nasıl yapılacağına ilişkin Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik'in[374] (Kimlik Doğrulama Yönetmeliği) ilgili maddelerine atıf yapılmıştır.

5809 sayılı EHK'nın 56. maddesinin 3. fıkra hükmü gereğince de yukarıda sayılan kimlik belgelerinin örneği alınmadan abonelik tesis edilmesi yasaklanmıştır. Abonenin kimlik belgesinin suretini almadan abonelik tesisi yapılması halinde, işletmecinin mevzuata aykırı şekilde tesis ettiği abonelik sözleşmesi nedeniyle, İdari Yaptırımlar Yönetmeliği uyarınca idari para cezası uygulanmaktadır.[375]

Abonelik sözleşmeleri imzalandıktan sonra ise Tüketici Hakları Yönetmeliği'nin 7/9 maddesinde belirtildiği üzere; abone tarafından sözleşmenin istenildiği şeklin

[374] R.G. 26.06.2021, S. 31523.

[375] BTK'nın 04.05.2021 tarih ve 2021/İK-SDD/120 sayılı Kurul Kararı'nda; Tüketici Hakları Yönetmeliği'nin 7/6-(a) ve (b) maddesine aykırılık teşkil edecek şekilde, kimlik belgesinin suretini almaksızın hizmet sunan işletmeci hakkında; İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) maddesinin 8. alt bendi uyarınca idari para cezası uygulanması kararı verilmiştir.

belirtilmemesi halinde, sözleşmenin kuruluş şekline göre değişkenlik gösterecek şekilde kağıt ortamında ya da diğer elektronik ortamlarda bir nüshası aboneye verilmelidir.

Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nde Değişiklik Yapılmasına Dair Yönetmelik'in[376] (Değişik Tüketici Hakları Yönetmeliği) 31 Aralık 2022 tarihinde yürürlüğe giren 5. maddesi ile Tüketici Hakları Yönetmeliği'nin 7. maddesine getirilen 12. fıkrada, uzun sayfalı abonelik sözleşmelerinde abonenin kendi yükümlülüklerinin ve tercihlerinin farkında olamaması halini bertaraf edebilmek için elektronik haberleşme sektörüne "sözleşme özeti" kavramı kazandırılmıştır.

Sözleşme özeti, Tüketici Hakları Yönetmeliği'nin 7/12 maddesinde belirtildiği üzere abonelik sözleşmesinin ayrılmaz parçası olup; bir nüshası abonelik sözleşmesi gibi yine kağıt veya elektronik ortamda abone olan kişiye verilmelidir. Ayrıca aynı hükümde yer verildiği üzere sözleşme özetinde, işletmeciye ilişkin unvan ve iletişim bilgilerinin yanı sıra abonelik numarası, seçilen tarife ve paket bilgisi, aylık ücret tutarı, hizmetin özellikleri, internet hizmetiyse abonenin adresine sunulabilecek internet hızları ve feshe ilişkin birtakım hususlar ve benzeri bilgilere yer verilmelidir. 31 Aralık 2022 tarihi itibariyle abonelik tesisi sırasında, abonelik sözleşmesinin bir nüshasının aboneye tesliminin yanı sıra bahsi geçen sözleşme özeti de aboneye sunulmaktadır.

Bu bölümde, abonelik sözleşmeleri vasıtasıyla abone olacak kişiden alınan kişisel veriler ayrıntılı şekilde incelenerek; bu verilerin hangi amaçlarla işlendiğine ilişkin hukuki dayanaklara yer verilerek ve bu verilerin toplanmasında hukuki yarar bulunmayan hallerin var olup olmadığının tespiti yapılarak çözüm yolları araştırılacaktır.

6.2.1. Abone Bilgi Formuyla Alınan Kişisel Veriler

Elektronik haberleşme sektöründe işletmeciler tarafından abonelik sözleşmeleri, BTK mevzuatına uygun olarak ve her abone ile aynı sözleşmenin imzalanabileceği şekilde standart formatta hazırlanmaktadır.[377] Abonelik sözleşmeleri, yükümlülük ve haklar bakımından her abone için aynı içerikte olsa da söz konusu sözleşmelerin aboneye özgü kısmını, genellikle bu sözleşmelerin başında bulunan abone bilgi formları oluşturmaktadır. Abone bilgi formu, abone ve işletmeciye ait kimlik ve iletişim

[376] R.G. 18.01.2022, S. 31723.
[377] Seda Öktem Çevik, *Mobil Telefon Abonelik Sözleşmesi*, (İstanbul: Beta Basım Yayım, 2008), 6.

bilgilerinin özet halde yer aldığı form olarak tanımlanabilmekte olup; genellikle abonelik sözleşmelerinin ilk sayfasında yer almaktadır.[378]

Abone adayı yeni abonelik yapmak üzere internet üzerinden veya yüz yüze işletmeciyle iletişime geçtiğinde ya da elektronik ortamda işletmeciye başvuru yaptığında; abonelik tesisi için birtakım kimlik ve iletişim bilgileri vermekte ve bu bilgiler form üzerine işlenmektedir. Bu bilgilerden bazıları, adres ve telefon bilgilerinden oluşan iletişim bilgileri ve ad, soyadı, kimlik belgesindeki bilgilerinden oluşan kimlik bilgileri; kurumsal abonelik ise yetkilinin kimlik bilgileriyle tüzel kişiliğe ait vergi kimlik bilgileri; aboneliğin kurulduğu yer bilgisidir. Ayrıca faturanın e-posta adresine gönderilmesi, abonelik numarasının rehbere kaydedilmesi, siyasi veya cinsel içerikli mesaj almak isteyip istemediği, numaranın karşı tarafta görünmemesi (CLIR)[379] gibi hususlara ilişkin olan abone tercihleri de abone bilgi formlarında bulunmaktadır.[380]

Abone bilgi formlarında bulunan abone tercihlerinin abone tarafından doğru şekilde belirtilmesi, abonelik kullanımı esnasında aboneye sunulan hizmetleri veya sunulan hizmetin uygulama şeklini doğrudan etkilemektedir. Tüketici Hakları Yönetmeliği'nin 7/10 maddesinde belirtildiği üzere, abonenin bilgilerinin rehbere eklenmesi tercihinin, abone bilgi formunda bulunan abone tercihleri bölümünde alınması gerekmektedir. Bu yöndeki tercihini değiştirme hakkı daha sonra aboneye sunulabilirken; konuya ilişkin açık rızanın abonelik sözleşmesinin bu bölümünde yer alması gerektiği hüküm altına alınmıştır.

Benzer şekilde, abone tarafından onay verilmediği halde kendisine işletmecinin başka bir şirketin reklamına aracılık ettiği reklam içerikli SMS gönderilmesi halinde, Kişisel Verilerin İşlenmesi Yönetmeliği'nin 13/6 maddesi uyarınca abone veya kullanıcının talebine yönelik ispat yükünün işletmecide olduğu belirtildiğinden; taraflara ilişkin hak ve yükümlülükleri belirleyen ve esaslı unsurlara yer verilen abonelik

---

[378] TT Mobil İletişim Hizmetleri A.Ş., TT Mobil Mobil Telefon Hizmetleri Bireysel Tip Abonelik Sözleşmesi, https://www.turktelekom.com.tr/tt-yardim/Documents/TT-mobil-bireysel-abonelik-sozlesmesi.pdf , Erişim Tarihi: 1 Eylül 2022.

[379] "Calling Line Identification Restriction"ın kısaltması olan CLIR, arayan hat tanımlama kısıtlaması anlamına gelir. Bu özellik etkinleştirilerek uygulanabilir hale geldiğinde, arayan tarafa ait ISDN numarası ve herhangi bir alt adres bilgisi kısıtlanarak aranan tarafa gösterilmesine izin verilmez. (ITU, Calling Line Identification Restriction) (CLIR), https://www.itu.int/rec/T-REC-I.251.4-199208-I/en , Erişim tarihi: 1 Eylül 2022.) Bir başka deyişle, telefon ile bir arama gerçekleştirildiğinde, aranan kişinin telefon numarası bilinmez hale gelir. Uygulamada operatörler arasında "özel numara" çağrıları olarak bilinen bu özellik, arayan kişinin arama öncesinde "numarayı gizle" özelliğini aktifleştirmesiyle meydana gelir.

[380] Netgsm A.Ş., Bireysel Sabit Telefon Hizmeti Abonelik Sözleşmesi, https://www.netgsm.com.tr/abonelik/sozlesme/bireyselabonelik.php , Erişim Tarihi: 1 Eylül 2022.

sözleşmesinde abonenin reklam içerikli SMS almaya yönelik tercihi bulunmadığından işletmecinin aboneden bu onayı başka hangi kanallardan almış olduğunu ispat etmesi gerekmektedir.

Abone tercihlerinin önemine işaret eden bir başka örnek ise; abonenin görme engelli olduğunu Abone Bilgi Formu'nda belirtmiş olması halidir. Mülga Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin[381] 5/1-(i) maddesinde, görme engelli abonelere abonelik sözleşmesinin ve faturalarının uygun formatta gönderilmesi, aboneye hak olarak sunulmuştu. İşletmeciler arasında abone dostu kullanım amacıyla Braille alfabesiyle abonelik sözleşmelerini hazırlayanların yanında, çoğu işletmeci abone talep etmediği sürece bu seçeneği sunmamaktaydı. Genel işlem şartlarını içeren abonelik sözleşmelerinde, abonenin işletmeci karşısında korunması gereken taraf olması sebebiyle, bu konuda da işletmeciye yükümlülük getirilmesi daha uygun olacağından; Kurum, abonenin görme engelli olması halinde abonelik sözleşmesinin şeklini ve uluslararası dolaşıma çıkan aboneye bilgi verilmesi hallerini yeniden düzenlemiştir. Tüketici Hakları Yönetmeliği'nin 7/11 maddesiyle işletmeciye, görme engelli aboneye abonelik sözleşmesi ve faturalarının Braille alfabesiyle veya seslendirilerek sunulması yükümlülüğünü getirmiştir.[382] Aynı şekilde, Tüketici Hakları Yönetmeliği'nin 14. maddesi uyarınca, uluslararası dolaşım hizmetinden yararlanmak isteyen aboneye tarife bilgisinin kısa mesaj yerine, abonenin talebinin olması halinde sesli mesaj şeklinde iletilmesi gerektiğine yer verilmiştir.

Abone bilgi formunda tarife ve paket bilgisine de yer verilerek; abonenin dahil olduğu paketin içeriğinden haberdar olması sağlanarak; herhangi bir yanlışlığın önüne geçilmek amaçlanmıştır. Söz konusu formdaki bir diğer önemli bölüm de abonelik sözleşmesi tesisi sırasında işletmeci adına evrak düzenlenmesinde görevli olan personele ilişkin kimlik bilgilerinin yer aldığı bölümdür. Kimlik Doğrulama Yönetmeliği yürürlüğe girmeden önce uzaktan elektronik yöntemlerle kimlik doğrulamak mümkün değildi. Bu sebeple abonenin bilgisi dışında sahte abonelik tesisi gibi durumlar söz konusu olabilmekteydi. Böyle durumlarda abone bilgi formunda bulunan işletmeci ya da görevli personeli adına EHK'nın 56/4 maddesinde belirtilen, kişinin bilgisi ve rızası olmadan

[381] R.G. 28.07.2010, S. 27655.
[382] Türk Telekomünikasyon A.Ş., Sesli Abonelik Sözleşmesi, https://www.turktelekom.com.tr/yardim/bireysel-mobil/abonelik-sozlesmeleri , Erişim Tarihi: 3 Eylül 2022.

işletmeci ya da onun temsilcisinin abonelik kuramayacağı, gerçek dışı evrak düzenleyemeyeceklerine ilişkin hüküm ve aynı maddenin 5. fıkrasında bahsi geçtiği üzere, gerçek dışı evrak düzenleme ya da evrakı gerçekte olmayan şekilde değiştirme yoluyla kurulan aboneliğin kullanılamayacağına dair hüküm uyarınca sahte abonelik tesis edilmesinden kaynaklı, EHK'nın 63/10 maddesi uyarınca, işlemi gerçekleştiren kişi hakkında soruşturma başlatılarak; elli günden yüz güne kadar adli para cezası ile cezalandırılmaktadır. Söz konusu ön ödeme emrinin yerine getirilmemesi halinde ise kişi hakkında kamu davası açılmaktadır.

6.2.2. Abonenin Adına Kayıtlı Fatura İstenmesi Suretiyle Alınan Kişisel Veriler

Abonelik sözleşmelerinin tesisi sırasında aboneden kimlik belgesi veya muadili belgelerin ibrazı mühim olduğu kadar ibraz edilen belgenin gerçekten ilgili şahıs tarafından sunuluyor olması hususu da bir o kadar önemlidir. Özellikle Kimlik Doğrulama Yönetmeliği yürürlüğe girmeden önce, belgenin doğruluğu mevzuatta belirtilen çeşitli yöntemlerle doğrulanabiliyorken; belgeyi sunan şahsın belgenin asıl sahibi olduğu hususu muallakta kalmaktaydı. İşletmecilerden bazıları, bu belirsizliğin önüne geçerek sahte aboneliği önleyebilmek adına kişiyi doğrulayabilmek için kimlik belgesi dışında aboneden adına kayıtlı fatura istemektedir.[383] Abone adına kayıtlı fatura yerine kredi kartı ekstresi, e-fatura veya bankada gerçekleştirilmiş olan işlemlere ilişkin dekontlar, abonenin üzerine kayıtlı araç ruhsatı, su, doğalgaz, elektrik veya telefon abonelikleri sözleşmeleri de geçerli kabul edilmektedir.[384]

Abone adına kayıtlı fatura istenmesindeki amaç, abonenin kimliğinin doğrulanması olmasına rağmen; aslında işletmeci tarafından ihtiyaç olunmayan birtakım kişisel veriler de aboneden alınmış olmaktadır. Örneğin, GSM aboneliği başlatmak isteyen şahıs tarafından kendi adına kayıtlı su aboneliğine ilişkin fatura örneğinin işletmeciye sunulmasıyla birlikte; ikametgah adresi olmayan bir adresin GSM hizmeti veren işletmecinin eline geçmesi durumu ortaya çıkmaktadır. Her ne kadar bu

[383] Turkcell İletişim Hizmetleri A.Ş., Nasıl Faturalı Hat Alabilirim?, https://m.turkcell.com.tr/yardim/turkcellli-olmak/turkcellli-olmak/nasil-faturali-hat-alabilirim , Erişim Tarihi: 3 Eylül 2022.

[384] Turkcell İletişim Hizmetleri A.Ş., Hat Almak İçin Gerekli Fatura Alternatifleri Nelerdir?, https://www.turkcell.com.tr/yardim/kampanya/kampanyalar-faturali/fatura-alternatifleri-nelerdir , Erişim Tarihi: 3 Eylül 2022.

işletmecinin amacı abonenin söz konusu bilgisini tutmak olmasa da abone tarafından kendisine bu kişisel verinin verilmesiyle birlikte işletmeci bu bilgiyi de saklamakla yükümlü hale gelmektedir. Bu durum, abone açısından kişisel verilerinin yetkili olmayan kişilerin eline geçmesine sebep olurken; işletmeci açısından da gereksiz yük mahiyetindedir.

Kimlik Doğrulama Yönetmeliği ile uzaktan elektronik ortamda kimlik doğrulanması imkanı sağlanarak abonenin Türkiye Cumhuriyeti kimlik belgesini NFC cihazına okutarak, e-Devlet üzerinden veya görüntülü doğrulama yöntemlerinden biri ile işlemlerini gerçekleştirebilmesi ve abonenin sunduğu evraklar ile görüntülerinin eşleştirilebilmesi suretiyle veya e-Devlet üzerinden elektronik imza kullanılarak aboneliğin gerçekleştirilebilmesi imkanı sayesinde, abonelik tesisi için aslında gerek olmayan belgelerin abone tarafından işletmeciye sunulmasının önüne geçilmiştir.

6.2.3. Abone Tarafından Vekaletname veya Vasi Belgesi Sunulması Suretiyle Alınan Kişisel Veriler

Kendisine vasi atanmış kimse adına abonelik başlatılmak istendiğinde, kişi sınırlı ehliyetsiz[385] olduğu için işletmeci tarafından abonelik tesisi esnasında vasi olan kişiden vasi belgesi sunulması istenmektedir. 18 yaşından küçüklerin adına abonelik tesis edebilmesi için noterden alınan anne veya baba tarafından verilmiş muvafakatnameye ek olarak anne veya babaya ait kimlik veya benzeri belgenin fotokopisine ihtiyaç duyulmaktadır. Bu konuda herhangi bir mevzuat birliği olmadığından; işletmeciler arasında faturalı veya ön ödemeli kullanımlara göre bu belgeler değişkenlik gösterebilmektedir.[386]

Kurumsal abonelik tesisi sırasında ise kurumsal aboneliğin yetkilisi olacak kişi, şirketi temsil ve ilzama yetkili kişi olabileceği gibi bu kişi tarafından verilmiş ve şirket adına abonelik tesis etmeye vekaletname suretiyle yetkili kılınmış vekil de

---

[385] Sınırlı ehliyetsizler, ayırt etme gücüne sahip olan küçük veya kısıtlılar olup; sınırlı ehliyetsizlerde kural ehliyetsiz olma, istisna ise ehliyetli olmadır. Bunlar karşılıksız kazanmalar, kişiye sıkı sıkıya bağlı olan haklar ve meydana gelen haksız fiil karşısında sorumlulukları bakımından tam fiil ehliyetine sahiptir. Ancak bir sınırlı ehliyetsizin geçerlilik taşıyacak bir işlem tesis edebilmesi için, yasal temsilcisi olan kişinin söz konusu işleme herhangi bir şekilde katılması gerekmektedir. (Mustafa Dural, Tufan Öğüz, *Türk Özel Hukuku Cilt II Kişiler Hukuku*, (İstanbul: Filiz Kitabevi, 2012), 84-85.)

[386] Turkcell İletişim Hizmetleri A.Ş., Yaşım 18'den Küçük, Nasıl Hat Alabilirim?, https://www.turkcell.com.tr/yardim/turkcellli-olmak/turkcellli-olmak/yasim-18den-kucuk-nasil-hat-alabilirim#:~:text=Turkcell%27li%20Olmak&text=Yeni%20hat%20al%C4%B1rken%20gereken%20t%C3%BCm,anne%20veya%20baban%C4%B1z%C4%B1n%20kimli%C4%9Fi%20gerekmektedir. Erişim Tarihi: 3 Eylül 2022.

olabilmektedir. Bunun gibi durumlarda abonelik tesisi için şirket yetkilisi veya vekilinden abonelik sözleşmesinin yanı sıra imza sirküleri, vekaletname, varsa imza beyannamesi, yetkilinin kimlik veya kimlik yerine geçen diğer belgelerden birinin fotokopisi ve şirketin vergi levhası, KDV tahakkuk fişi veya şirketin faaliyet belgesi istenmektedir.[387] Kamu kurumu adına abonelik tesisi sırasında ise yetki belgesi, atama kararı, görevlendirme yazısı veya kişinin kamu kurumu adına işlem yapmaya yetkili olduğunu gösteren yetki yazısı istenmektedir. Dernek, vakıf veya sendikalar için ise sayılan belgelerin yerine yetki belgesi veya karar defterinin noter tarafından tasdik edilmiş ilk sayfası ve ilgili elektronik haberleşme hizmetine dair kişinin abonelik açmaya yetkili kılındığını gösteren karar sayfasının işletmeciye sunulması gerekmektedir.[388]

Her ne kadar yukarıda sayılan belgeler vasıtasıyla şirket yetkililerine ilişkin kişisel veriler işletmeciler tarafından işlenmek zorunda kalınsa da haberleşmeye ilişkin bir aboneliğin yetkisiz kişilerce tesis edilmesi veya kullanılması hali, o şirket veya dernek gibi kuruluşlar adına haberleşmenin gerçekleştirildiği anlamına geleceğinden; söz konusu belgelerle birlikte yetkili kişinin doğrulanması elektronik haberleşme sektöründeki abonelikler için önemli bir aşama olarak kabul edilmektedir.

6.3. ABONELİK YAPMA YÖNTEMİNE GÖRE DEĞİŞKENLİK GÖSTEREN KİŞİSEL VERİLER

EHK'nın 50/1 maddesinde yer alan, abonelik sözleşmesinin yazılı ya da elektronik ortamda tesis edilebileceğine ilişkin hüküm ve Tüketici Hakları Yönetmeliği'nin 7/1 maddesindeki sözleşmenin yazılı şekilde ya da Kimlik Doğrulama Yönetmeliği çerçevesinde kimlik teyidi yapmak suretiyle elektronik ortamda oluşturulabileceğine dair hükümlerden anlaşılacağı üzere; elektronik haberleşme sektöründe abonelik sözleşmelerinin kurulumu şekil şartına bağlanmıştır.

EHK'nın 50/1 maddesinin devamında belirtildiği üzere; ilgili kanun maddesi ile elektronik ortamda kurulacak abonelik sözleşmelerine dair ayrıntıların yer alacağı usul ve esasların Kurum tarafından ayrıca düzenlenmesinin önü açılmış; bu hüküm

[387] Turkcell İletişim Hizmetleri A.Ş., "Nasıl Kurumsal Hat Alabilirim?", https://m.turkcell.com.tr/kurumsal/yardim/turkcelli-olmak/abonelik-islemleri/nasil-kurumsal-hat-alabilirim , Erişim Tarihi: 3 Eylül 2022.

[388] Mobildev, "SMS aktivasyon için gerekli evraklar nelerdir? Turkcell - Vodafone Ek evraklar," https://www.mobildev.com/support-knowledge-detail.asp?sid=66&id=1&sssid=41 , Erişim Tarihi: 3 Eylül 2022.

doğrultusunda da BTK tarafından hazırlanan Kimlik Doğrulama Yönetmeliği yürürlüğe girmiştir.

İlgili Yönetmeliğin 1. maddesinde belirtildiği üzere; abonelik sözleşmesi, numaranın başka bir işletmeciye taşınması, nitelikli elektronik sertifika, kayıtlı elektronik posta ve SIM kart değişikliği için abone tarafından başvurulması halinde işletmecinin ilgili işlemleri elektronik ortamda gerçekleştirmesi durumunda başvuran kişinin kimlik doğrulaması, söz konusu Yönetmelik hükümleri doğrultusunda gerçekleştirilecektir.

Aynı Yönetmeliğin 5. maddesinde *"Kimlik doğrulamaya ilişkin genel hususlar"* başlığı altında, elektronik haberleşme sektöründe ilgili Yönetmeliğin 1. maddesinde yer alan, işlemlerin tesisi sırasında abonenin kimliğinin doğrulanması için hangi yöntemlerin kullanılabileceğinden bahsedilmektedir. Yeni abonelik tesisi, yüz yüze ıslak imzalı aboneliğin yanı sıra ilgili hüküm doğrultusunda; elektronik ortamda yüz yüze, e-Devlet kapısı üzerinden, yapay zeka ya da işletmecinin yetkili kıldığı personel tarafından görüntülü şekilde doğrulama ve Türkiye Cumhuriyeti Kimlik Kartı'yla beraber PAdES oluşturması yoluyla gerçekleştirilebilmektedir.

6.3.1. Yüz Yüze Islak İmzalı Abonelik Tesisi Sırasında Alınan Kişisel Veriler

Sözleşmenin kuruluşu bakımından temel nitelikte olan ve Kimlik Doğrulama Yönetmeliği[389] yayımlanmadan önce de var olan abonelik türü, yüz yüze aboneliktir. Yüz yüze abonelikte, işletmecinin hizmetlerinden faydalanmak isteyen kişi ile işletmecinin sözleşme yapma yetkisine sahip çalışanı veya bayisiyle bir araya geldikten sonra, abone bilgileri doldurularak sözleşmenin tamamlanması ve taraflarca imzalanmasının ardından sözleşme kurulmuş sayılır.

Tüketici Hakları Yönetmeliği'nde 18 Ocak 2022 tarihinde yapılan değişiklik ile uzaktan aboneliğe imkan tanınmasından önce ilgili Yönetmeliğin 7/1 maddesi uyarınca, elektronik haberleşme sektöründe abonelik sözleşmelerinin usulüne uygun kurulmuş sayılabilmesi için temel şart ıslak imza veya 5070 sayılı Elektronik İmza Kanunu'nun[390]

---

[389] BTK, 22.12.2021 tarih ve 2021/DK-BTD/403 sayılı Kurul Kararıyla, (https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorunde-basvuru-sahibinin-kimliginin-dogrulanma-sureci-hakkinda-yonetmelikte-degisiklik-yapilmasina-dair-yonetmelik/403-2021-web.pdf . Erişim Tarihi: 4 Eylül 2022.) ilgili Yönetmeliğin 31.12.2021 olan yürürlük tarihi, 01.03.2022 olarak değiştirilmesi için karar alınmış olup; ilgili Değişiklik Yönetmelik, 31.12.2021 tarih ve 31706 (6. Mükerrer) sayılı R.G.'de yayımlanmıştır.

[390] R.G. 23.01.2004, S. 25355.

5. maddesinde[391] belirtildiği üzere elektronik imza ile kurulmasıydı. Zira, BTK'nın birçok kararında da belirtildiği üzere, yüz yüze ıslak imzalı yapılan aboneliklerde abonelik sözleşmesinin ıslak imzalı aslının bulunmaması gerekçesiyle işletmecilere idari yaptırım uygulamıştır.[392]

Yüz yüze abonelik, tarafların bir araya gelmesini gerektirmektedir. Gelişen teknoloji ve bu teknolojinin de en fazla elektronik haberleşme sektöründe kendini gösterdiği düşünüldüğünde; teknolojinin sağladığı avantajlardan yararlanılarak; kişiler birbirine uzak olsa da bir sözleşmenin kurulabilmesine imkan sağlanması kaçınılmaz hale gelmiştir. Bu sebeple de Kimlik Doğrulama Yönetmeliği yayımlanarak kişinin kimliğinin uzaktan doğrulanmasına olanak sağlayan yöntemlere açıklık getirilmiş olup; uzaktan abonelik yapılmasının önü açılmıştır.

Elektronik haberleşme sektöründe abonelik aşamasındaki en önemli husus, abone olmak isteyen kişinin doğrulanması aşamasıdır. İşletmeciye abonelik için sunulan kimliğin gerçekten kimlik sahibi tarafından sunulup sunulmadığının tespiti gerekmektedir. Bu kimlik doğrulaması konusunda yükümlülük işletmecide olup; işletmeci adına işlemi yürüten personel veya işletmecinin bayisi tarafından yüz yüze abonelikte yapılabilecek tek kontrol yönteminin ise fiziki olarak göz ile yapılabilen kontrol olduğu açıktır.

Yüz yüze abonelikte yalnızca göz ile kontrol yapılabildiği düşünüldüğünde; sunulan kimliğin sahte kimlik olabilme ihtimali işlemi gerçekleştiren tarafından çoğunlukla tespit edilememekte ya da fotoğraftaki kişi farklı bile olsa personel veya bayinin ihmalinden kaynaklı olarak; kimliği sunan kişinin aslında kimliğin sahibi olmadığını fark edebilmek güçleşmektedir. İşletmeciler, yüz yüze abonelik yapılırken yaşanabilecek olan söz konusu olumsuz sonuçları olabilecek durumu mümkün olduğunca ortadan kaldırabilmek için kimlik dışında başka bir belge vasıtasıyla kişiyi doğrulayabilmek amacıyla aboneden adına kayıtlı fatura talebinde bulunabilmektedir.

---

[391] 5070 sayılı Kanun'un 5/1 maddesinde, güvenli elektronik imzanın kişinin eliyle attığı imza ile aynı hukuki sonuçları meydana getireceği hükmolunmuştur.

[392] BTK, 19.01.2016 tarih ve 2016/DK-SDD/30 sayılı Kurul Kararında; Tüketici Hakları Yönetmeliği'nin 15/6 maddesine aykırı şekilde; sözleşmenin aslının tespitler sırasında görülemediği, yine aynı maddeye göre yetkili kişinin temsile yetkili olduğunu gösteren belge ile imza sirkülerinin abonelik sözleşmesiyle beraber saklanması gerekmesine rağmen saklanmadığı ve mevzuata uygun abonelik sözleşmesi olmadan abonelere hizmet sunulması sebebiyle işletmeci hakkında, İdari Yaptırımlar Yönetmeliği'nin 12/1-(a) maddesinin 8. alt bendi uyarınca idari para cezası uygulanmasına karar verilmiştir. https://www.btk.gov.tr/uploads/boarddecisions/aloses-numara-tasima-sistemi-baglantisi-ve-abonelik-sozlesmesi-sikayeti-plandisi-inceleme.pdf . Erişim Tarihi: 4 Eylül 2022.

Diğer bir deyişle, amaç aboneliği gerçekleştiren kişinin kimliğinin doğrulanması iken; abonelik tesisi için aslında gerekli olmayan birtakım belgeler aboneden talep edilmek zorunda kalınmaktadır.

Yüz yüze ıslak imzalı abonelik tesisi esnasında kimlik kontrolü yükümlülüğünün personel veya bayi gibi kişilerin inisiyatifine bırakılmasının yanı sıra abonelik sözleşmesinin kuruluşu aşamasında görev alan çalışan veya bayiye ait imzalar da işlenen bir diğer kişisel veri olması sebebiyle bu verilerin de korunması durumu işletmeci açısından başka bir yükümlülük teşkil etmektedir.

Yüz yüze abonelikteki kimlik doğrulamaya ilişkin bahsi geçen problemlerin varlığına rağmen; özellikle teknolojiye uzak olmayı seçen abonelik tesisi talebinde bulunan kişiler bu yöntemi tercih etmeye devam etmektedir.

6.3.2. Kimlik Doğrulamanın Elektronik Ortamda Yapıldığı Abonelik Sözleşmelerinde Alınan Kişisel Veriler

Tüketici Hakları Yönetmeliği'nde 18 Ocak 2022 tarihinde yapılan değişiklikten önce, her ne kadar güvenli elektronik imza ile yan yana olmayan işletmeci ve abone arasında uzaktan abonelik tesis edilebiliyor olsa da tüketicilerin hepsinin e-imzaya sahip olmaması sebebiyle elektronik haberleşme hizmeti almak isteyenlerin, abonelik sözleşmesi tesisi için bu hizmetleri sunan ve BTK tarafından yetkilendirilmiş olan işletmecilerle fiziki olarak bir araya gelmesi gerekmekteydi. Bu durum özellikle küçük ölçekli işletmecilerin abonelere erişimini kısıtlamaktaydı. Geniş bayi ağı olmayan işletmeciler, yerel bazda hizmet verebilmekteydi. Bu durum, küçük ve orta ölçekli işletmecilerin büyük ölçekli işletmecilere nazaran pazar paylarının oldukça düşük olmasına sebebiyet vermekteyken; elektronik haberleşme sektöründeki paydaşlar arasında etkin rekabetin oluşmasına engel olan bir durum olarak görünmekteydi.

Ayrıca kimlik doğrulamanın göz ile kontrol sağlanarak gerçekleştirilmesi, sahte aboneliklerin ortaya çıkmasına ortam oluşturmaktaydı. Kimliğin gerçek sahibi olmayan kişiler tarafından sunulduğunda yalnızca göz ile kontrolün gerçeği ortaya çıkaran güvenli bir kontrol yöntemi olmaması sebebiyle işletmecinin personeli tarafından gözle kontrol edilse bile sahte kimliğin anlaşılamaması sebebiyle yeterli kontrollerin yapılamamasıyla sahte aboneliklerin gerçekleştirilmesinin önüne geçilememekteydi. Bununla birlikte, işletmecilerin personellerini çalışmaya teşvik etmesi amacıyla başarılı işlem başına prim vermesi veya hedeflenen kotanın sağlanması zorunluluğu sebepleriyle personellerin

işlemi gerçekleştiren kişinin kimliğin asıl sahibi olup olmadığını sorgulamadan işlemi tamamlamasına neden olabilmekteydi.

Abonelik kurulurken istenen belgeler arasında olan kişi adına kayıtlı fatura da herhangi bir faturanın elektronik ortamda oynanmasıyla istenilen kişi veya adres üzerinde gösterilebileceği için bu da aboneliğin gerçek kişi tarafından yapılmasını teşvik edici bir uygulama değildir. Kimliğin ve abonelik sözleşmesinin sayfalarının tek tek taranması, kağıt üzerinde gerçekleştirilmesi gereken iş yükünün fazla olması ve kağıt ortamında bilgi güvenliğinin sağlanmasında zorluk çekilmesi gibi sebeplerle kimlik doğrulama ve aboneliğin kurulumunun elektronik ortamda gerçekleştirilmesinin önemi gün geçtikçe artmıştır.

Tüketici Hakları Yönetmeliği'nin 7/1 maddesinde yapılan değişiklik ile; abonelik sözleşmelerinin elle veya güvenli elektronik imza ile imzalanması suretiyle kurulması kuralına alternatif olarak Kimlik Doğrulama Yönetmeliği vasıtasıyla başvuranın kimliğinin doğrulanarak sözleşmenin kurulabilmesi imkanı getirilmiştir. Söz konusu değişiklik doğrultusunda, el yordamıyla atılan ve e-imza ile imzalanan sözleşmeler yerine yazılı veya elektronik ortamda kurulan sözleşmeler şeklinde farklı bir ayrıma gidildiği görülmektedir.

Bu çerçevede, Kimlik Doğrulama Yönetmeliği'nin 5/1 maddesinde yer verildiği üzere, elektronik haberleşme sektöründe faaliyet gösteren işletmeci ile abone arasında akdedilecek olan abonelik sözleşmeleri; yüz yüze, mobil uygulama veya internet sitesi üzerinden sağlanan arayüz aracılığıyla elektronik ortamda kurulabilmektedir. Aynı maddenin 2. fıkrasında ise elektronik ortamda sözleşmenin kurulması esnasında elzem olan kimlik doğrulama işleminin hangi kanallar aracılığıyla gerçekleştirilebileceğine yer verilmiş olup; ilgili işlemlerin e-Devlet üzerinden, Türkiye Cumhuriyeti Kimlik Kartı varsa PAdES oluşturma yöntemiyle, yakın alan iletişimi (Near Field Communication-NFC) özelliğine sahip belgenin ICAO 9303 standardı kapsamında yapay zeka ya da yetkili kişi tarafından görüntülü doğrulanması ve aboneyle yüz yüze olunması halinde ise kimlik belgesinin yalnızca yapılan işleme özgülenmesi suretiyle video kaydının alınması suretiyle gerçekleştirilebileceğinden bahsedilmiştir.

6.3.2.1. E-Devlet Üzerinden Başvuru Sahibinin Kimliğinin Doğrulanma Sürecinde Alınan Kişisel Veriler

Kimlik Doğrulama Yönetmeliği'nin 6. maddesinde, e-Devlet üzerinden abonelik kurulacağı zaman kişinin kimliğinin ne şekilde doğrulanacağına dair ayrıntılara yer verilmiştir. Buna göre, abonelik tesis etmek isteyen kişinin öncelikle, Türkiye Cumhuriyeti Kimlik Kartı'nın kart okuyucuyla doğrulanması suretiyle, internet bankacılığı ve mobil bankacılık uygulamaları vasıtasıyla veya güvenli elektronik imza kullanarak e-Devlet'e giriş yapması gerekmektedir.

Esasen e-Devlet'e mobil imza veya kişiye özgülenen e-Devlet şifresiyle de giriş yapılabilse de ilgili hüküm incelendiğinde, abonelik tesisi işlemi için kimlik doğrulama aşamasında bu iki seçeneğin kullanılamadığı görülmektedir. Elektronik ortamda abonelik tesis edilebilmesinden önce, yüz yüze abonelik sürecinde abonelik tesisi gibi çeşitli işlemler için işletmeciler tarafından abonenin kimliğinin doğrulanabilmesi, belgeyi sunan kişiyle belgenin üzerinde yazan ismin aynı kişi olduğunun teyidi amacıyla adına kayıtlı faturanın kişinin gerçekliğini gösterme konusunda güvenilir bir evrak olarak görülmemesi sebebiyle bazı işletmeciler kişinin yalnızca kendisinde bulunduğu düşünülen şifre ile giriş yapılan e-Devlet üzerinden alabildiği Yerleşim Yeri ve Diğer Adres Belgesi'ni kişiden talep edilebilmekteydi.[393]

İşletmeciler tarafından yalnızca kişinin erişebildiği belgelerin talep edilmesiyle gerçek kişiyle muhatap olabilmek amaçlanmış olmasına rağmen suç işleme saikiyle hareket eden kimseler bu faaliyetleri sırasında kullanacakları telefon numarası veya internet aboneliklerinin kendi adına olmasını istememeleri sebebiyle, genellikle maddi menfaat sağlama vaadiyle kişilerin kimliklerini abonelik tesisi için kullanmak amacıyla e-Devlet şifrelerini almaktadır. Şifreleri alınan kişiler, söz konusu aboneliğin nasıl sonuçlar doğurabileceği bilincinde olmadan; e-Devlet şifresini başkalarıyla paylaşarak yerleşim yeri belgesi gibi belgelerin kendisi dışındaki şahıslar tarafından alınmasına ve kendileri adına abonelik başlatılmasına rıza göstermektedir.

Yüz yüze şekilde yapılan kimlik doğrulama, yalnızca göz ile kontrol yapılabildiğinden; hata yapılmasına müsait bir kontrol işlemi olması sebebiyle, hukuka aykırı şekilde abonelik tesis etmek isteyen kişi, sahte kimlikle birlikte başkasına ait

[393] Netgsm, Netgsm Aboneliği İçin Gerekli Belgeler Nelerdir?, https://bilgibankasi.netgsm.com.tr/bilgi-bankasi/netgsm-aboneligi-icin-gerekli-belgeler-nelerdir/ , Erişim Tarihi: 5 Eylül 2022.

şifreyle birlikte e-Devlet üzerinden aldığı belgeyi işletmeciye sunmaktadır. E-Devlet şifresinin kişinin yalnızca kendisinde olması gerektiği kabulünden kanaatle; işletmecinin işlem yapmaya yetkili personeli tarafından söz konusu belge doğrulamaya tabi tutulduğunda; belgenin gerçek olduğu görüldüğünde, haklı olarak abonelik tesis etmek isteyen kişinin gerçekten kimlikte adı yazan kişi olduğu düşünülmektedir. Söz konusu abonelik vasıtasıyla suç işlendiği ortaya çıktığında ise kimliğin gerçek sahibi tarafından aboneliği kendilerinin başlatmadıkları iddia edilmektedir. Bu durumda, aslında e-Devlet üzerinden alınan belgenin kimlikte adı yazan kişi tarafından değil de başkası tarafından sunulduğu anlaşılamadığından; işletmeciler hakkında EHK'nın 56/4 maddesinde belirtilen kişinin bilgisi dışında abonelik tesis edilemeyeceği kuralından hareketle aynı Kanun'un 63/10 maddesi uyarınca adli para cezası uygulanmaktadır.

Bahsi geçen durumların varlığı sebebiyle, e-Devlet şifresinin kişiler tarafından banka şifresi gibi dikkatle korunamadığı düşüncesinden hareketle, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin ilgili Yönetmelik yayımlanmasından önce Kurum'a yapmış oldukları talepler doğrultusunda bu şifre ile yeni abonelik tesisine imkan verilmek istenmediği düşünülmektedir.

Mobil imza ile e-Devlet'e girilerek abonelik kurulmasına Kimlik Doğrulama Yönetmeliği'nde yer verilmemesinin sebebi ise mobil imzanın kişinin SIM kartına tanımlanabilen bir özellik olması sebebiyle kişinin telefonunun çalınması halinde rızası olmadan kendi adına abonelik başlatılması hususunun risk teşkil etmesi ya da mobil imzanın e-imza kadar yaygın kullanımının olmaması gösterilebilir.

E-Devlet üzerinden yapılan kimlik doğrulamaya dair ayrıntılı bilgiler Kimlik Doğrulama Yönetmeliği'nin 6. maddesinin 2, 3 ve 4. fıkralarında yer almaktadır. İlgili maddenin 1. fıkrasında bahsi geçen yöntemlerden biri ile e-Devlet'e giren abone veya abone adayının başvuruda bulunduğu işletmeci tarafından yapılacak olan işleme ilişkin ayrıntılı bilgileri ve abone adayına ait kişisel ve iletişim bilgileri gösterilerek söz konusu bilgileri onaylaması istenilmektedir. Ardından, doğrulama işleminin gerçekleştiği bilgisi, ilgili işletmeciye iletilir. Söz konusu bilgilerde farklılık varsa, e-Devlet üzerinde kişiye ait olarak görünen bilgiler esas alınmaktadır. İlgili kimlik doğrulama işleminin gerçekleştirilebilmesi, işletmecinin e-Devlet'e Kurum aracılığıyla entegrasyonu ile veya herhangi bir aracı olmadan doğrudan yapılabilmektedir.

Elektronik haberleşme sektörüne ilişkin sunulan hizmetler kapsamında işletmeciye başvurarak başlattığı başvuru sürecindeki kimlik doğrulama aşamasını e-Devlet üzerinden tamamlamak isteyen kişi, Kimlik Doğrulama Yönetmeliği'nin 6/1 maddesinde yer alan yöntemlerden biri ile e-Devlet'e giriş yaptıktan sonra, e-Devlet üzerinden işletmecinin BTK'nın sistemine entegre olabildiği internet sayfasına girebilmektedir.[394]

İlgili internet sayfası incelendiğinde söz konusu işlemlerin tamamlanabildiği işletmeciler listesinin halihazırda BTK tarafından yetkilendirilen işletmecilerden[395] çok azının entegrasyon yaptığı görülmektedir. Bunun en temel sebebi, abonelik başlatmak isteyen kişinin işletmeciye başvurduktan sonra yalnızca kimlik doğrulama aşaması için e-Devlet'e girmesi ve aboneliğin kalan aşamaları için işletmeciyle tekrar iletişime geçmesi durumunun yeni abonelik başlatma sürecini operasyonel anlamda böldüğü ve uzattığı düşüncesidir.

Yeni abonelik başlatmak isteyen kişinin bu doğrulama sürecinde başka bir ortama yönlendirilmesi, süreci bölerek uzattığından abone adayının işletmeciden uzaklaşarak abone olma talebinin sona ermesine neden olabilmektedir. Bu sebeple işletmeciler bu seçeneğin yerine abone adaylarını yapay zeka ile aboneliğe yönlendirerek tüm doğrulama ve imza süreçlerini tek bir ekran üzerinden yürütmeyi tercih etmektedirler. Buna karşılık, bayi ağı geniş olmayan, henüz sistemlerine yapay zeka ile aboneliği sunmamış olan veya abonelerine kimlik doğrulama seçeneklerinin hepsini sunabilmek isteyen işletmeciler ise doğru abonelik tesisi amacıyla sunulan bu e-Devlet üzerinden kimlik doğrulama seçeneğini kullanmak isteyebilmektedir.

Söz konusu entegrasyonun sağlanabilmesi için diğer seçenek, e-Devlet'in sağlayıcısı olan Türksat A.Ş. ile işletmeci arasında yapılması gereken bir sözleşme olmasıdır. Bu entegrasyonu sağlayan işletmecilerin işlemlerini yürütülebilmesi için Türksat tarafından ayrı bir sayfa sağlanmaktadır. İşletmecilerin kendi sistemlerini ilgili yapıya uyarlamaları gerekmekte olup; henüz her işletmeci bu entegrasyonu

---

[394] E-Devlet, e-Kayıt Başvurusu Onay İşlemleri, https://www.turkiye.gov.tr/btk-e-kayit-basvurusu-onay-islemleri-gercek-kisi , Erişim Tarihi: 10 Eylül 2022.

[395] BTK tarafından yetkilendirilmiş işletmeciler listesi için Bkz., https://yetkilendirme.btk.gov.tr/Yetkilendirme/isletmeci-arama.xhtml;jsessionid=s-ongxpEOACSniG9oFAksr38pppER6EQEq8U41f7.be1 , Erişim Tarihi: 10 Eylül 2022.

sağlamamıştır. Bu nedenle ilgili yapı üzerinden tüm elektronik haberleşme sektörü işletmecilerinden yeni abonelik başlatılabilmesi şimdilik mümkün değildir.[396]

Herhangi bir şekilde söz konusu entegrasyonunu sağlamış olan işletmecilerin hizmetlerine ilişkin yapılacak olan abonelik işlemlerine ilişkin kimlik doğrulama işlemleri ise e-Kayıt sayfası üzerinden gerçekleştirilebilmektedir. Örneğin abone veya abone adayı, kimliğini doğrulayarak abonelik sözleşmesi, SIM değişikliği gibi çeşitli başvurularını ilgili sistem üzerinden onaylayabilmekte ve işlemlerini tamamlayabilmektedir. Entegrasyonu bulunmayan bazı işletmeciler ise yalnızca e-Devlet üzerinden kimliğin doğrulanmasını sağlamakta; fakat abonelik sözleşmesinin imzalanması aşamasını gerçekleştirememektedir.

Her ne kadar ilgili sayfadaki bilgilendirme metninde numara taşıma başvurularının da bu sistem üzerinden onaylanarak tamamlanabileceği belirtilmiş olsa da Kimlik Doğrulama Yönetmeliği uyarınca elektronik ortamda kimliğin doğrulanması halinde doğrulama işlemine ait elde edilen bilgilerin, Numara Taşınabilirliği Yönetmeliği[397] hükümleri doğrultusunda numarasını başka bir işletmeciye taşımak isteyen abonenin taşıma talebini içeren evraka ait bilgilerin ve görüntü kayıtlarının verici işletmeci tarafından alındıktan sonra numaranın taşınacağı alıcı işletmeciye tüm bu verilerin gönderilmesi söz konusu olduğunda; numaranın taşınacağı işletmecinin aslında ihtiyacının olmadığı fakat sadece taşıma işlemi başlatan işletmeci numarasını karşı işletmeciye taşıma talebinde bulunan abonesinin kimliğini doğrulamak üzere almış olduğu çok sayıda kişisel veriyi, kendisinin ihtiyacı olmadığı için haklı olarak saklama yükümlülüğü altına girmek istememektedir. Ayrıca NTS de böyle yüklü miktardaki kişisel veriyi işletmeciler arası taşıma yükümlülüğüne sahip olmak istememektedir. Bu sebeple şu anki uygulama kapsamında henüz numara taşıma işlemleri için kimlik doğrulama süreci e-Devlet üzerinden gerçekleştirilememektedir.

Ayrıca söz konusu e-Kayıt sisteminde, işletmeciye başvuruda bulunan kişilere, e-Devlet üzerinden kimliklerini doğrulama imkanı sunulduktan sonra kişinin doğrulama işleminin gerçekleştiği bilgisinin işletmeciye iletilmesi sistemi kurulmuş olsa da e-Devlet üzerinden gerçekleştirilen doğrulama işlemine yeni bir işlem numarası verilmediğinden

[396] Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş., "E-devlet'te Abonelik Sözleşme Sürecini İşleten İlk Telekom Operatörü Türksat Kablo Oldu," https://www.turksat.com.tr/tr/haberler/e-devlette-abonelik-sozlesme-surecini-isleten-ilk-telekom-operatoru-turksat-kablo-oldu , Erişim Tarihi: 10 Eylül 2022.
[397] R.G. 02.07.2009, S.27276.

işletmecinin bu doğrulamayı ispat yükümlülüğünü gereği gibi yerine getirememesi durumu ortaya çıkmaktadır. Olması gereken ise nasıl işletmeci başvuruya ilişkin bir işlem numarasını aboneye veriyor ve abone yalnızca e-Devlet'te o işlem numarası vasıtasıyla kimlik doğrulama işlemini gerçekleştiriyor ve söz konusu işlem ile doğrulama faaliyeti eşleştiriliyorsa; aynı şekilde ilgili işlemin tamamlandığına ilişkin de işletmeciye e-Devlet tarafından bir işlem numarası gönderilmelidir.

Entegrasyon bulunmayan işletmecilerden yeni hat almak isteyen abone adayları, e-Devlet üzerinden "Yeni Mobil Hat Başvuru İşlemleri" sayfasından abonelik işlemlerini başlatabilmektedir. Bu sayfada kişiye öncelikle, abonelik başlatmak istediği işletmecinin abonelik sözleşmesi sunularak onaylaması sağlandıktan sonra, kimlik bilgileri ve adresinin NVİ üzerinden alınarak abonelik sözleşmesinin kuruluşu için işletmeciye gönderileceği bilgisi verilmekte olup; bu konuda abone adayının açık rızası alınmaktadır. Söz konusu onayların verilmesinin ardından işletmeciye ait tüm tarifelerin listesi başvurana sunulmaktadır. Kendisine uygun tarifeyi seçen kişi, bir sonraki aşama olan "Numara Seçme" bölümüne geçiş yapmaktadır. Seçilen numaranın ardından kişinin kimlik ve iletişim bilgilerinin teyit edildiği bölüme geçilmektedir. Ardından abone olmak isteyen kişiden kimlik kartının fotoğrafının çekilerek sisteme yüklenmesi istenmektedir. Abonelik sözleşmelerinin başındaki abone bilgi formlarında abone tercihlerine ilişkin alınan onaylar, e-Devlet üzerinden başvuru yapılması halinde, "Opsiyonlar" başlığı altında alınmaktadır. Söz konusu tercihlerin yapılmasının ardından aboneliğe ilişkin ön izleme yapıldıktan sonra sonuç sayfasına geçilebilmektedir. Burada bahsi geçen yöntemle, yeni abonelik başvuruları tamamlanabilmektedir.[398]

E-Devlet entegrasyonu ile mobil hat başvurusunun yapılabilmesinin yanı sıra aboneler aboneliklerinin iptal edilmesi için fesih başvurusu yapabildikleri gibi Borç ve Alacak Bilgilerinin Sorgulanmasına İlişkin Usul ve Esaslar'ın[399] 4/3 maddesi uyarınca, abonelikleri hakkında borç ve alacak sorgulaması da yapabilmektedirler. İlgili borç

[398] TT Mobil İletişim Hizmetleri A.Ş., Yeni Mobil Hat Başvuru İşlemleri, https://www.turkiye.gov.tr/ttmobil-yeni-mobil-hat-basvuru-islemleri , Erişim Tarihi: 14 Eylül 2022.

[399] BTK'nın 22.09.2014 tarih ve 2014/DK-THD/466 sayılı Kurul Kararı'yla söz konusu usul ve esaslar onaylanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/borc-ve-alacak-bilgilerinin-sorgulanmasina-iliskin-usul-ve-esaslar.pdf . Erişim Tarihi: 14 Eylül 2022.

sorgulama sayfasına giriş için de e-Devlet üzerinden sunulan dört giriş seçeneğinden biri kullanılarak girilebildiği için güvenlik seviyesinin[400], seviye-2 olduğu düşünülmektedir.

Telefon veya internet aboneliği borcu sorgulama veya fesih başvurusu işlemleri için Kimlik Doğrulama Yönetmeliği'nin 6/1 maddesinde yer verilen dört seçenekten biri ile sisteme giriş yapılarak işlemler tamamlanabilmekteyken; ilgili hükmün aksine, söz konusu yöntem ile sisteme giriş yapılmak istendiğinde, yeni abonelik başvuru işlemleri için yalnızca e-imza ile e-Devlet'e giriş yapılmış olması şartı arandığı görülmektedir.

Yalnızca e-imza ile e-Devlet'e giriş yapılarak yeni hat başvuru sayfası üzerinden aboneliğin tüm aşamaları tamamlanabilmektedir. İnternet-mobil bankacılık üzerinden, TCKK ile veya e-imza ile e-Devlet'e giriş yapılarak e-Kayıt sayfası üzerinden ise yalnızca işletmeciye önceden yapılan başvurular doğrultusunda kimlik doğrulama aşaması sonlandırılabilmektedir. Yeni abonelik tesisi işleminin tamamının yapılabilmesi sürecinin, yalnızca kimlik doğrulama aşamalarının tamamlanabilmesine nazaran daha önemli ve sonuca ulaşan bir işlem olması sebebiyle; bu durum, e-Devlet üzerinden ilgili sayfalara girişteki güvenlik seviyelerinin farklı şekilde belirlenmesini anlamlı kılmaktadır. Yeni hat başvuru sayfasının yalnızca e-imza ile girişte kullanılabilmesi, ilgili sayfanın güvenlik seviyesinin seviye-3 ya da seviye-4 olduğunu; e-Kayıt sayfasının ise dört seçenekle birlikte girilebiliyor olması ise güvenlik seviyesinin seviye-2 olduğunu göstermektedir.

[400] İşletme içerisinde kullanılan sistemlere, yazılımlara ve veri tabanına saldırı riskine karşı, işletmeler ve kurumlar genellikle birden fazla güvenlik düzeyi oluşturmayı tercih etmektedir. Öncelikle yapılması gereken bir güvenlik stratejisi oluşturmaktır. Her seviye güvenliğin kendine göre ayrı ön koşulları bulunmaktadır. Seviye arttıkça işlemi gerçekleştirebilmek için ön koşul da artmakta ve zorlaşmaktadır. Güvenlik seviyeleri genellikle dört düzeyden oluşmaktadır. Seviye-1 güvenlik düzeyi, ulaşıldığında güvenlik tehlikesinin en az olduğu birim ve uygulamalar için belirlenmektedir. Seviye-2 güvenlik düzeyi, genellikle işletmelerin sistemlerine girişte önerilen düzeyde güvenlik olup; çok sayıda önemli saldırıyı önleyebilir düzeyde güvenliğin sağlandığı anlamına gelmektedir. Bu düzeyde, sistemlere çok faktörlü doğrulama ile giriş yapılabilmektedir. 3. Seviye güvenlik, güvenlik açıklarının tespiti ve kontrolünün sağlandığı, işletmeci tarafından ulaşılması hedeflenen seviyedir. 4. Seviye güvenlik, düzenlemeye tabi sektörlerde, değerli veriler işleyen işletmeciler tarafından kullanılmaktadır. Böyle bir güvenlik seviyesi, yüksek maliyetli kaynak yatırımı gerektirmektedir. (Searchinform, "Information Security Levels," searchinform.com, https://searchinform.com/challenges/information-security/information-security-basics/key-aspects-of-information-security/the-basic-principles-of-information-security/information-security-levels/ , Erişim Tarihi: 14 Eylül 2022; Aldridge, "IT Security Levels," aldridge.com, https://aldridge.com/it-security-levels/ , Erişim Tarihi: 14 Eylül 2022.)

6.3.2.2. ICAO 9303 Standardına Uygun Yakın Alan İletişimi Özelliği Olan Belge ile Abonelik Başlatılması Esnasında Başvuru Sahibinin Kimliğinin Doğrulanması Sürecinde Alınan Kişisel Veriler

Yakın alan iletişimi özelliği olan belge ile yapay zeka marifetiyle başvuranın kimliğinin doğrulanması aşamasının nasıl gerçekleştiği, Kimlik Doğrulama Yönetmeliği'nin 7. maddesinde açıklanmaktadır. İlgili maddenin 5. fıkrasına göre, yakın alan iletişimine (Near Field Communication-NFC) sahip kimliklerin yine bu özelliğe sahip cihazlara okutulması suretiyle başvuranın kimliğinde bulunan kimlik bilgileri ve fotoğrafı işletmeci tarafından alınmaktadır.

NFC, NFC etiketleri içeren iki cihaz-nesne arasında kısa menzilli radyo dalgaları kullanarak iletişim sağlayan kablosuz bir teknoloji olarak adlandırılmaktadır. Manyetik alan indüksiyonu kullanılarak; her iki cihaz birbirine temas ettiğinde veya birbirine çok yaklaştırıldığında NFC teknolojisini kullanarak cihazların birbirleriyle haberleşebilmeleri mümkün hale gelmektedir. Söz konusu iki cihaz veya nesnenin arasında bilgi alışverişinin gerçekleşebilmesi için yaklaşık dört santimetrelik kısa bir menzilin olması gerekmektedir. Önlenmesi gereken bazı güvenlik tehditleri içerdiğinden NFC teknolojisi, Bluetooth ve Wi-Fi teknolojisi gibi kısa bir mesafe üzerinden iki nesne arasında veri alışverişi yapılabilmesi için RFID (Radyo Frekansı Tanımlama)[401] kullanır. Hizmet sağlayıcı olan operatörler, e-Devlet hizmetleri, dijital imza hizmetleri gibi katma değerli hizmetlerinin kullanımında NFC teknolojisinden faydalanmaktadır.[402]

NFC özellikli akıllı cihazlarla sadece basit bir dokunuşla işlem yapılabilir ve bilgilere erişim sağlanabilir. NFC cihazları aynı anda veri gönderip alabildiği için bu teknolojinin gelecekte daha da yaygın hale geleceği söylenebilir.[403]

---

[401] Radyo frekansıyla tanımlama veya yaygın olarak bilinen adıyla RFID (Radio Frequency Identification), herhangi bir manuel müdahaleye gerek duymadan nesneleri, konumları ve kişileri bilgi işlem sistemlerine otomatik olarak tanımlama yeteneğini paylaşan çeşitli bilgi ve iletişim teknolojilerini ifade eden üst bir kavramdır. Etiket ve okuyucudan oluşabilmektedir. RFID okuyucu, çevresinde bir etiketin bulunduğuna ilişkin uyarı vermekte olup; bu uyarı, tespit ettiği etiketin okutulmasını istediği anlamına gelmektedir. Okutma işlemiyle alınan veriler, kaydedilir veya başka bir şekilde işlenir. Özellikle RFID'deki RF kısmı, bu yeteneğin bilgi işlem sistemi ile tanımlanan öğe arasındaki kablosuz iletişim tarafından etkinleştirildiğine işaret etmektedir. (George Roussos, *Networked RFID: Systems, Software and Services*, (London: Springer, 2008), 1.)

[402] Jain, "NFC: Advantages, Limits," 6.

[403] Vibhor Sharma, Preeti Gusain, Prashant Kumar, "Near Field Communication," *Proceedings of the Conference on Advances in Communication and Control Systems (CAC2S 2013)*, (Atlantis Press, 2013): 342-343, https://www.atlantis-press.com/proceedings/cac2s-13/6331 , Erişim Tarihi: 19 Eylül 2022.

NFC teknolojisi sayesinde, ICAO 9303 standardına[404] uygun olarak; kimlik kartı ile cihaz birbirine dokundurulmadan bilgilerin aktarımı gerçekleştirilebilmektedir. Bu şekilde bilgilerin alınması, ilgili Yönetmeliğin EK-1'inde pasif kimlik doğrulama olarak adlandırılmış olup; pasif doğrulama ile elde edilen verilerin aktif şekilde teyidi aşamasına geçilmektedir. Aktif kimlik doğrulamada ise başvuru sahibinden alınan kimlik bilgileri ve tarih, işlem türü, abone numarası gibi olan işlemin ayrıntılarına ilişkin verilerle, pasif doğrulamadan alınan veriler karşılaştırılır. Söz konusu verilerin yetkili makamlar olan, kimlik kartının doğrulandığı haller için İçişleri Bakanlığı'na ait kök sertifikasından, diğer ülkelere ait belgeler için ise ICAO açık anahtar rehberindeki o ülkeye ait kök sertifikası üzerinden düzenlendiğinin kontrolü sağlanır. NFC özelliği sayesinde, sözleşmeye ait temel bilgiler kimliğe gönderilmekte ve kimlikten alınan doğrulama da işletmeciye ulaştırılmaktadır. Bu doğrulamaya ilişkin bilgiler de oluşturulan pdf dosyasına eklenmektedir. İşletmecilerin bahsi geçen seçeneği kimlik doğrulama amacıyla kullanabilmesi için yapay zeka kullanılarak abonelik yapılacak olan mobil veya internet uygulamasının bu hususları sağlayacak şekilde geliştirilmesi gerekmektedir.[405]

Söz konusu kimlik bilgilerinin doğrulanmasının ardından işlemi gerçekleştiren kişinin kimlikteki kişi olduğunun teyidi amacıyla, kimlik kartındaki fotoğraf ile kişinin canlı görüntüsünün yapay zeka aracılığıyla doğrulanması aşamasına geçilmektedir.

Kimlik Doğrulama Yönetmeliği'nin 7/6 maddesinde belirtildiği üzere, söz konusu kimlik bilgi ve verilerin teyidi aşaması, görüntülü kimlik doğrulamasının bir parçasından ibaret olup; işletmeci, başvuranın kimliğinin belirlenen standartlara uygun olduğu, geçerlilik süresinin uygun olduğu, kimlik belgesinde yer alan MRZ (Machine Readable Zone) gibi alanlardaki fotoğraf ve diğer bilgilerinin uyumlu olduğunu NVİ üzerinden veya diğer standartlar doğrultusunda teyidini sağlar.

Pasaportların dijital olarak kopyalanması, kimlik ve bilgi doğrulama ve dolandırıcılık hadiselerinin tespit edilmesinde önemli rol oynamaktadır. Ad, doğum

---

[404] Havaalanlarında pasaport geçişlerinde pasaport teyidi için ve ulusal elektronik kimlik kartlarında bilgilerin kontrolünün sağlanması adına bir makine tarafından okunabilen belgelerin tümünde, gerçekten geçerli bir belge sahibi olunduğunu belirleyen ve bir okuyucu marifetiyle kimlik doğrulamasının sonuçlandırılmasını sağlayan bir protokol kullanılır. Uluslararası havacılık standartlarından sorumlu BM Kuruluşu ICAO, e-pasaportların uluslararası olarak okunabilmesi için, Uluslararası Sivil Havacılık Otoritesi tarafından tanımlanan, makine tarafından okunabilen seyahat belgeleri için standartlaştırılmış bir protokol uygulamaktadır. Bu standart, ICAO 9303 standardı olarak adlandırılmaktadır. (Ross Horne, Sjouke Mauw, "Discovering Epassport Vulnerabilities Using Bisimilarity," *Logical Methods in Computer Science* 17, no.2 (2021), 24. https://lmcs.episciences.org/7537/pdf . Erişim Tarihi: 19 Eylül 2022.)

[405] Kimlik Doğrulama Yönetmeliği, EK-1.

tarihi, son kullanma ve veriliş tarihi gibi bilgiler, pasaportlarda ve farklı makamlardan alınan vizelerde çeşitli şekillerde görüldüğünden, Makine Tarafından Okunabilir Bölge teknolojisi ile dijital kopyaların bulundurulması, fiziksel pasaportlar ve vizelerin aksine sahtecilik vakalarının gerçekleşmesine engel teşkil etmektedir. Bu sebeple pasaportlar ve vizelerde yer alan Makine Tarafından Okunabilir Bölge (Machine Readable Zone-MRZ) teknolojisi kritik öneme sahiptir. Bilgi doğrulama amacıyla, MRZ teknolojisi önemli bilgileri önceden belirlenmiş bir formatta bünyesinde bulundurur. MRZ teknolojisi, verilerin işlenmesini kolaylaştırmak amacıyla pek çok ülkenin pasaportlarında ve vizelerinde bulunmakta olup; genellikle kimlik bilgilerinin yer aldığı sayfada, pasaportun başlangıç bölümünde konumlandırılan MRZ metni, sayfanın alt kısmında 44 karakterlik iki satır halinde yer almaktadır. Pasaport yanında, pek çok ülkenin kimlik kartlarında da yer verilen alternatif MRZ biçimleri ile kimliklerin doğrulanması gerçekleştirilmektedir.[406]

Kimlik Doğrulama Yönetmeliği'nin 7/2 maddesinde yer verildiği üzere, görüntülü şekilde yapılan kimlik doğrulaması işleminin kesinti olmadan ve gerçek zamanlı olarak gerçekleştirilmesi gerekmektedir. Söz konusu görüntü kaydına, ilgili 7. maddenin 3. fıkrasında belirtildiği üzere, başvuran kişiden alınan telefon numarası veya e-posta adresine gönderilen tek kullanımlık şifre ya da link gönderilir. Buradaki amaç, beyan edilen iletişim bilgisinin aktif olarak kullanılıp kullanılmadığı hususunun doğrulanmasıdır.

Kimlik Doğrulama Yönetmeliği'nin 7/4 madde hükmü gereğince, ilgili teyit işleminin ardından, başvuranın video kaydının alınarak kimliğinin doğrulanabilmesi işlemi için görüntüsünün işlenmesi gerektiğinden; öncelikle işletmeci tarafından yapılacak olan işleme faaliyetine yönelik aydınlatma yükümlülüğü yerine getirilir ve bu bilgilendirmede de söz konusu doğrulama işleminin e-Devlet ya da yüz yüze kanallar vasıtasıyla da gerçekleştirilebileceği bilgisi başvurana iletilir. Yapılan bilgilendirme sonrasında KVKK uyarınca başvuranın rızası alınır. Bu konuda açık rıza vermeyen başvuran için işleme devam edilmez ve kişi başka bir kimlik doğrulama kanalına yönlendirilir.

[406] Yichuan Liu, Hailey James, Otkrist Gupta, Dan Raviv, "MRZ Code Extraction from Visa and Passport Documents Using Convolutional Neural Networks," *International Journal on Document Analysis and Recognition (IJDAR)*, (2020): 2-3. https://arxiv.org/pdf/2009.05489.pdf . Erişim Tarihi: 20 Eylül 2022.

Yapılan bilgilendirme, açık rıza alımı ve kimlik teyidi aşamalarının ardından Kimlik Doğrulama Yönetmeliği'nin 7/7 madde hükmü gereğince, kimlik belgesi üzerindeki fotoğraf ile başvuran kişinin aynı kişi olduğunun, kişinin işlemi o anda ve hazırda bulunarak yaptığının tespiti için başvuranın yüzünün tam olarak görünebileceği şekilde ve gözleri açık olarak şekilde kamera vasıtasıyla farklı açılardan yüzünün görüntüsü alınır. Alınan bu görüntüdeki yüz ile kimlik belgesindeki çipte kayıtlı ve belge üzerinde basılı olan yüzün aynı kişiye ait olduğunun teyidi iki şekilde yapılabilmektedir. Bunlardan ilki, Kimlik Doğrulama Yönetmeliği'nin EK-2'sinde yer alan yapay zeka ile doğrulamadır. Bu yöntem uyarınca; Ulusal Teknoloji ve Standartlar Enstitüsü Yüz Tanıma Üretici Testi 1:1 (National Institute of Standards and Technology Face Recognition Vendor Test 1:1 (NIST FRVT1:1)), Türk Standartları Enstitüsü veya Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute) standartlarında belirtilen teknik özelliklere uygun olduğunu gösteren raporu BTK'ya sunmaktadır. Böylece başvuran kişinin canlılık anlamında gerçek bir kişi olduğunun tespiti yapılmış olur.

Başvuran kişinin fotoğrafının doğrulanabildiği bir diğer yöntem ise yetkili marifetiyle tespit yapılmasıdır. Buna ilişkin ayrıntılara ise Kimlik Doğrulama Yönetmeliği'nin EK-3'ünde yer verilmiştir. Öncelikle sistemin yalnızca başvuran tarafından başlatılabileceği ve yetkili tarafından ise kontrol ve onaylama işlemlerinin yapılabileceği şekilde kurulması gerekmektedir. Yetkilinin yaptığı kontrol işlemi riskli bulunduysa, dosya ikinci bir onaya daha gönderilmektedir. Oluşturulan süreçlere ilişkin dokümanlar hazırlanır ve yapılan testlerdeki sonuçlar da raporlanmaktadır. İşletmeci, kendi adına doğrulamayı yapacak olan yetkili personelinin gerekli eğitimleri almasını ve eğitimlerin yılda en az bir kere yenilenmesini sağlayarak; erişim yetki alanlarını belirlemektedir. Kimlik doğrulama esnasında görüntülü olarak yapılacak görüşmede yetkili personelin soracağı sorular önceden işletmeci tarafından belirlenir ve görüşme esnasındaki ses ve görüntünün kesintiye yer vermeyecek şekilde düzgün olması sağlanmaktadır. Bu yöntem ile gerçekleştirilen doğrulama sonucunda şüphe bulunması halinde yapay zeka aracılığıyla doğrulama yöntemi denenmektedir. Bu durumda da kimlik belgesindeki fotoğraf ile görüşmenin gerçekleştirildiği kişi arasında uyumsuzluk çıkarsa, söz konusu doğrulama işlemi geçersiz kabul edilir.

Her iki yöntemde de yapılan görüntü kaydı sırasında, gerçekleştirilmek istenen işleme ilişkin bilgilerin bulunduğu ve Kimlik Doğrulama Yönetmeliği'nin 7/8 maddesinde belirtilen cümlenin başvuran tarafından okunması istenmektedir. Ayrıca ilgili maddenin 9. fıkrasında da belirtildiği üzere, işletmeci tarafından gerekli tedbirlerin alınmasına rağmen kimliğin gerçek sahibi tarafından kullanılmadığının anlaşılması halinde, ilgili başvuru süreci hemen sonlandırılmaktadır.

Aynı Yönetmeliğin 7/10 maddesinde de benzer şekilde, video kaydının yapıldığı esnada başvuranın bulunduğu ortamın ışığının az olması sebebiyle kimliğin doğrulanmasında güçlük çekiliyorsa veya başka bir belirsizlik olması durumunda yine sürece son verilmesi gerektiği belirtilmiştir. Tüm bu süreçte başvuru sahibinin doğru şekilde tespiti yükümlülüğü işletmecidedir. Video görüntüsünün net olmaması halinde abonenin kimliğinin tespitinde zorlanılacaktır. Çekilen video kaydı, abonelik sözleşmesinin ayrılmaz bir parçası niteliğinden olduğundan; bu görüntünün net olmaması, abonelik sözleşmesinin eksiksiz kurulmadığı anlamına gelecektir. Bu durum ise işletmecinin Tüketici Hakları Yönetmeliği'nin 7. maddesinde yer verilen abonelik sözleşmesini tam şekilde kurma yükümlülüğünü yerine getirmemesi sonucunu doğuracaktır.

Kimlik kartlarının çipli şekilde geliştirilerek basılması, yeni akıllı telefonların neredeyse hepsinde NFC özelliğinin bulunmasıyla birlikte; kişinin uzaktan doğrulanabilmesine ve dolayısıyla elektronik ortamda abonelik kurulabilmesine de imkan tanımasına sebep olmuştur.

6.3.2.3. TCKK ile Birlikte PAdES Oluşturarak Abonelik Başlatılması Esnasında Başvuru Sahibinin Kimliğinin Doğrulanma Sürecinde İşlenen Kişisel Veriler

Kimlik Doğrulama Yönetmeliği EK-4'te ayrıntılarına yer verilen Türkiye Cumhuriyeti Kimlik Kartı ile PAdES oluşturularak işlem sağlamak isteyen kişinin kimliğinin doğrulanmasında öncelikle PINpad[407] olarak adlandırılan kart okuyucu veya

[407] İşletmeler, hassas konumların güvenliğini sağlamak için ek güvenlik amacıyla bazen hem kart okuyucuları hem de PIN tuş takımlarını kullanmaktadır. Bu durumda, belirli lokasyona ulaşabilmek için anahtar kartı yanında genellikle sayısal bir kod olan kişisel kimlik numarası (PIN) tuşlanmalıdır. Anahtar kartlarından ve PIN bloklarından daha güçlü güvenlik isteyen kuruluşlar, biyometrik giriş kontrollerine yönelmektedir. Biyometrik kontroller, kişinin erişim sağlamaya yetkili olup olmadığını belirlemek adına bir kişinin vücudunun göz, el gibi belirli bir özelliğini ölçümleyerek yapılmaktadır. (Peter Gregory, *IT Disaster Recovery Planning For Dummies*, (Hoboken: Wiley Publishing, 2011), 134.) Bu doğrultuda,

TSE'nin yayımladığı TS 13678 standardına[408] sahip kart erişim cihazının (KEC)[409] bulunması gerekmektedir. Başvuruyu yapan kimse, kart okuyucuya kimlik kartını yerleştirdikten sonra kimliğin içerisinde bulunan sertifika, cihaz tarafından okunur ve kimliğin Türkiye Cumhuriyeti İçişleri Bakanlığı tarafından üretiminin sağlandığı, güvenli sertifika zincirinde[410] yer aldığı ve çevrimiçi sertifika durum protokolü[411] vasıtasıyla geçerli olduğunun kontrolü yapılarak; kimlik kartı doğrulama işlemi gerçekleştirilir. Gerçekleştirilmek istenen işleme ilişkin başvuran tarafından verilen bilgilerle oluşturulan pdf dosyasındaki bilgilerle söz konusu kontrole tabi tutulan kimliğin sertifikasında kayıtlı olan kimlik bilgilerinin birbiriyle uyumlu olup olmadığı kontrol edilmektedir. Ardından, söz konusu işleme özgü pdf dosyasının özet niteliğindeki temel bilgileri kimlik kartına gönderilmektedir. Buna karşılık kimlikten bu işleme özgü gelen şifre ise belgeye eklenmektedir. Ayrıca bu şifre zaman damgasıyla da damgalanmakta; işlemin ne zaman gerçekleştirilmek istendiğinin kaydı tutulmaktadır. Söz konusu belgenin başvuran tarafından bu şekilde imzalanmasının ardından işletmeci de kendi e-imzasıyla evrakı imzalamaktadır.

---

elektronik haberleşme sektöründeki işletmeciler de kişinin kimlik bilgilerini teyit edebilmek için PINpad özellikli cihazlar kullanarak, kişinin bilgilerine erişim sağlamaktadır. E-devlet kimlik kartı ile birlikte teslim edilen şifre, söz konusu PINpad cihazı ile doğrulanmaktadır.

[408] TS 13678, Elektronik Kimlik Doğrulama Sistemi Standardı, https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073086073081073066071066080088098075 , Erişim Tarihi: 21 Eylül 2022.

[409] Kart Erişim Cihazı (KEC), EKDS (Elektronik Kimlik Doğrulama Sistemi) ile ilgili olan elektronik ortamdaki uygulamalarda kimlik kartının yetkili kurum tarafından alındığının ve kartın hamiline ait olduğunun teyidi maksadıyla kullanılmaktadır. (https://bilgem.tubitak.gov.tr/tr/icerik/ekds-elektronik-kimlik-dogrulama-sistemi , Erişim Tarihi: 22 Eylül 2022.)

[410] Haberleşme için kullanılan internetin yaygınlaşması, internet güvenliğinin nasıl sağlanacağına ilişkin zihinlerde bazı sorular ortaya çıkarmıştır. SSL (Secure Sockets Layer- Güvenli Giriş Katmanı) ve TLS (Transport Layer Security- Taşıma Katmanı Güvenliği) olarak adlandırılan internet protokolleri, internet güvenliğinin temel taşları olup; bu teknolojilerin ayrılmaz bir parçası olarak da kullanılan sertifikalardır. Sertifika Otoriteleri (Certificate Authorities-CAs), alan adlarının iddia edilen kişi olduğunu doğrulayan sertifika vererek, bir kullanıcının Sertifika Otoritesi'ne güven duyması halinde, Sertifika Otoritesi'nce doğrulanmış alan adlarına da güven duymasına imkan tanınır. Sertifika Otoriteleri de sırasıyla diğer Sertifika Otoriteleri'nin doğrulanmış verileri ile bu verilerin karşılaştırılmasını sağlayarak sertifika zinciri ya da güven zinciri oluşturur. (Sebastian Klasson, Nina Lindström, "Longitudinal Analysis of the Certificate Validation Chains of Big Tech Company Domains," *Linköping University Department of Computer and Information Science Bachelor's Thesis*, 15 ECTS, (2021): iii. http://liu.diva-portal.org/smash/get/diva2:1586424/FULLTEXT01.pdf , Erişim Tarihi: 22 Eylül 2022.)

[411] OCSP (Online Certificate Status Protocol-Çevrimiçi Sertifika Durumu Protokolü) olarak adlandırılan bu protokol, geçerlilik ya da imzaya ilişkin sertifikaların doğrulanması için kullanılmakta olup; bu protokol ile sertifika durum bilgisi anında alınabilir. Söz konusu protokol, OCSP sunucusunca imzalanmış bir cevabın gönderilmesine neden olan bir sertifika durumuna ilişkin soru-cevap şeklinde çalışarak; sertifikanın iptal edildiği, iptal edilmediği ya da sertifikaya ilişkin bir bilginin bulunmadığı şeklinde bilgilendirme yapmaktadır. (Witold Mackow, Jerzy Pejas, "Unauthorized Servers for Online Certificates Status Verification," iç. *Information Processing and Security Systems*, ed. Khalid Saeed, Jerzy Pejas, (Newyork: Springer, 2005), 167-168.)

Cihazdan gelen şifrenin yapılmak istenen işleme özgü olarak ortaya çıkması, kimlik kartından cevap niteliğinde gelen bu özel nitelikteki şifrenin başka bir sözleşmeye veya evraka yüklenmek istenmesi halinde, kimlik bilgileri uyuşmayacağından kimlik doğrulaması aşamasının geçersiz olarak kabul edilmesine sebep olmaktadır. Kişinin kendisiyle ile yapılmak istenen işlem eşleştirilmiş olacağından; bu kişinin haberi olmadan işlemin gerçekleştirildiği iddiasında bulunulamayacağı gibi söz konusu şifre ile başkasına ait bir evrak da onaylanamayacaktır. Bu sayede, işletmeci tarafından hukuka aykırı şekilde kişinin haberi olmadan abonelik açılması gibi durumların da önüne geçilmiş olmaktadır.

Kimlik Doğrulama Yönetmeliği'nin EK-4'ünde belirtildiği üzere, bahsi geçen işlemler çerçevesinde, oluşturulan dosyaya başvuranın adı, soyadının ve kimlik numarasının yanı sıra kimlik kartının sertifika bilgileri, kökü ve alt kökü ve çevrimiçi sertifika durum protokolüne göre yapılan doğrulamaya ilişkin bilgiler dercedilmektedir. Söz konusu pdf dosyası ise daha sonra uzun dönemli saklamaya ilişkin oluşturulan PAdES-LTV formatına dönüştürülerek saklanmaktadır. PAdES-LTV, imzanın doğrulandığı bilgilerden oluşan ilk kısım ve doğrulama verilerinin yer aldığı bilgilerin uzun süreli şekilde saklanmasını sağlayan ikinci kısımdan oluşmaktadır. Uzun Dönem Doğrulama (Long Term Validity) olarak adlandırılan LTV, belgeyi uzun süreler boyunca saklamak isteyen tarafından bilgilerin bulunduğu pdf dosyasına eklenmektedir.[412]

6.3.2.4.Yüz Yüze Kanallarda Kimliğin Elektronik Ortamda Doğrulanması Suretiyle Gerçekleştirilen Abonelik Tesisi Sırasında İşlenen Kişisel Veriler

Yüz yüze abonelik vasıtasıyla gerçekleştirilen sahte abonelik sayılarındaki artış sebebiyle ve gelişen teknoloji ile birlikte uzaktan aboneliğe imkan sağlanması amacıyla yayımlanan Kimlik Doğrulama Yönetmeliği ile birlikte, abone olmak isteyen kişi ile işletmeci bir araya gelse bile kimlik doğrulaması aşamasında kolaylık sağlanması ve sunulan kimliğin sahte olma ihtimalinin ortadan kaldırılabilmesine olanak tanınıyor olması sebebiyle taraflar yüz yüze bile olsa abonelik sözleşmeleri elektronik ortamda kimlik doğrulama vasıtasıyla kurulmaya başlanmıştır.

[412] Nick Pope, "Protecting Long Term Validity of PDF Documents with PAdES-LTV," iç. *ISSE 2009 Securing Electronic Business Processes*, ed. Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider, (Mörlenbach:Vieweg+Teubner, 2010), 323.

Yüze yüze kanallarda kimliğin elektronik ortamda doğrulanması suretiyle gerçekleştirilen abonelik tesisi seçeneğinden, Kimlik Doğrulama Yönetmeliği'nin 5/2-(ç) maddesinde bahsedilmiştir.

Kimlik Doğrulama Yönetmeliği'nin 8. maddesinde ise yüz yüze kanallar vasıtasıyla abonelik işlemlerinin yürütülebilmesi için gerekli olan kimlik doğrulamanın ne şekilde yapılabileceğine yer verilmiştir. Yapılacak olan tüm işlemlerden önce, ilgili maddenin 3. fıkrasında yer verildiği üzere, başvuranın beyan ettiği iletişim adresine gönderilen tek kullanımlık doğrulama şifresiyle söz konusu iletişim bilgisinin aktif olarak kullanıldığı teyit edilmektedir. Bunun ardından aynı maddenin 1. fıkrası uyarınca, yüz yüze kanallarda kimlik doğrulama işlemi, başvurana sağlanan cihazlar vasıtasıyla e-Devlet üzerinden veya ICAO 9303 standartlarına uygun olarak yapay zeka veya yetkili marifetiyle yapılabileceği gibi TCKK ile PAdES oluşturularak da gerçekleştirilebilmektedir.

Kimlik Doğrulama Yönetmeliği'nin 8/2 madde hükmü gereğince kimlik doğrulama, alınacak olan video kaydı vasıtasıyla ve kimlik belgesinin NFC özelliğini taşıması durumunda, kart okuyucu vasıtasıyla gerçekleştirilebilecektir. Bu özelliğe sahip olmayan kimlikler için ise kimliğin fotoğrafının sonradan yapıştırılmamış olduğu, kimlikteki yazı karakterlerinin olması gerekene uygun olduğu gibi hususların değerlendirilmesi gerekmektedir. Akabinde belgenin MRZ'sinin olması halinde belgede bulunanlar ile elde edilen verilerin uyumluluğu incelenmektedir. Söz konusu incelemenin ardından; NVİ üzerinden de ilgili bilgiler kontrol edilmektedir. İlgili Yönetmeliğin 7/4 maddesindeki hükümde belirtilen bilgilendirme yapılarak başvuranın onayının alınmasının ardından ise kişinin kamerada yüzünün görüntüsü alınmakta olup; kimlikteki fotoğraf ile uyumu kontrol edilmektedir.

Kimlik Doğrulama Yönetmeliği'nin 8/2-(d) hükmü doğrultusunda, ilgili doğrulama işlemlerinin akabinde elde edilen veriler doğrultusunda hazırlanan işlem belgesi başvuranın yüzünü de içerecek şekilde kişiye gösterilerek; işletmeci tarafından gösterilen ve işlem numarası gibi bilgileri içeren cümlenin başvuran tarafından okunduğu an video kaydına alınmaktadır. Bu video kaydı, oluşturulan pdf dosyasına işlenmektedir. Fakat bu esnada başvuranın biyometrik verileri alınmamaktadır. Zira, Kimlik Doğrulama Yönetmeliği'nin 10/2 maddesinde de TS 13678 standardı kapsamında kimliğin doğrulanmasına yönelik yapılan işlemler hariç olmak üzere, ilgili Yönetmelik

doğrultusunda gerçekleştirilen kimlik doğrulama işlemleri esnasında kişilerin biyometrik verilerinin işlenmemesi gerektiğine yer verilmiştir. İlgili hüküm incelendiğinde, söz konusu mevzuat ile abonenin cihaz üzerine imza atarken ekrana yaptığı baskı ve çizgilerin devamlılığı gibi biyometrik verilerin alınmasının istenmediği, zaten kişinin kimliğinin elektronik olarak sorgulanmasıyla birlikte kimliğin doğrulanması konusunda şüphe kalmadığı için özel nitelikli kişisel veri olan biyometrik verilerin alınmasının gerek olmadığı anlaşılmaktadır.

Kişisel Verileri Koruma Kurulu'nun biyometrik imzaya ilişkin vermiş olduğu 27.08.2020 tarihli ve 2020/649 sayılı kararında, 6098 sayılı TBK'nın 14. ve 15. maddelerinde sadece el ile imza atılabileceğine ilişkin kurala karşılık biyometrik imzanın KVKK'nın 6/3 maddesi kapsamında değerlendirilip değerlendirilemeyeceğine dair KVK Kurumu'ndan görüş istendiğine yer verilmiştir. Biyometrik imza, tablet gibi cihazlar üzerine atılmakta olup; işlem yapılmak istenen belgeye bağlanmaktadır. Islak imza ile biyometrik imza birbirine denk değildir. Islak imzada imzanın nasıl oluştuğuna ilişkin geometrik ve dinamik özelliklerine dikkat edilmektedir. Biyometrik imzada ise imzanın atılması esnasında cihaza yapılan basıncın miktarı, kalemin hızı, imzanın yönü ve kişiye özgü olan diğer özellikler dikkate alınmaktadır. Biyometrik veri, özel nitelikli veri olduğundan ancak kişinin açık rızasının bulunduğu veya KVKK'nın 6. maddesinde öngörülen hallerin gerçekleşmesi halinde işlenebilecektir. Fakat KVKK'nın 6/3 maddesinde yer verilen kanunlarda öngörülme haline TBK'nın 15. maddesinin dahil olmadığı belirtilmiştir. Bu doğrultuda kişinin yalnızca açık rızası dahilinde, gerekli aydınlatmaların yapılmış olması kaydıyla ve Kurul'un belirlemiş olduğu Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler'de[413] öngörülen tedbirlerin alınması halinde biyometrik imzanın işlenebileceğine yer verilmiştir.[414]

Geçmiş dönemlerde bazı işletmeciler tarafından dijital imza ile abonelikler yapılmaktaydı. Abonelik yapılırken aboneler tablet üzerine imza atmaktaydı. İmzanın tablete atılması esnasında kalemin ekrana yaptığı basınç, hız, ivme gibi biyometrik veriler

[413] KVK Kurulu, 31.01.2018 tarih ve 2018/10 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/4110/2018-10 , Erişim Tarihi: 25 Eylül 2022.
[414] KVK Kurulu, 27.08.2020 tarih ve 2020/649 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6815/2020-649 , Erişim Tarihi: 25 Eylül 2022.

de işletmeci tarafından işlenmekteydi.[415] Bu veriler, kişiye özgü özellikler içermesi sebebiyle, KVK Kurulu'nun 2020/649 sayılı kararında özel nitelikli kişisel veri olarak kabul edilmiştir. Yalnızca ilgili kararda yer verilen hallerde ve belirtilen önlemlerin alınması halinde biyometrik imzanın işlenebileceği belirtilmiştir. Biyometrik imza verilerinin bir kaleme yüklenmesiyle aynı imza o kişi orada bulunmasa bile kaleme attırılabileceğinden; söz konusu yöntemin güvenli olmadığı açıktır. Bu sebeple zamanında işletmeciler tarafından elde edilen biyometrik verilerin adli ve idari makamlar tarafından istenmesinin haricinde başka hiçbir işlem için kullanılmaması gerektiğine, Kimlik Doğrulama Yönetmeliği'nin Geçici 1/1 maddesinde yer verilmiştir. Aksi durumun ilgili Yönetmelik hükmünün yanı sıra KVKK'nın da ihlali anlamına geleceği açıktır.

7. ABONELERİN ELEKTRONİK HABERLEŞME HİZMETİ KULLANIMINDAN KAYNAKLANAN KİŞİSEL VERİLERİ

7.1. ABONE DESEN YAPISIYLA İŞLETMECİ TARAFINDAN BTK'YA GÖNDERİLEN KİŞİSEL VERİLER

Abone teknik detayı ya da abone rehber dosyaları olarak da adlandırılan abone desen yapısı; elektronik haberleşme mevzuatında yer alan hizmetlerden olan mobil, sabit telefon hizmeti, internet servis sağlayıcılığı, altyapı işletmeciliği hizmeti, uydu haberleşme hizmeti (UHH), GMPCS (Mobil Uydu) hizmetlerini[416] kapsayacak bilgileri içermektedir. Bu alanda hizmet veren işletmeciler, aboneleri hakkındaki detaylı bilgiyi BTK'ya göndermekle yükümlü kılınmıştır.[417]

---

[415] Turkcell İletişim Hizmetleri A.Ş., "Güvenli Dijital İmza Nedir ve Neden Güvenlidir?," https://www.turkcell.com.tr/yardim/hattiniz/abonelik-islemleri/guvenli-dijital-imza-nedir-ve-neden-guvenlidir , Erişim Tarihi: 25 Eylül 2022.

[416] GMPCS (Global Mobile Personal Communications By Satellite-Küresel Mobil Kişisel İletişim Uydu), küçük ve kolay taşınabilir terminal cihazlarla erişim sağlanabilen bir dizi uydudan ulusötesi, bölgesel ya da küresel kapsama alanı taşıyan kişisel bir iletişim olarak adlandırılmakta olup; cep telefonları ile benzer hizmetler vermektedir. GMPCS hizmetleri, iki taraflı ses, faks, mesajlaşma, veri ve hatta geniş bant multimedya hizmeti içermektedir. (ITU, GMPCS-MoU, https://www.itu.int/en/gmpcs/Pages/default.aspx , Erişim Tarihi: 25 Eylül 2022.)

[417] TELKODER, "Abone Deseni Yükümlülüğüne İlişkin Tespit ve Öneriler," 1-3, https://telkoder.org.tr/wp-content/uploads/2020/06/20-028.pdf , Erişim Tarihi: 25 Eylül 2022.

Abone dosyaları ile abonelere ait abonelik başlangıç ve bitiş tarihleri, abonenin ad-soyadı bilgisi, unvanı-mesleği, aboneliğin tesis adres bilgileri ile kurumsal abonelik ise yetkilisine ilişkin bilgiler gibi çeşitli konulara ilişkin Kurum'a bilgi aktarımı olmaktadır.[418]

EHK'nın 6. maddesiyle BTK, elektronik haberleşme hizmetlerine dair işletmecileri yetkilendirmeye ilişkin gerekli tedbirleri alarak denetleme ve mevzuatın gereklerinin yerine getirilmesini isteme hakkına sahipken; yine EHK'nın 12. maddesinde işletmecilerin elektronik haberleşme sektöründe milli güvenlik ve 5397 sayılı Kanun[419] ve 5651 sayılı Kanun ile getirilen mevzuattaki düzenlemelere ilişkin talepleri karşılamaya yönelik yükümlülüklerini yerine getirebilmek amacıyla teknik altyapıyı kurmakla yükümlü kılınmıştır.

24 Ekim 2018 tarihindeki BTK kurul kararıyla[420] elektronik haberleşme sektöründeki işletmeciler tarafından hazırlanması istenen abone desen yapısı, 16 Nisan 2019 ve 25 Nisan 2019 tarihlerinde birtakım değişikliklere uğramış, 8 Mayıs 2019 tarihinde ise son haline kavuşmuştur.[421]

Söz konusu hükümlerden hareketle, Yetkilendirme Yönetmeliği'ndeki 19/1-(u) maddesi uyarınca işletmeciler, milli güvenliğe yönelik taleplerin karşılanması amacıyla Kurum tarafından belirlenen veri, bilgi ve belgeleri yetkili mercilere teslim etmekle yükümlü kılınmıştır.

Abone desen yapısı ile işletmecilerin aboneleri hakkında ayrıntılı abonelik bilgisi verilmesinin sağlanması amaçlanmaktadır. Bu veriler sürekli ve düzenli olarak BTK'ya aktarılmakta olup; böylece Kurum'daki verilerin güncelliği sağlanmaktadır. Ayrıca abone desen yapısının temel amacının abone yerine, telefon numarası veya interneti kullanan

---

[418] TELKODER, "Abone Deseni Yükümlülüğüne İlişkin Tespit ve Öneriler," 1.
[419] RG. 23.07.2005, S. 25884.
[420] Serbest Telekomünikasyon İşletmecileri Derneği'nin (TELKODER) 11.06.2020 tarih ve 20-028 sayılı BTK'ya görüş bildirdiği yazıda, ilgili BTK Kurul Kararı'nın sayısının 2018/DK-BSD/314 olduğu belirtilmiştir. https://telkoder.org.tr/wp-content/uploads/2020/06/20-028.pdf , Erişim Tarihi: 25 Eylül 2022.
[421] TELKODER'in abone desen yapısıyla ilgili BTK tarafından alınan kurul kararlarının iptali için Danıştay 13. Dairesi'nde açılan ve Danıştay'ın ilk derece mahkemesi sıfatıyla gördüğü 2019/2412 E. Sayılı davada, yürütmenin durdurulması isteminin reddedildiğine ilişkin yayınlanan kararda, abone desen yapısıyla ilgili diğer BTK Kurul Kararları'nın sayısının 16.04.2019 tarih ve 2019/DK-BSD/109, 25.04.2019 tarih ve 2019/DK-BSD/117 ve 08.05.2019 tarih ve 2019/DK-BSD/131 sayılı Kurul Kararları olduğu görülmektedir. https://telkoder.org.tr/wp-content/uploads/2022/04/Dan%C4%B1%C5%9Ftay-13.-D.-2017-968-Y%C3%BCr%C3%BCtmenin-Durdurulmas%C4%B1-Red-Karar%C4%B1.pdf , Erişim Tarihi: 25 Eylül 2022.

gerçek kullanıcıya ulaşmak olduğu açıktır.[422] Örneğin, kurumsal abonelikte abonelik ticari işletmenin üzerine iken; aslında kullanıcıları şirket içerisindeki gerçek kişilerdir. Kurum tarafından ilgili gerçek kişilere ulaşılması ile elektronik haberleşme hizmetini çoğu zaman araç olarak kullanarak hukuka aykırı eylemleri gerçekleştiren şahıslara ulaşılabilmesinin sağlanması hedeflenmektedir.

Suç unsuru teşkil eden herhangi bir eylemin takibi veya tespiti için en önemli ve belki de ilk başvurulması gereken husus gerçekleşen haberleşmenin tespiti veya gerçekleşmekte olan haberleşmenin izlenmesidir. Özellikle kurumsal aboneliklerde abonelik yetkilisi kurum yetkilisi olmakla birlikte, fiilen aboneliği kullananlar ise o kurum veya şirkette çalışanlardır. İnternet aboneliği düşünüldüğünde kurum veya şirketteki ortak kullanıma tahsis edilmiş internetten herkes faydalanmakta, telefon aboneliğinde ise dahililer vasıtasıyla aynı abonelik numarası üzerinden yüzlerce kişi arama yapabilir veya aranabilir konumda bulunmaktadır. Bu durum, internet aboneliğine bağlı IP adresinden hangi sayfaların ziyaret edildiği veya telefon aboneliği üzerinden suç teşkil edebilecek faaliyetlerle ilgili aramaların kim tarafından yapıldığının tespit edilememesi sorununu ortaya çıkarmaktadır. Söz konusu durumların bertaraf edilebilmesi ve suça konu fiilin kim tarafından gerçekleştirilmiş olduğu, abone desen yapısı ile oluşturulan abone dosyaları vasıtasıyla DDI hizmet numarası[423] gibi bilgilerin BTK'ya gönderilmeye başlanmasıyla çözülmek istenmiştir.

İşletmeciler, abone desen yapısında bulunan kişisel verileri, KVKK'nın 5/2-(ç) maddesinde belirtilen veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmek maksadıyla BTK ile paylaşmaktadır. Aktarılan bu verilerin BTK tarafından işlenmesinin kişisel verilerin korunması konusunda ayrıksı tutulabilmesinin hukuki dayanağı ise KVKK'nın 28/1-(ç) maddesinde belirtilen, milli güvenliği ve savunmayı gerektiren

[422] Rekabetçi Telekomünikasyon İşletmecileri Derneği (TELEKOMDER), "Ortak Abone Kayıt Deseni'ne Geçiş Nasıl Olmalı?," https://www.telekomder.org/ortak-abone-kayit-desenine-gecis-nasil-olmali/ , Erişim Tarihi: 25 Eylül 2022.

[423] Bir kamu kurumu ya da şirket telefon ile arandığında, aramanın cevaplandırılması süresince bazı yönlendirmeler yapılarak, ana telefon hattına bağlı, telefon şirketlerinin dahili numarayı kullanan kişiye özgülediği kişiye doğrudan bağlanmayı sağlayan özellik, DDI ya da DID olarak kısaltılan Direct-Dial-In (DDI)- Direct-Inward-Dialling (DID) "Doğrudan Dahili Arama" olarak adlandırılır. Böylelikle söz konusu kamu kurumu ya da şirket, çalışanlarına ayrı bir fiziki hatta gerek olmadan, doğrudan dahili hatta giden bir telefon numarası oluşturmuş olmaktadır. Arayan kişinin bakış açısından, doğrudan arama numarası herhangi bir standart telefon numarasına benzemektedir. Ancak DDI, arayanı kurum ya da şirket içerisindeki belirli bir dahili numaraya veya konuma götüren bir numara kullanmaktadır. Bunun modern hali VoIP telefon sistemi olarak adlandırılır. Bunlar fiziksel değil, geniş bant üzerinden sanal bağlantılardır. VoIP'de doğrudan arama, maliyeti düşük olduğu için daha çok tercih edilmektedir. (DDI, https://dialogictelecom.com/2021/01/what-is-a-ddi-telephone-number/ , Erişim Tarihi: 26 Eylül 2022.)

hallerde kamu kurumları tarafından önleyici tedbirlerin alınabilmesi amacıyla faaliyetlerin KVKK kapsamından istisna tutulmasına ilişkin hüküm olup; BTK'nın milli güvenliğin sağlanması sebebiyle söz konusu veri toplama faaliyeti, KVKK kapsamının dışında tutulduğu söylenebilir.

BTK'ya işletmeciler tarafından abone desen yapıları vasıtasıyla gönderilen ayrıntılı abone bilgilerinin, EHK'nın 6/1-(ı) maddesi kapsamında gönderildiği söylenebilir. Söz konusu hükümde, BTK'ya işletmecilerden diğer kurumların talep edebileceği her türlü bilgi ve belgeyi isteyebilme ve kendi bünyesinde saklayabilme yetkisi verilmiştir. İlgili madde ile BTK'ya herhangi bir yargı kararı olmadan ve haberleşme özgürlüğüne aykırı olarak her türlü bilgi ve belgeyi işletmeciden alabilmesine olanak sağlayan çok geniş bir yetki verildiği ve bunun Anayasa'nın 12., 13. ve 22. maddelerine aykırı olduğu iddiasıyla, madde hükmünde geçen "her türlü" ifadesinin bulunmaması gerektiği belirtilerek iptali istenmiştir. Konuyla ilgili Anayasa Mahkemesi kararında, ilgili hükümdeki iptali istenen ifadenin, BTK'nın kuruluş amaçlarından biri olan sektöre ilişkin şikayetlerin değerlendirilmesi ve işletmecilerin denetlenmesi amacı çerçevesinde kullanılabileceği belirtilmiştir. BTK'ya ilgili madde ile verilen yetkinin sınırlarının elektronik haberleşme sektöründeki hizmet ve sistemlere yönelik olarak, işletmecilerin açıklayabilecekleri ticari sırlarının korunması ve çerçevesinin çizilmesi, abonenin kişisel verilerinin korunması gibi yine aynı Kanun'daki çeşitli hükümlerle belirlenmiş olduğuna yer verilerek; söz konusu "her türlü" ifadesiyle BTK'ya kişilerin özel hayatının gizliliğine ya da haberleşmenin özgürlüğünü kısıtlayacak veya müdahale edecek bilgi ve belgelerin alınmasına yönelik bir yetki verilmediği ifade edilmiştir. Bu sebeple "her türlü" ifadesinin EHK'nın 6/1-(ı) maddesinden çıkartılmasına, iptal edilmesine gerek olmadığına hükmedilmiştir.[424]

Elektronik haberleşme sektörünü düzenleyen kurum olan BTK ile ilgili sektörde hizmet veren işletmecilerin uymakla yükümlü bulundukları hükümler ve yetkilerinin 5809 sayılı EHK ile belirlenmiş olması, BTK'nın işletmecilerden talep edebileceği bilgi ve belgenin de sınırlandırıldığı anlamına geldiğinden; ilgili kararın yerinde olduğu, her ne kadar söz konusu kanun metninde "her türlü" ifadesi yer alsa da BTK'nın yetkisi dışındaki alan ve konularda işletmecilerden bilgi talep edemeyeceği söylenebilir.

[424] Anayasa Mahkemesi'nin 2008/115 E., 2011/86 K. sayılı Kararı, https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2011-86-nrm.pdf , Erişim Tarihi: 26 Eylül 2022.

7.2. ABONENİN ELEKTRONİK HABERLEŞME HİZMETİ KULLANIMINDAN KAYNAKLI ORTAYA ÇIKAN TRAFİK VE KONUM VERİLERİ

Elektronik haberleşme ağı ile iletişimin gerçekleştirilmesi veya faturalamaya ilişkin olarak iletişimin yönlendirilmesi, süresi ve zamanına ilişkin her türlü veri trafik verisi olarak adlandırılmaktadır.[425]

Elektronik haberleşme hizmetlerinin sağlanması, genellikle kişisel veri olarak da nitelendirilen trafik ve konum verilerinin işlenmesini gerektirir. Bu tür veriler, bir hizmetin (veya bir ağın) kullanıcısı hakkında, tanımlama ya da adresleme bilgileri, bir kullanıcının terminal donanımının konumu hakkında bilgiler ve sonuç olarak kullanıcının konumu veya iletişimin zamanı ve süresi dahil olmak üzere ayrıntılı bilgileri içermektedir.[426]

7.2.1. AB Düzenlemeleri Çerçevesinde Trafik Verilerinin İşlenmesi

2002/58/EC sayılı Direktif'in 2. maddesinde trafik verileri, elektronik haberleşme ağı üzerinde haberleşmenin gerçekleştirilmesi ya da ücretlendirilebilmesi için işlenmekte olan veri şeklinde tanımlanmıştır. Aynı maddede, konum verileri, elektronik haberleşme ağı üzerinde işlenen ve bu hizmeti kullanan kişinin iletişim esnasında kullandığı cihazın coğrafi anlamda konumunu gösteren veri olarak tanımlanmıştır.

Söz konusu Direktif'in 6/2 maddesine göre, haberleşme hizmetinin sunumunda abonenin aldığı hizmeti faturalama ve haberleşme esnasında operatörler arasındaki arabağlantıdan kaynaklanan ödemelerin hesaplanabilmesi için trafik verilerinin işlenebileceği belirtilmiştir. Bu işleme faaliyetinin süresi ise faturaya itiraz süresi ya da ödemenin takibinin yapılabileceği sürenin bitimine kadar olacak şekilde belirlenmiştir. Aynı hükmün devamında ise elektronik haberleşme alanında faaliyet gösteren hizmet sağlayıcının, aboneye pazarlama ve katma değerli hizmetlerin sağlanması amacıyla abonenin onayı dahilinde trafik verilerini işleyebileceği belirtilerek, söz konusu onayın abone tarafından geri alınma imkanının da aboneye verilmesi gerektiği vurgulanmıştır.

[425] Information Commissioner's Office (ICO), "Traffic Data," https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/traffic-data/ , Erişim Tarihi: 26 Eylül 2022.
[426] Kosta, Data Protection Law, 379.

Ayrıca hizmet sağlayıcının, aboneyi ya da kullanıcıyı işlenen kişisel verilerin neler olduğu ve ne kadar süreyle bu trafik verilerinin işleneceğine dair onay alınmadan önce bilgilendirme yükümlülüğünü de yerine getirmesi gerektiği belirtilmiştir.

Elektronik haberleşme sektörü vasıtasıyla cezai anlamda suç oluşturan olayların soruşturulması ve kovuşturulması sürecinde haberleşmenin takibinin yapılabilmesi adına trafik verilerinin incelenmesi önem teşkil etmektedir. Bu anlamda bir suça ilişkin doğrudan delil niteliğinde bir trafik verisi ya da delil toplanması için yardımcı olabilecek bir trafik verisi olayların çözümlenmesi aşamasında kullanılabilir. AB veri koruma mevzuatına göre, kural olarak elektronik haberleşme sürecinde elde edilen trafik verilerinin, elektronik haberleşmenin tamamlanmasının akabinde silinmesi gereklidir. Bu ilkenin, trafik verilerinin faturalandırma amaçlı saklanması gerekliliği gibi birtakım istisnaları mevcuttur. Bununla birlikte, kolluk kuvvetleri tarafından hizmet sağlayıcılardan her bir aboneye ilişkin trafik verilerinin tamamının belirli bir süre saklanması talep edilmektedir. Bu durum, mahremiyet hakkı ve veri koruma savunucuları tarafından endişeyle karşılanmaktadır.[427]

İşletmeciler, bir yandan trafik verilerinin kanuna ve yönetmeliklere uygun olarak saklanmaması halinde idari para cezalarının uygulanacak olması bir yandan da trafik verilerinin saklanması ve korunması için server gibi ilave ekipman satın alınması, ekipmanların saklanacağı güvenlikli fiziki mekanlar, ek personel istihdamı, güvenlik için gereken arayüz ve güvenli ağ maliyetleri göz önünde bulundurulduğunda; trafik verilerinin farklı nedenlerle saklanması süreci, işletmelerin öngörülemeyen durumlarla karşılaşmasına sebep olabilir. Öte yandan ISS'ler gibi işletmeciler, trafik verilerinin saklandığı bilgisinin abone açısından bir güvensizliğe neden olabileceği kaygısını taşıyarak, müşteri kaybına sebep olabilecek hamlelerden uzak durmak istemektedir.[428]

Kural olarak trafik verilerinde, iletinin içeriği bulunmamalıdır. Trafik verileri ile diğer veriler arasında bir ayrım yapılarak iletim (trafik verileri) ve içerik (içerik verileri) olarak ayrı yasal rejimler oluşturmak hedeflenmektedir. Uygulamada trafik ve içerik verileri çoğu zaman aynı anda oluşturulmaktadır. Böylelikle, yalnızca elektronik haberleşmenin gerçekleşmesi için gerekli trafik verilerinin yanında, abonenin ya da

[427] Caroline Goemans, Jos Dumortier, "Enforcement Issues - Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity," (2003), 2, https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/440retention-of-traffic-data-dumortier-goemans2f90.pdf , Erişim Tarihi: 1 Ekim 2022.
[428] Goemans, "Traffic Data," 5-6.

kullanıcının ilgi duyduğu alanların da gösterildiği içerik verilerinin ayrıştırılması zarureti ortaya çıkmaktadır. Aksi halde trafik verilerinin toplanması, depolanması ve işlenmesi ile bir abonenin elektronik haberleşme hizmetlerini kullanımı izlenerek kendisine dair doğrudan ya da dolaylı pek çok bilgi elde edilebilmekte ve bu sayede, ISS'ler ve diğer işletmeciler, doğrudan pazarlama yapmak amaçlı trafik verilerini elinde bulundurarak, bunu farklı amaçlar için kullanabilmektedir.[429]

Ağ güvenliği sebebiyle kamu makamlarının, ISS'lerden ağ trafiğinin analizini ve belirli türdeki günlük bireysel iletişim verilerinin bilgilerini talep etmesinin, işletmecilere yüklediği sorumluluklar ve işletmeciler açısından yaşanabilecek zorluklar yanında güvenlik gerekçesiyle suç ve suçlunun takibi ve sonuçları açısından anlamlandırılabilir nedenleri bulunmaktadır. Kolluk makamları, iletişim ağları kullanılarak işlenen, bilgisayar sistemlerine sızma, ticari sırların çalınması, önemli bilgi teknoloji sistemlerinin sabote edilmesi, telefon sistemlerinin kötüye kullanılması, dolandırıcılık, uyuşturucu kaçakçılığı, insan kaçakçılığı, terör gibi suçların etkin olarak coğrafi ya da kronolojik olarak takibinin yapılabilmesi için trafik verilerine ihtiyaç duymaktadır.[430] Fakat trafik verileriyle ilgili dikkat edilmesi gereken bir diğer husus ise trafik verileri sayesinde kesin değil, olası kullanıcı ve cihaza ulaşılabilmesidir. Diğer bir ifadeyle, kişinin e-imzasının veya kayıtlı elektronik posta adresinin başkaları tarafından kullanılması veya hackerların hukuka aykırı faaliyetlerini başkalarına ait cihazlar üzerinden gerçekleşiyor gibi göstermeleri muhtemel olduğundan; trafik verilerine dayanarak faillerin tespit edilmesi aşamasında tüm bu durumların dikkate alınarak gerekli değerlendirmelerin yapılması gerekmektedir.[431]

AB Veri Koruma Otoriteleri ve Article 29 Çalışma Grubu, kanuni gereklilikler ve yaptırımlar ölçüsünde trafik verilerinin istisnai olarak tutulabileceğini; ancak mahremiyete yönelik kabul edilemez riskleri barındıran trafik verilerinin rutin olarak saklanmasının AİHS'nin özel hayata saygının konu edildiği 8. maddesi ve ifade özgürlüğüne yer verilen 10. maddesi uyarınca belirlenen temel hakları ihlal edeceği anlamına geleceğini belirterek, temel hakların, demokratik bir toplumda adaletin temelini

[429] Goemans, "Traffic Data," 4-5.
[430] Goemans, "Traffic Data," 5-6.
[431] Öztekin, Türk İnternet Hukuku, 171.

teşkil ettiğini ve devlet müdahalesi ile gerçekleşebilecek keyfi durumlar karşısında bireyleri koruyucu bir vazife üstlendiğini vurgulamaktadır.[432]

Kolluk makamlarının suçun tespiti ve ulusal güvenliğin korunması gerekçeleriyle trafik verilerinin saklanması sürecine ilişkin daha somut gerekçeler belirlemesi ve trafik verilerinin saklanma sürelerinin kısa olması gerekliliği göz ardı edilemez. Ayrıca trafik verileri ile tıbbi, dini, cinsel, politik gibi hassas kişisel veriler de dahil olmak üzere, bir kişiye dair ilgi alanları internet ortamındaki trafiğinin taranması ile elektronik postaları, cep telefonu hareketleri dahil olmak üzere neredeyse bütün kişisel verilerinin her an ifşa edilebileceği endişesi nedeniyle kişisel verilerin hakkı çerçevesinde bireylerin korumaya tabi tutulması gerekmektedir. Aksi halde elektronik haberleşmenin her geçen gün yaygınlaştığı ve hemen her faaliyetin elektronik ortamda planlandığı ve gerçekleştirildiği günümüzde, bu durum tüm nüfusun günlük hayatının izinsiz olarak takip edilebileceği gibi bir tehlike ortaya çıkarmaktadır. Bu nedenle trafik verilerinin genel olarak saklanması, kişisel verilerin korunması hakkının ihlal edilebileceği konusunda güven eksikliğine neden olmaktadır.[433]

7.2.2. AB Düzenlemeleri Çerçevesinde Konum Verilerinin İşlenmesi

Trafik verilerinin yanı sıra kişilerin günlük yaşamdaki anlık davranışlarının takibini sağlayan bir diğer veri türü de konum verisidir. Bir elektronik haberleşme ağı kullanıcısının terminal cihazının bulunduğu enlem, boylam ve rakım bilgisi, kullanıcının seyahatinin gerçekleştiği yön ve konum bilgisinin kaydedildiği zaman bilgileri konum verisi olarak adlandırılmaktadır.[434]

Konum tabanlı hizmetler, GSM ve GPS'den WiFi ve Bluetooth'a kadar çok çeşitli teknolojilere dayanabilir. Elektronik Haberleşme Direktifi ile, konum tabanlı hizmetlerin sağlanması için trafik verileri olarak nitelendirilmeyen konum verilerinin işlenmesine ilişkin özel kurallar da düzenlenmiş olup; bu verilerin işlenmesine yalnızca verilerin anonim hale getirilmesi halinde veya kullanıcıların ya da abonelerin onayı ile izin verilmektedir.[435]

---

[432] Goemans, "Traffic Data," 7.
[433] Goemans, "Traffic Data," 8.
[434] Information Commisioner's Office (ICO), Location Data, https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/ , Erişim Tarihi: 2 Ekim 2022.
[435] Kosta, Data Protection Law, 379.

Trafik verileri haricindeki konum verilerinin işlenmesi hususunda, Elektronik Haberleşme Direktifi'nin 9. maddesine göre işletmeci, katma değerli hizmet sağlamak istediği aboneden veya kullanıcıdan işleme faaliyetini gerçekleştirmek için onay almalıdır. Trafik verileri dışındaki konum verilerinin işlenmesine yalnızca veri sahibinin rızası alındığında izin vermesi anlamlıdır; çünkü katma değerli hizmetler, bireylere kişisel deneyimlerini geliştirmek için sunulan ek hizmetlerdir. Bununla birlikte, Elektronik Haberleşme Direktifi'nin 9. maddesi, yalnızca bir elektronik iletişim hizmetinin bir kullanıcısının cihazının coğrafi konumunu gösteren konum verilerine ve bir kamu iletişim ağı aracılığıyla iletilen konum verilerine uygulandığı için sınırlı bir kapsama sahiptir. Bu nedenle örneğin kullanıcıya cep telefonu aracılığıyla kendisine en yakın eczaneyi bulmasını sağlayan konum tabanlı bir hizmetin sunulması için konum verilerinin işlenmesi gerekerek kullanıcının kendisinin rızasının gerekli olduğu açıktır.[436]

Konum verisini işleyecek olan işletmeci, kişiden onay alınmadan önce, işleyecek olduğu konum verisi türü, işleme süresi ve amacı, aktarılıp aktarılmadığı hususlarında aboneyi bilgilendirmekle yükümlüdür. Ayrıca abonelere ya da kullanıcılara vermiş oldukları onayları basit ve ücretsiz bir yöntemle geri çekme imkanı da tanınmalıdır. Article 29 Çalışma Grubu, söz konusu verinin konum verisi olması sebebiyle, rızanın aboneden değil, terminal cihaz kullanıcısından alınması gerektiğini düşünmektedir. Fakat bu durumun uygulanabilirliği ise tartışmalıdır. Örneğin küçük yaştakilerin kullandığı cihazlarda onayın kullanıcıdan alınması durumunda, alınan onayın geçerliliğinin sorgulanacağı açıktır.[437] Söz konusu onayın varlığı halinde işlenebilmesinin yanı sıra ilgili konum verilerinin anonim hale getirilmesi suretiyle de katma değerli hizmetin aboneye sağlanabilmesi için konum verilerinin işlenebilmesi mümkündür.[438]

Alman Veri Koruma ve Gizlilik Yasası da[439] konum verilerinin işlenmesine ilişkin 13. madde hükmünde, konum verilerinin yalnızca anonimleştirilerek veya kullanıcının bilgisi dahilinde katma değerli hizmetlerin sunulabilmesi için işlenebileceğini belirtmiştir. Katma değerli hizmetler, ilgili Yasa'nın 2/5 maddesinde konum verilerinin

[436] Kosta, Data Protection Law, 345.
[437] Kosta, Data Protection Law, 338.
[438] Kosta, Data Protection Law, 345.
[439] Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien* (Telekommunikation- Telemedien-Datenschutz-Gesetz - TTDSG), 23.06.2021, https://www.gesetze-im-internet.de/ttdsg/TTDSG.pdf , Erişim Tarihi: 2 Ekim 2022.

bir SMS'in iletiminin ötesinde kullanıcıya sağlanan ek hizmetler ve telekomünikasyon hizmetinin faturalandırılmasını sağlayan ek hizmetler olarak tanımlanmaktadır.

Alman Veri Koruma ve Gizlilik Yasası'nın 13. maddesinin devamında, katma değerli hizmet sunumu esnasında kullanıcının mobil cihazının konumu her belirlendiğinde, hizmet sağlayıcının kullanıcıyı bilgilendirmesi gerektiğine yer verilmiştir. İlgili konum verilerinin üçüncü taraflara aktarılması ise yine kullanıcının onayına bağlıdır. Kullanıcılara yapılan her bilgilendirmede, kullanıcının onayını geri çekmesine imkan sağlanan ücretsiz ve kolay bir imkan sağlanması gerektiği vurgulanmıştır.

Teknolojinin her geçen gün gelişmesi ve mobilitenin artmasıyla birlikte konum verileri kullanılarak kişilerin hareketleriyle bağlantılı faaliyetlerin ayrıntılı kayıtlarının tutulması, bireylerin kişisel mahremiyetini en aza indirgemektedir. Bireyleri konum verilerini takip ederek onları izlemek, davranışlarını ve tercihlerini ayırt etmeye ve gözlemeye yönelik, gizlilik taşıyan kişisel bilgileri aralıksız olarak elde etmek imkanı tanımaktadır.[440] Buna karşılık, trafik ve konum verilerinin bireyler açısından yalnızca aleyhe delil teşkil edecek yönde veriler olduğu düşünülmemelidir. Örneğin, bir kişinin olay saatinde başka bir yerde olduğunun trafik ve konum verileri sayesinde kanıtlanmasının, yargılama sürecini kısaltarak kişinin masumiyetinin kanıtlanmasını kolaylaştıracağı açıktır.[441]

Bir başka açıdan konum verilerini incelemek gerekirse; konum verilerinin bir RFID ağı veya bir Bluetooth ağı aracılığıyla iletilmesi halinde, kullanıcının yine onayının aranıp aranmayacağı sorgulanmalıdır. Buna karar verebilmek için söz konusu ağın halka açık olup olmadığının belirlenmesi önemlidir. Elektronik iletişim ağının halka açık olmaması durumunda konum verilerinin işlenmesi, Elektronik Haberleşme Direktifi'nin 9. maddesinin koruma alanı dışında kalacaktır. Böyle bir durumda işleme faaliyetinin, yalnızca ilgili kişinin rızası kapsamında yapılması değil kişisel verilerin işlenmesine izin veren genel hükümlere uygun olarak yapılması gerekecektir.[442]

---

[440] Jonathan Andrew, "Locatian Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights," *European University Institute Department of Law PhD Theses*, (2018): 20, 26, https://cadmus.eui.eu/bitstream/handle/1814/51585/Andrew_2018_LAW_add_addendum.pdf?sequence=4&isAllowed=y , Erişim Tarihi: 2 Ekim 2022.
[441] Öztekin, Türk İnternet Hukuku, 172.
[442] Kosta, Data Protection Law, 345.

7.2.3. Türk Hukukunda Abonenin Elektronik Haberleşme Hizmetlerini Kullanımından Kaynaklı Elde Edilen Trafik ve Konum Verileri

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 4/1-(k) maddesine göre trafik verisi, iletişimin gerçekleştirilmesi ya da haberleşme hizmetinin sunumunda abonenin aldığı hizmeti faturalama maksadıyla işlenen veriler olarak tanımlanmıştır. Buradaki tanımda trafik verisinden geniş şekilde söz edilerek; haberleşmeye dair hemen her verinin trafik verisi olabileceğinden bahsedilmiştir.

5651 sayılı Kanun'un 2/1-(j) maddesinde ise trafik bilgisi, ilgili kanunun internet hizmetine yönelik hazırlanmış olması sebebiyle, trafik verisi internet yönünden tanımlanmış olup; tarafların IP adresleri, port bilgisi, aktarılan verinin boyutu, sunulan hizmetin türü, başlangıç ve bitiş zamanı ve varsa aboneye ilişkin kimlik verileridir.

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 4/1-(h) maddesinde belirtildiği üzere konum verisi, kamuya açık olan elektronik haberleşme hizmeti kullanıcısının cihazının konumunu tespit eden ve elektronik haberleşme şebekesinde ya da hizmeti doğrultusunda işlenen veri olarak tanımlanmıştır.

Trafik ve konum verilerinin işlenmesine ilişkin temel hükümler EHK'nın 51. maddesinde yer almaktadır. EHK'nın 51/2 maddesinde; haberleşmenin gizliliği ilkesi gereğince, iletişimi gerçekleştiren tarafların rızası olmadan iletişimin takip edilemeyeceği, dinlenemeyeceği, kayıt altına alınamayacağı ya da kesintiye uğratılamayacağı ve saklanamayacağı belirtilmiş olup; bunun aksinin yalnızca mevzuat veya yargı kararları gereğince gerçekleştirilebileceğine yer verilmiştir.

Ayrıca EHK'nın 51/9 maddesinde bahsi geçen abone şikayetleri ya da denetimlerin varlığı halinde trafik verilerinin işlenmesi hususu çerçevesinde, EHK'nın 51/7 hükmünde ise trafik verilerinin, kullanıcıyla işletmeci arasında iletişim vasıtasıyla hukuka aykırı eylem gerçekleştirilmiş olması, arabağlantı, fatura düzenleme gibi hususlardan doğan anlaşmazlıkların çözümünde, ilgili trafik verisinin sadece işletmecinin yetki verdiği kişiler tarafından işlenebileceği hüküm altına alınmıştır.

Hizmetlerin pazarlaması veya katma değerli hizmetlerin sunumu için trafik veya konum verileri işlenmek istendiği takdirde ise yine 51/7 hükmü gereğince, ilgili veriler ancak anonimleştirilerek ya da iletişimi gerçekleştiren tarafların rızalarının bulunması kaydıyla, yalnızca bilgilendirmesi yapılan konularda ve sürede işlenebilmektedir.

EHK'nın 51/8 maddesinde ise konum verilerinin işlenmesine ilişkin hükme yer verilmiştir. İlgili konum verilerinin, mevzuatın öngördüğü hallerde veya yargı kararları uyarınca işlenebileceği, acil durumların varlığı halinde ise kişinin rızası olmasa bile 5902 sayılı Kanun'da belirtildiği üzere kişinin konum ve kimlik verisinin işletmecinin yetkilendirdiği kişiler tarafından işlenebileceği düzenlenmiştir.

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 9. maddesine göre trafik ve konum verisinin işletmeci tarafından işleneceği hallerde, KVKK'nın 10. maddesinde yer verilen aydınlatma yükümlülüğünün yanı sıra işletmeci, aboneyi veya kullanıcıyı işleme amacı ve süresiyle birlikte trafik veya konum verisi türü hakkında ayrıca bilgilendirmekle yükümlü kılınmıştır.

İdari Yaptırımlar Yönetmeliği'nin 13/3 maddesinde ise trafik ve konum verisini işlemeye yönelik yükümlülüklerini yerine getirmeyen işletmeciler hakkında, ihlalin yaşandığı yıldan bir önceki yıla ait net satış gelirlerinin yüzde 3'üne kadar idari para cezası uygulanması öngörülmüştür.

Anayasa Mahkemesi bir kararında, kişinin adına kayıtlı telefon hattına ait internet verilerinin, log kayıtlarının, telefonunun IMEI bilgilerinin ve açık Wi-Fi noktası kullandığına ilişkin bilgilerin gerçek kişi hakkında bilgi edinmeye yarayan bilgiler olduğuna yer verilmiştir. Dolayısıyla bu bilgilerin düzeltilmesini veya silinmesini talep etme hakkının özel hayata saygı kapsamında, kişisel verilerin korunmasını isteme hakkı çerçevesinde incelenmesi gerektiği belirtilmiştir. Bununla birlikte, bir kişisel verinin varlığı halinde, veriye herhangi bir müdahale veya sınırlama yapılması durumunda Anayasa'nın 20/3 hükmünde bahsi geçen kişisel verileri koruma hükümlerinin geçerli olacağı vurgulanmıştır. Başvurucunun, işletmeciye ait başka abonelerle birlikte ortak kullanması sağlanan IP adresinden internete giriş yapılan log kayıtlarına ulaşma talebinin geri çevrilmesinin, kişinin kişisel verilerinin korunması hakkı kapsamında Anayasa'nın 40. maddesinde yer verilen etkili başvuru hakkının engellenmesine yol açtığı belirtilmiştir. Ayrıca başvurucunun ilk derece mahkemesine yapmış olduğu başvurunun, güncel bir yararın bulunmaması sebebiyle menfaat yokluğu gerekçesiyle reddedilmiş olmasıyla, etkili başvuru hakkının ihlal edildiğinden hareketle yargılamanın yenilenmesi gerektiğine karar verilmiştir.[443] İlgili kararda, kişinin trafik ve konum verisine ilişkin

[443] AYM, 2018/6161 Başvuru numaralı 28.06.2022 tarihli Karar; https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161 , Erişim Tarihi: 21 Aralık 2022.

bilgileri içeren log kayıtları ve açık Wi-Fi noktası kullanımına ilişkin verilerinin kişisel veri olduğu belirtilmiş olup; bu karar doğrultusunda yargı makamları tarafından incelenen trafik ve konum verilerinin işlenmesine ilişkin uyuşmazlıklarda, ilgili kararın önemle dikkate alınacağı düşünülmektedir.

7.2.4. Türk Hukukunda Trafik ve Konum Verilerinin Aktarılması

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(e) maddesinde, trafik ve konum verilerinin aktarılacağı hallerde, aktarım yapılacak verinin kapsamı, amacı, süresi ve aktarılacak olan üçüncü tarafın adı ve adresiyle birlikte üçüncü taraf yurt dışındaysa hangi ülkede bulunduğu konusunda bilgilendirme yapılmasının akabinde ilgili kişinin rızasının alınabileceğine ve söz konusu bilgilerin değişmesi halinde ise ilgili kişiden yeniden rıza alınması gerektiğine yer verilmiştir.

Trafik ve konum verisi aktarılmadan önce ilgili kişinin açık rızasının alınması hususuna ek olarak ise Kişisel Verilerin İşlenmesi Yönetmeliği'nin 8/1-(f) maddesinde belirtildiği üzere işletmeci, açık rıza alınmadan önce yapılan bilgilendirmede verilerin hangi taraflar ile paylaşılacağına yer verildiyse yalnızca onlara aktarılabileceğini ve bilgilendirmede belirtilen amaç doğrultusunda bu verilerin işlenmesini temin etmesi gerekmektedir.

EHK 51/8 maddesinde değinildiği üzere; acil durumlar halinde kullanıcının açık rızası bulunmasa bile kişinin kimlik ve konum verilerinin işlenebileceğine yer verilmiş olup; Elektronik Haberleşme Sektöründe Acil Yardım Çağrı Hizmetlerine İlişkin Yönetmelik'in[444] (Acil Yardım Yönetmeliği) 4. maddesinde belirtildiği üzere, GSM ve IMT-2000/UMTS[445] işletmecilerinin acil çağrı merkezilerine, kişinin konum ve kimlik bilgilerini iletme yükümlülüğü getirilmiştir. İlgili işletmeci tarafından, acil durumda olduğu düşünülen kişinin cihazında sim kartı takılı olmasa bile ilgili acil yardım çağrısını acil yardım merkezlerine iletmesi gerektiği belirtilmektedir.

Acil Yardım Yönetmeliği'nin 5. maddesinde ise işletmecinin, acil yardım çağrısında bulunan kişinin konumunu en az yüzde 90 doğru olacak şekilde belirlemesi ve üç ayda bir BTK'ya ortalama değerlerini bildirmesi gerektiği iletilmiştir.

---

[444] R.G. 05.06.2012, S. 28314.

[445] Hem karasal hem de uydu iletimini içeren hizmetleri sunan işletmecilerdir. (ETSI, "Satellite for UMTS/IMT-2000," etsi.org, https://www.etsi.org/technologies/satellite/satellite-umts-imt-2000 , Erişim Tarihi: 4 Ekim 2022.)

5651 sayılı Kanun'da 26 Şubat 2014'te yapılan değişiklik ile işletmecilerin bildirim yükümlülüklerinden bahsedilen 3. maddesindeki, işletmecilerin TİB'e verdiği trafik verilerinin hakimler tarafından talep edilmesi halinde TİB'in ilgili mercilere ileteceği hususundan bahsedilen 4. fıkra hükmünün iptali istenmiştir. Anayasa Mahkemesi kararında, söz konusu iptali istenen maddede belirtilen trafik verilerinin aktarılacağı ilgili mercilerin kim olduğunun net bir şekilde belli olmadığı, verilerin aktarım amacının sınırsız ve muğlak olduğu iddiasıyla, ilgili hükmün uygulanması halinde özel hayatın gizliliğinin ihlal edileceği, kişilerin açık rızası veya kanunda belirtilen hallerden herhangi biri olmadan ilgili trafik kişisel verisinin işlenmesinin Anayasa'nın 2., 13. ve 20. maddelerine aykırılık teşkil edeceğinden iptalinin gerektiği belirtilmiştir. Yapılan başvurunun incelenmesi neticesinde; Mahkeme de ilgili Anayasa hükümleri çerçevesinde, temel hakların özüne dokunulmamak kaydıyla, yalnızca zorunlu hallerde ve kanunla sınırlandırılabileceğine yer vererek; İnsan Hakları Evrensel Bildirgesi'nin 8. maddesi doğrultusunda, trafik verisinin iletişimin başlangıç ve bitiş zamanı, kişilerin kimlik bilgisi gibi hususları içermesi sebebiyle kişisel veri sayıldığına kanaat getirmiştir. Ayrıca Mahkeme, AİHM'in de kararlarında kişinin kişisel verilerinin rızası olmadan işlenmesi halinin her zaman özel hayatı ilgilendireceği düşüncesi bulunduğuna yer vermiştir. Dava konusu madde hükmünün, herhangi bir gerekçe gösterilmeksizin trafik verilerinin aktarılmasına olanak sağladığı ve bu verilere erişilmesi halinde kişilerin fikirleri, tercihleri ve hayatı hakkında ayrıntılı bilgilere erişilebilmesinin mümkün olduğu düşüncesi doğrultusunda; özel hayata müdahalenin mümkün olduğu kanaatine varmıştır. İlgili hükmün sınırlarının belirsiz olması sebebiyle keyfi müdahalelere karşı korunması gerektiği düşünülerek; Anayasa'nın 20. maddesine açıkça aykırılık teşkil ettiği belirtilerek söz konusu 5651 sayılı Kanun'un 3/4 maddesinin iptal edilmesine karar verilmiştir.[446]

İptal edilen ilgili 5651 sayılı Kanun'un 3/4 maddesinin, her ne kadar suçların önlenmesi amacıyla oluşturulduğu düşünülse de trafik verisinin hakim kararı doğrultusunda ilgili kuruma gönderilmesi işleminde hakim kararı ifadesinin çerçevesi belirli değildir. Bu durumda, hakim kararının içeriği ne olursa olsun herhangi bir sebep belirtilerek trafik verisinin istenmesi halinde de işletmeci tarafından ilgili trafik

[446] AYM, 2014/149 E., 2014/151 K. sayılı Kararı, https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-151-nrm.pdf , Erişim Tarihi: 4 Ekim 2022.

verilerinin sunulması gerekecektir. Trafik verisi, kişinin inisiyatifine bırakılamayacak kadar önemli bilgiler içermesi sebebiyle, ilgili iptal kararının yerinde olduğu düşünülmektedir.

7.2.5. Türk Hukukunda Trafik ve Konum Verilerinin Yurtdışına Aktarılması

Trafik ve konum verilerinin yurt dışına aktarılması hususu EHK'nın 51/6 maddesinde ayrıca düzenlenerek; kişisel verilerin yurtdışına aktarımı, KVKK ve ilgili diğer mevzuata uyulmasının yanı sıra ilgili kişinin açık rızasının alınması koşuluna bağlanmıştır. Kişisel Verilerin İşlenmesi Yönetmeliği'nin 5/2 maddesinde ise trafik ve konum verilerinin milli güvenlik sebebiyle yurt dışına çıkartılamayacağına yer verilmiştir. Görüldüğü üzere EHK ile Yönetmelik hükümleri birbiriyle çelişmektedir.

Her ne kadar EHK'nın 12/2 maddesinde belirtildiği üzere BTK'nın kişisel verilerle ilgili mevzuata uygun şekilde işletmecilere yükümlülük getirebileceğinden bahisle, BTK'nın düzenlediği Kişisel Verilerin İşlenmesi Yönetmeliği'ne getirilen ilgili 5/2 maddesinin EHK 51/6 maddesinden öncelikli olarak uygulanması gerektiğine dair farklı bir görüş[447] mevcut ise de normlar hiyerarşisine göre EHK, Kişisel Verilerin İşlenmesi Yönetmeliği'nden üstündür.

Yönetmelik hükümlerinin kanun hükmüne aykırı olmadan ve kanunun çizdiği sınırı aşmadan hükmün ayrıntılarını düzenlemesi beklenmekteyken; ilgili hususta yönetmelik hükmüyle kanun hükmünün sınırları aşılmıştır. Bu durumda, üst kademede olan kanuna uyumun hukuka uygun olacağı yönünde kanaat getirerek; trafik verilerinin ilgili kişinin açık rızası olması halinde yurtdışına aktarılabileceği söylenebilir.

Ayrıca ilgili Yönetmeliğin 5/2 maddesinde trafik ve konum verilerinin yurtdışına aktarılması yasaklanmış gibi görünse de aynı Yönetmeliğin 8/1-(f) maddesinde trafik ve konum verilerinin aktarılması için açık rıza alınması gerektiği hallerde, alınacak rızanın bilgilendirmesinde üçüncü tarafın yurtdışında bulunması halinde ülke adının da ilgili kişiyle paylaşılması gerektiği hususuna yer verilerek, aslında Yönetmeliğin de EHK 51/6 hükmü doğrultusunda yurtdışına aktarımı yasaklamadığı anlaşılmaktadır. Bununla birlikte, trafik ve konum verilerinin aktarılması konusunda ilgili Yönetmelik hükümlerinin kendi içerisinde çeliştiği de görülmektedir.

[447] Öztekin, Türk İnternet Hukuku, 177.

8. ABONELİK TESİSİNDEN SONRA ABONENİN KİŞİSEL VERİLERİNİN GÜNCELLENMESİ

Abonelik tesisinden sonra aboneliğin yetkilisine veya aboneliğin kurulduğu adrese ilişkin değişiklikler olabilmektedir. Abonenin değişiklik olan bilgileri işletmeciye bildirmesi, işletmecinin aboneye sunduğu hizmetin kalitesini etkileyeceği gibi, BTK'ya olan yükümlülüğünü yerine getirirken abone bilgilerinin doğru aktarılması açısından da önem arz etmektedir.

Yetkilendirme Yönetmeliği'nin 19/1-(a) maddesinde de yer verildiği üzere, işletmeci Kurum'a doğru ve eksiksiz şekilde bilgi vermekle yükümlü kılınmıştır. Aksi halde, İdari Yaptırımlar Yönetmeliği'nin 23/2 ve 24. maddeleri doğrultusunda öncelikle uyarma yaptırımı uygulanmakta; tekrarı halinde ise idari para cezası uygulanmaktadır.[448]

Ayrıca abone tarafından internet ve uydu hizmeti gibi adrese dayalı hizmet alımı söz konusuysa, adres değişikliği halinde abone tarafından eski adreste hizmet almaya devam edilemeyeceği için işletmeciye bu bildirimi yapması gerekmektedir.

Aboneliğin kuruluşu sırasında alınan evrakın işletmeciler tarafından saklanması yükümlülüğü olduğu gibi abonelik tesisinden sonra bu bilgilerde değişiklik olması halinde, ilgili değişikliğin BTK'ya gönderilen abone dosyalarında değiştirilerek gönderilmeye devam edilmesi gerektiğinden, bu yeni bilgilerin de artık aboneliğe ilişkin bilgiler olması hasebiyle işletmeci tarafından işlenmeye ve saklanmaya başlanması gerekmektedir.

Aboneler tarafından işletmecilere yapılacak olan bu bildirimlerde yeknesaklık olması ve eksik bilgi verilmesi sebebiyle abonenin talebine cevap verilememesi durumlarının bertaraf edilebilmesi amacıyla, işletmeciler tarafından genellikle bu işlemler için ayrı maktu formlar hazırlanmaktadır.[449] Bu formlar aracılığıyla talebini

---

[448] BTK Kurulu'nun 14.09.2021 tarih ve 2021/İK-YED/282 sayılı kararında, talep edilen bilgiyi göndermeyen işletmeciye idari para cezası uygulanmıştır. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-acentelik-ve-bilgi-verme-ile-ilgili-mevzuat-ihlali-high-speed/282-2021-web.pdf , Erişim Tarihi: 4 Ekim 2022.

[449] Netgsm A.Ş., Yetkili Değişikliği Formu, https://www.netgsm.com.tr/belgeler/formlar/netgsm-yetkili-degisikligi-formu.pdf ; TTNet A.Ş., İnternet Ek Hizmet Talep/Değişiklik Formu, https://bireysel.turktelekom.com.tr/evde-

işletmeciye ileten abonelerin doğrulanması amacıyla yine kişinin kimliğini ispatlamaya yarayan belgelerin abone tarafından sunulması gerekmektedir.

Elektronik ortamda kimlik doğrulamanın mümkün kılınmasıyla birlikte, artık bu bildirimler için gereksiz yere aboneden evrak istemenin önüne geçilerek; işletmecilerin tarafından fazla evrak alınması yoluyla bu verilerin de kişisel veriler kapsamında saklanması yükü altına girmeleri önlenmiş olacaktır.

9. RESMİ MERCİLERİN TALEPLERİNİN İŞLETMECİ TARAFINDAN KARŞILANMASI

İletişimi sağlayan araçların taşınabilir olmasıyla birlikte kullanımı yayınlaşmış ve uzakta olan kişiler arası iletişim ihtiyacı kolayca sağlanmaya başlamıştır. Hayatın her anında bu araçlar kullanılabildiği gibi adli vakaların gerçekleşmesi esnasında da kullanılmaktadır.

Haberleşmeyle ilgili bir olay olmasa bile iletişimin tespitiyle çözüm üretilebileceği veya araştırmaya katkı sağlayabileceği düşünülen durumların varlığından kaynaklı kamu kurum ve kuruluşları veya yargı makamları tarafından vakaların aydınlatılabilmesi için bazen iletişimin izlenmesi bazen de iletişimin kimler arasında gerçekleştiğinin tespitinin yapılması gerekmektedir. İletişimin izlenmesi yalnızca BTK tarafından yapılabilmekteyken; adli makamlar ve Ticaret İl Müdürlükleri tarafından iletişimi gerçekleştiren kişilerin kimliğinin tespiti veya kendileri tarafından bildirilen iletilerin gönderilip gönderilmediği gibi hususlar elektronik haberleşme sektöründeki işletmecilerden talep edilebilmektedir.

Adli makamlar tarafından başlatılan soruşturmalara esas olması açısından iletişimi gerçekleştiren kişilerin kimliğinin tespiti elektronik haberleşme sektöründeki işletmecilerden talep edilebilmektedir. Cumhuriyet savcılıkları, mahkemeler ve Cumhuriyet savcılığı emriyle emniyet müdürlükleri tarafından işletmecilerden abonelerinin abonelik sözleşmesinin aslı veya sureti, kimlik bilgileri, iletişim bilgileri, IP

internet/web/destek/internet/SozlesmeVeTaahhutnameler/INTERNET_EKHiZMET.pdf , Erişim Tarihi: 8 Ekim 2022.

log kaydı, port bilgisi, CDR kayıtları,[450] haberleşme hizmetini kullanmak amacıyla yapılan ödemelere ilişkin ayrıntılı bilgiler gibi konularda bilgi talep edilmektedir. 5271 sayılı Ceza Muhakemesi Kanunu (CMK)'nın[451] 332. maddesi uyarınca, işletmeciler tarafından bu talepler on gün içerisinde karşılanması gerekmektedir. Yetkili makamlarca istenilen bilgiye ilgili hükümde belirtildiği üzere, on gün içerisinde cevap vermeyen işletmeci hakkında ise Türk Ceza Kanunu (TCK)'nın[452] 257. maddesinde belirtilen görevi kötüye kullanma suçu kapsamında işlem yapılmaktadır. Bu sebeple elektronik haberleşme sektöründeki işletmeciler, diğer sektörlerdeki işletmecilere nazaran daha fazla sayıda ve daha uzun süre kişisel verileri işlemek zorunda kalmaktadır. İşletmecilerin bu kişisel verileri paylaşma suretiyle işleme faaliyetinin KVKK'nın 5/2-(ç) çerçevesinde, veri sorumlusunun hukuki yükümlülüğünü yerine getirmesi kapsamında olduğu söylenebilir.

Yalnızca adli soruşturmalara esas olması açısından değil, 6563 sayılı Kanun kapsamında gönderilen ticari elektronik iletilerin tespiti ve idari soruşturma başlatılabilmesi bakımından iletileri gönderenlerin tespiti için ticaret il müdürlükleri tarafından da elektronik haberleşme sektöründeki işletmecilerden bilgi talep edilmektedir. Ticari Elektronik İleti Yönetmeliği'nin 15/3 maddesinde, ticaret il müdürlükleri tarafından talep edilen bilgilerin, iletiyi gönderen hizmet sağlayıcı ve iletinin gönderilmesine aracılık eden aracı hizmet sağlayıcılar tarafından on beş gün içerisinde verilmesi gerektiği belirtilmektedir.

Rızası olmadan ticari elektronik ileti gönderilen tüketicilere, e-Devlet üzerinden şikayette bulunabilecekleri bir uygulama hazırlanmış olup;[453] bu sayfa üzerinden gelen şikayetler üzerine, yetkili makamlar tarafından İYS aracılığıyla, ticari elektronik iletilerin tüketicinin rızası dahilinde gönderilip gönderilmediğinin tespiti yapılmaktadır. Alıcının önceden rızasının alınmadığı durumların tespiti halinde, şikayete konu iletiyi gönderen

---

[450] Call Detail Records-Çağrı ayrıntı kaydı (CDR), bir telekom işlemi hakkında arama başlangıç saati, arama bitiş saati, arama süresi, görüşmenin tarafları, hücre kimliği, istenen web siteleri gibi ayrıntılı bilgileri içeren bir kayıttır. CDR, elektronik haberleşme sektörünün en değerli veri kaynağı olup; elektronik haberleşmeye ilişkin ücretlendirme ve faturalama, ağ verimliliği, dolandırıcılık tespiti, katma değerli hizmetler gibi temel süreçlerde kullanılmaktadır. (Sara B. Elagib, Aisha-Hassan A. Hashim, R. F. Olanrewaju, "CDR Analysis using Big Data Technology," International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering, 2015, 467, https://ieeexplore.ieee.org/document/7381414 , Erişim Tarihi: 9 Ekim 2022.)

[451] R.G. 17.12.2004, S. 25673.

[452] R.G. 12.10.2004, S. 25611.

[453] E-Devlet, Ticari Elektronik İleti Şikayet Sistemi, https://www.turkiye.gov.tr/gtb-ticari-elektronik-ileti-sikayet-sistemi , Erişim Tarihi: 9 Ekim 2022.

nümerik veya alfanümerik başlığa sahip abonenin kimlik bilgileri (T.C. kimlik no, ad, soyadı, unvan bilgileri) ve telefon, adres gibi iletişim bilgilerine ulaşılabilmesi amacıyla, iletinin gönderiminin sağlandığı işletmeciden bilgi istenmektedir. Ticari İleti Yönetmeliği'nin 15. maddesinde bahsi geçen sürecin işleyişine yer verilmiştir. Şikayete konu iletinin İYS tarafından incelenmesinin akabinde, ticaret il müdürlüğünün, konuyla ilgili bilgi ve belge talebinde bulunma sürecine geçilmektedir. Bu aşamada, il müdürlüğü tarafından hizmet sağlayıcı olan ve kendi ürünlerini pazarlamak adına ticari elektronik iletiyi gönderen şirketin kendisinden konuyla ilgili bilgi istenmekte veya aracı hizmet sağlayıcı olan işletmeciden şikayete konu iletiyi gönderen abonesinin bilgileri talep edilmektedir. İlgili hüküm kapsamında, on beş gün içerisinde cevabi yazının il müdürlüğüne gönderilmesi gerekmektedir. Bu süre, gerekli görüldüğü takdirde en fazla on beş gün daha uzatılabilmektedir. Bahsi geçen süre içerisinde gerekli bilgileri il müdürlüğüne teslim edemeyenler hakkında idari işlem başlatılmaktadır. Hizmet sağlayıcının talebiyle birlikte iletinin gönderimini sağlayan aracı hizmet sağlayıcıya İYS üzerinden bilgi sorulması halinde ise yine on beş gün içerisinde ilgili aracı hizmet sağlayıcı olan işletmeci tarafından sistem üzerinden cevap verilmektedir.

CMK'nın 135. maddesi uyarınca, adli amaçlı iletişimin tespit edilmesi, dinlenmesi ve kayıt altına alınması gibi görevleri bulunan Telekomünikasyon İletişim Başkanlığı (TİB), 671 sayılı KHK'nın[454] 22. maddesi uyarınca kapatılmış olup; görevleri BTK'ya devredilmiştir. Böylece BTK, 3 Temmuz 2005 tarihinde kabul edilen 5397 sayılı Kanun kapsamında önleyici ve istihbari amaçlı nitelikli hırsızlık ve dolandırıcılık, kasten öldürme gibi CMK'nın 135. maddesinde sayılan suçlar hakkında iletişimi tespit ederek; dinleme ve kayda alma ile sinyal bilgilerinin değerlendirilmesi işlemlerini gerçekleştirebilmektedir.

İletişimin tespit edilmesi, dinlenme ve kayda alınma işlemlerinin kişisel verilerin işlenmesi anlamına geldiği açıktır. Lakin KVKK'nın 28/1-(ç) maddesinde belirtildiği üzere; kamu, ekonomik ve milli güvenliğin sağlanması üzere kanun tarafından yetkilendirilmiş kamu kurum veya kuruluşlarının gerçekleştirilen koruyucu, önleyici ve istihbari çalışmalar doğrultusunda işleme faaliyetleri istisnai hallerden biri olarak sayılmış olup; KVKK kapsamı dışında tutulmuştur. Bir başka deyişle, BTK, kendisine kanunla verilen önleyici ve istihbari görevleri yerine getirmek adına kişisel verileri

[454] R.G. 17.08.2016, S. 29804.

işlediğinden; bu faaliyetleri KVKK kapsamı dışında değerlendirilerek kişisel verilerin korunması bağlamında BTK'ya herhangi bir yükümlülük getirilmediği söylenebilir.

BÖLÜM 3

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İMHA EDİLMESİNE KADAR GEÇEN SÜREÇ VE DEĞERLENDİRİLMESİ

1. ELEKTRONİK HABERLEŞME SEKTÖRÜNDEKİ İŞLETMECİDEN BİLGİ TALEP EDİLMESİ

Teknolojide yaşanan gelişmelerle birlikte, internet hızları giderek artmaktadır. Bu artışla birlikte, bireyler arası iletişimden nesneler arası iletişime kadar hayatın neredeyse her alanında internetin kullanımı giderek yaygınlaşmaktadır. Uluslararası Telekomünikasyon Birliği tarafından yapılan araştırma, dünya nüfusunun yarısından fazlasının internet kullandığını göstermekle birlikte; ülkemizde ise internet kullanan abone sayısının BTK tarafından yapılan araştırmaya göre, 2008 yılında yaklaşık 6 milyon olduğu, 2020 yılı itibarıyla ise 78 milyonu geçtiği belirtilmiştir. Ayrıca Türkiye İstatistik Kurumu (TÜİK) tarafından 16-74 yaş arası internet kullanımının yüzde 79 olduğu belirtilmiştir.[455] İnternetin akıllı telefonlar vasıtasıyla kullanımının yaygınlaşmasıyla da mobil abone sayısında her geçen gün artış yaşanmakta olup; 2022 yılı itibarıyla 4.5G abone sayısının 82 milyonu aştığı tespit edilmiştir. Buna karşılık, sabit telefon abone sayısı ise giderek azalmakta olup[456]; 2022 yılı itibariyle 11,5 milyon civarında sabit telefon abonesi bulunmaktadır.[457]

Bahsi geçen istatistiki verilerden elektronik haberleşme sektöründeki hizmetlerin ülkemizdeki kullanımının artış gösterdiği çıkarımı yapılabilmektedir. Hizmetlerin kullanımının artmasıyla, kişisel verileri işleme faaliyetlerinin de artacağı bir gerçektir. Bu

[455] Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 11, http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf , Erişim Tarihi: 11 Ekim 2022.
[456] BTK, Türkiye Elektronik Haberleşme Sektörü 2022 yılı 2. Çeyrek Üç Aylık Pazar Verileri Raporu, 55, https://www.btk.gov.tr/uploads/pages/pazar-verileri/2022-2-kurumdisi.pdf , Erişim Tarihi: 11 Ekim 2022.
[457] BTK, 2022/2 Üç Aylık Pazar Verileri Raporu, 32.

sebeple tüm dünyada kişisel veri işlemenin ne şekilde olması gerektiği, verilerin ve mahremiyetin korunması, işleme faaliyetiyle ilgili bilgilendirme ve bilgi alma süreçlerinin nasıl ilerlemesi gerektiğine ilişkin bir dizi düzenleme yapılmaya başlanmıştır.

Bir veri sahibinin kendi kişisel verilerine ve verilerinin işlenme şekline ilişkin bilgilere erişim hakkı vardır. AB düzenlemelerinde belirtilen bu hak, AB veri koruma yasasının temelini oluşturmaktadır. Erişim hakkı doğrultusunda, verilerin sahibine anlaşılır bir biçimde ya da elektronik ortamda işlendiği durumlarda ise elektronik biçimde iletilmesi gerekmektedir. Bireylerden gelen bu tür taleplerin gecikmeden veya bireye yüksek ücrete mal olmadan yerine getirilmesi gereklidir. Taleplerin açıkça aşırı olduğu ve veri sorumlularının talep edilen bilgileri sağlamaları için gerekli olan idari maliyetleri dikkate alınarak hesapladıkları makul bir ücretin talep edilebileceği durumlar dışında, bireylerden elektronik ortamda gelen bilgi taleplerinin ücretsiz olarak karşılanması gerekmektedir.[458]

Ülkemizde de kişisel verilerin korunmasına verilen önem arttıkça, verisi işlenen ilgili kişilerin de bu konuda Anayasa tarafından korunacak temel haklarına ilişkin düzenleme yapılma ihtiyacı ortaya çıkmıştır. Söz konusu ihtiyaç ve uluslararası düzenlemelere uyum sağlayabilmek amacıyla, 5982 sayılı Kanun[459] ile yapılan değişiklik üzerine Anayasa'nın 20. maddesine getirilen 3. fıkrasında, bireylerin kişisel verilerinin korunmasını, değiştirilmesini, silinmesini talep etme, hangi kişisel verilerinin işlendiği konusunda bilgilendirilme, bilgilendirildiği amaç dahilinde işlenip işlenmediğini sorgulama, verilerine ulaşabilme hakkına sahip olduğu belirtilmektedir. Ayrıca kişisel verilerin yalnızca kanunda belirtilen durumlarda ya da ilgili kişinin açık rızasının bulunması halinde işlenebileceğine yer verilmiştir. Bununla birlikte, bilgi edinme hakkına yer verilen bir diğer hüküm de herkesin bilgi edinme ve kamu denetçisine başvurabileceğine ilişkin Anayasa'nın 74. maddesidir.

Elektronik haberleşme sektöründeki işletmeciler, ilgili hükümler dolayısıyla kişisel verilerini işledikleri abonelere veya kullanıcılara bilgi vermekle ve ilgili kişilerin bilgi talep edebilmesi için gerekli kanalları sağlamakla yükümlüdür.

[458] Lynskey, Data Protection Law, 181-182.
[459] R.G. 13.05.2010, S. 27580.

KVK Kurulu'nun 29.09.2020 tarih ve 2020/746 sayılı kararına konu olan olayda, ilgili kişinin abonelik sözleşmesi ilişkisinden kaynaklı aldığı hizmetle ilgili yaşanılan uyuşmazlık sebebiyle veri sorumlusu ile abone olmak isteyen kişi arasında gerçekleştirilen ses kayıtlarının ve görüşmelere ilişkin tarih bilgisini içeren detayların kişisel veri olduğu iddiasıyla kayıtlı elektronik posta (KEP) adresi aracılığıyla abone adayı tarafından gönderilen talep karşısında ilgili kayıtların kendisine verilmediğini belirten abone adayı, konunun incelenmesi amacıyla KVK Kurumu'na başvuruda bulunmuştur. Veri sorumlusunun, KVK Kurumu'na gönderdiği savunmada; ilgili kişi tarafından veri sorumlusuna ait olan KEP adresine gönderilen talebin, söz konusu KEP adresinin kişisel verilerle ilgili bilgi talep edilebilecek uygun kanal olmadığı, kişisel verilere dair taleplerin gönderildiği ayrı bir KEP adresi olmaması sebebiyle de kendilerine ait internet sitesi ya da ana ortaklığın KEP adresi üzerinden bu başvurunun gönderilmesi gerektiği belirtilerek, ilgili kişinin talebini gönderdiği kanalın yanlış olduğu ileri sürülmüştür. KVK Kurulu ise bu konuda, veri sorumlusunun kendisine ait KEP adresi üzerinden bu türden taleplerin karşılanabilmesi için gereken düzenlemeleri yapması gerektiği yönünde karar vermiştir. Veri sorumlusunun savunmasında belirttiği bir diğer husus ise kurulan abonelik sözleşmesi sebebiyle bazı kişisel verilerin elde edildiği ve ilgili kişinin kişisel verilerinin KVKK 5/2-(c) maddesi doğrultusunda, sözleşmenin kurulması ya da ifasıyla ilgili olarak işleme faaliyetinin gerçekleştirilmiş olmasına ilişkindir. Bununla birlikte, veri sorumlusunun müşteri hizmetleri ile abonenin ses kayıtlarını içeren kişisel verilerinin paylaşılmasının farklı amaçlarla kullanılabilmesi ihtimali ve ilgili ses kayıtlarının müşteri hizmetleri çalışanının da kişisel verisini içermesi sebebiyle, kişisel verilerin korunması açısından farklı sonuçların ortaya çıkma durumu düşünülerek paylaşılmadığı belirtilmiştir. Bu açıklamalar karşısında KVK Kurulu, Anayasa'nın 20. maddesi çerçevesinde, kişilerin kişisel verilerinin korunmasını talep etme hakkının anayasal hak olduğunu, kişinin işlenen verilerine erişebilmesinin ve tam olarak bilgilendirilmesinin de bu kapsamda yer aldığını belirtmiş; ayrıca KVKK'nın 11/1-(b) maddesi uyarınca ilgili kişinin kişisel verileriyle ilgili bilgi isteyebileceğine ilişkin hakkının olduğunu vurgulamıştır. Bu doğrultuda Kurul, müşteri hizmetleri çalışanın kişisel verilerine, aboneye bilgi verilme sırasında yer vermeden ya da maskeleme yapılarak tedbirlerin alınabileceğini, ses kayıtlarının kendisi yerine dökümlerinin de ilgili kişiyle paylaşılabileceğini belirtmiştir. Diğer taraftan, ilgili kişinin kişisel verilerine dair

veri sorumlusundan bilgi talep etme hakkı bulunsa da veri sorumlusu tarafından teknik imkanlar ölçüsünde veri güvenliği de göz önünde bulundurularak ancak veriye makul şekilde ulaşılabilir olmasına imkan tanınarak; bu hakkın kullanılması gerektiği KVK Kurulu tarafından vurgulanmıştır.[460]

İlgili karardan anlaşılacağı üzere; işletmeci tarafından kişinin bilgi edinme hakkına önem verilmesi ne kadar elzem olsa da bu hak doğru kanaldan talep edilmediği takdirde hakkın kullanımı mümkün olmamaktadır. Bu sebeple öncelikle hangi konularda bilgi talep edilebileceğinden bahsedildikten sonra, bilgi talep edilebilecek kanallar ve işletmecilerin bu taleplere cevap verme süreçleri incelenecektir.

1.1. ABONE VEYA KULLANICININ BİLGİ TALEP EDEBİLECEĞİ HUSUSLAR

İlgili kişinin kişisel verilerine erişim hakkı, diğer bir ifadeyle bilgi talep etmesine, 95/46/EC sayılı Direktif'in 12. maddesinde yer verilmiş olup; verilerin işlenip işlenmediği, hangi amaçlarla işlendiği, verilerin aktarıldığı alıcı kategorileri, eksik veya yanlış olan verilerin düzeltilmesinin talep edilmesi gibi hususlar bu hak kapsamına dahil edilmiştir.

GDPR ise 63. başlangıç paragrafında erişim hakkını, 95/46/EC sayılı Direktif'e göre daha ayrıntılı şekilde incelemiş olup; ilgili Direktif'te yer verilen konuların dışında kişinin kendi sağlık verilerine ulaşabilmesinin de bu hak kapsamında olduğu belirtilmiştir. Bunun yanı sıra gerektiğinde erişim hakkı kullanımının, başkalarına ait fikri mülkiyet ve yazılımların korunması gibi hakların da korunması amacıyla sınırlandırılabileceğine yer verilmiştir.[461]

İlgili kişi, kişisel verilerine her daim ulaşabilmeli, üzerinde söz sahibi olabilmeli ve verilerinin geleceğini belirleyebilir olmalıdır. Söz konusu fiilleri gerçekleştirmenin yolu ise ilgili verilere erişebilir olmaktan geçmektedir.[462]

Her alanda olduğu gibi elektronik haberleşme alanında da abone veya kullanıcılar tarafından kişisel verilerine erişme talebiyle, bu konuda bilgi edinme hakları kullanılmaktadır. İç hukukumuzda, elektronik haberleşme sektörünü düzenleyen 5809

---

[460] KVK Kurulu'nun 29.09.2020 tarih ve 2020/746 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6954/2020-746 , Erişim Tarihi: 11 Ekim 2022.
[461] Küzeci, Kişisel Verilerin Korunması, 254.
[462] Dülger, KVK Hukuku, 476.

sayılı EHK ve buna bağlı olarak kişisel verilerin işlenmesine yönelik ayrıntılı hükümlere yer verilen Kişisel Verilerin İşlenmesi Yönetmeliği'nde ilgili kişi olan abone ve abone adaylarının bilgi edinme haklarına yönelik özel bir hüküm yer almamaktadır. Bu sebeple elektronik haberleşme sektöründe bilgi edinme hakkı konusunda genel nitelikteki KVKK hükümleri uygulanmaktadır.

KVKK'nın 11. maddesinde ilgili kişinin hangi konularda bilgi talep edebileceğine ilişkin hüküm yer almaktadır. Herkesin kişisel verilerinin işlenip işlenmediği, hangi verilerinin işlendiği, işleme amaçlarının ne olduğu ve belirtilen amaçlar dahilinde kullanılıp kullanılmadığını sorgulama, verilerin aktarıldığı üçüncü kişilerin kimler olduğunu öğrenme, eksik ya da yanlış şekilde işleme varsa bunun düzeltilmesini talep etme hakkı bulunmaktadır. Ayrıca hükmün devamında belirtildiği üzere ilgili kişinin, işleme faaliyetinin hukuka uygunluk sebeplerinin ortadan kalkması durumunda verilerinin silinmesini veya yok edilmesini isteme, bahsi geçen düzeltme veya silme faaliyetlerinin gerçekleştirilmesi halinde verilerin aktarıldığı üçüncü kişilere bilgi verilmesini talep etme, verilerinin özellikle otomatik işleme faaliyetleriyle analiz edilmesi sonucunda ilgili kişi aleyhine bir sonuç ortaya çıkıyorsa buna itiraz etme ve hukuka aykırı işleme faaliyeti sebebiyle ilgili kişi zarara uğradıysa bunun tazminini isteme amaçlarıyla veri sorumlusuna başvurma hakkının olduğuna yer verilmiştir.

Elektronik haberleşme sektöründeki hizmetlerden faydalananlar, bahsi geçen KVKK hükmü doğrultusunda sıklıkla işletmecilere başvurmaktadır. Aboneler özellikle, abonelik feshi talebinde bulunduktan sonra taleplerinin karşılanıp karşılanmadığı, ilgili işletmecilerde abonenin kendisinin adına kayıtlı aboneliğinin bulunup bulunmadığı, aboneliği vasıtasıyla gerçekleştirmiş olduğu iletişimin CDR kayıtları gibi ayrıntılara veya abone adına düzenlenen faturaların içeriğine ilişkin detaylı bilgi alma amacıyla işletmecilerden bilgi talep edebilmektedir.

1.2. VERİ SAHİBİ BAŞVURU FORMU

Elektronik haberleşme sektörü, abonelik tesisinden başlamak üzere özellikle hizmetin kullanımından kaynaklı kişisel verilerin çokça oluştuğu ve işletmeciler tarafından mevzuat kapsamında işlenmek zorunda kalındığı bir sektördür. Bu sebeple diğer sektörlere nazaran ilgili kişiler, yerine göre veri sorumlusu ve veri işleyen sıfatı değişmekte olan işletmecilere sıkça başvurmaktadır. Dolayısıyla da kişisel verilerin

işlenmesi ve korunması kavramları kullanılmaya başlandığı andan itibaren işletmecilerin işletmelerini bu sürece uyumlaştırma gerekliliği ortaya çıkmış olup; KVKK'ya uyumlu işletmecilik anlayışı hızla yerleşmeye başlamıştır.

İşletmeci tarafından bilgi talep eden aboneye cevap vermek ne kadar önemliyse, doğru şekilde anlaşılan talebin yine doğru şekilde cevaplanması da bir o kadar önemlidir. Bu noktada, veri sahibi ya da ilgili kişi başvuru formu olarak da adlandırılan formlar, bilgi edinme hakkını kullanmak isteyen kişilerin taleplerinin işletmeciler tarafından daha net anlaşılabilmesine olanak sağlamaktadır.

Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'de[463] (Veri Sorumlusuna Başvuru Tebliği) veri sorumlusuna başvuru usulleri ve söz konusu başvuruya yanıt verebilme işleminin veri sorumlusu açısından maliyet gerektirmesi durumunda alınabilecek ücretlere ilişkin açıklamalara yer verilmiştir. Söz konusu Tebliğ'in 5/2 maddesinde, ilgili kişi tarafından yapılacak olan başvurunun içeriğinde asgari bulunması gereken hususların; başvuranın kimlik bilgileri ve iletişim adreslerinin yanı sıra talep konusu olduğu belirtilmiştir.

Veri Sorumlusuna Başvuru Tebliği'nin 5/2 maddesinde asgari olarak belirtilen hususlar doğrultusunda elektronik haberleşme sektöründeki işletmeciler tarafından veri sahibi başvuru formları hazırlanmaktadır. Bu formlarda genel olarak; kişisel verisi işlenen ve bilgi edinmek isteyen kişiye ait kişisel ve iletişim bilgilerinin yanı sıra işletmeciyle bilgi edinmek isteyen kişinin arasındaki hukuki ilişkiye dair nitelendirmenin ve işletmeciden ilgili kişinin kişisel verisiyle ilgili bilgi talep edilen hususun ne olduğu konusunda bilgilerin yer aldığı bölümler bulunmaktadır. Ayrıca ilgili 5/2 hükmünün devamında, veri sahibi başvuru formunun hangi kanallardan işletmeciye ulaştırılması gerektiğine yer verilmektedir. Bilgi edinme talebinde bulunulmasının akabinde, işletmeci tarafından açıklamanın yapılabilmesinde gerekli ise veri sahibinden konuyla ilgili bazı bilgiler talep edilebileceğine dair bilgilendirmenin ilgili formda yer alması gerekmektedir. Bununla birlikte veri sahibi başvuru formlarında, söz konusu bilgi talebine ne kadar süre içerisinde cevap verileceği bilgisine yer verilmektedir.[464] İşletmeciler, başvuru formlarını internet sayfasında hazır bulundurarak; abone veya kullanıcıların forma kolay bir şekilde ulaşmalarını sağlamaktadır. Son olarak, Veri

[463] R.G. 10.03.2018, S. 30356.
[464] Netgsm A.Ş., Başvuru Formu, https://www.netgsm.com.tr/belgeler/formlar/netgsm-ilgili-kisi-basvuru-formu.pdf , Erişim Tarihi: 11 Ekim 2022.

Sorumlusuna Başvuru Tebliği'nin 5/3 maddesinde, başvuranın bilgi talebinde bulunurken; talebine ilişkin sunabileceği varsa bilgi ve belgenin de başvuruya ilave edilmesi gerektiğinden bahsedilmiştir.

1.3. BİLGİ TALEP EDİLEBİLECEK KANALLAR

Veri Sorumlusuna Başvuru Tebliği'nin 5. maddesinde veri sorumlusuna başvuru yöntemleri sınırlı sayıda sayılmıştır. Veri sahibi, işletmeciye bizzat giderek yazılı olarak talepte bulunabileceği gibi, elektronik ya da mobil imza kullanarak işletmecinin KEP adresine göndereceği ileti yoluyla veya veri sahibi tarafından işletmeciye daha önceden bildirerek kaydettirdiği e-posta adresine ileti gönderme suretiyle söz konusu başvuru işlemini hukuka uygun şekilde gerçekleştirmiş sayılabilecektir. Veri sahipleri, veri sorumlusu tarafından verisini işlediği kişilere sunulan yazılım ya da uygulamalar kullanılmak suretiyle de bilgi edinme taleplerini iletebilir.

Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin vermiş oldukları hizmetin haberleşme gibi temel bir hakka dayanması nedeniyle halihazırda birçok yükümlülüğünün olması ve bu sektörün teknolojiyle iç içe olması hali, işletmecilerin sürekli olarak yeni düzenlemelere uyumlaştırmaya açık olan işletmecilik anlayışları, başvuru kanallarına değinilen ilgili hükümdeki kanalların tamamının aboneye sağlanması aşamasında zorluk çekmemelerine sebep olmaktadır.

Veri Sorumlusuna Başvuru Tebliği'nin 5. maddesindeki veri sorumlusu tarafından veri sahibinin başvurması amacıyla geliştirilen yazılım veya uygulama ile başvuru imkanının sağlanması, elektronik haberleşme sektöründeki işletmecilerin hemen hemen hepsinin kendi hizmetlerini sunduğu bir ara yüz geliştirmiş olmaları sebebiyle kolaylıkla uyum sağlayıp; abonelerine sunabileceği bir başvuru kanalı yöntemidir. Nitekim uygulamada işletmecilerden bazıları bilgi edinmek isteyen abonelerini kendi ara yüzleri üzerindeki kişisel verilerle ilgili bilgi edinme bölümüne yönlendirerek; "4. Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunmasına Yönelik Alınan Teknik ve İdari Tedbirler" başlığı altında ayrıntılı şekilde yer verilecek olan arayüze girişin iki aşamalı doğrulama vasıtasıyla[465] yapılabilmesi sayesinde, talepte bulunan kişinin kimliğini de doğrulayarak; yetkisiz kişilere bilgi verilmesinin önüne geçilmek amaçlanmaktadır.

[465] Turkcell İletişim Hizmetleri A.Ş., https://hizligiris.com.tr/hizligiris/generic/sms_otp , Erişim Tarihi: 14 Ekim 2022.

Bilgi talep eden veri sahiplerinin bu taleplerini veri sorumlularına ilettikleri kanalın ne denli önemli olduğuna KVK Kurulu, 01.10.2019 tarihli ve 2019/296 sayılı kararında, internet sitesinden ilgili kişinin yaptığı başvuruyu kimlik teyidi gerçekleştiremediğini öne sürerek reddeden operatör şirket hakkında KVK Kurulu'na yapılan başvuruda, ilgili kişi internet üzerinden bireysel faturalı telekomünikasyon hizmeti aldığı operatör şirkete KVKK başvuru formunu doldurarak göndermiştir. Veri sorumlusu operatör, KVKK talep formunu, Veri Sorumlusuna Başvuru Tebliği'ne uygun olarak hazırladığını belirtmiştir. Kurum ayrıca kişilerin kimlik tespitini yapabilmek amacıyla ilgili kişiye noter ya da elektronik imzalı posta gibi kanallarla şirket adresine bu formların gönderilmesi gerektiğini ifade etmiş; elektronik ortamda gönderilen KVKK formunun söz konusu formata uygun olmadığına yer vermiştir. KVK Kurulu, ilgili kişinin sahip olduğu hakları vurgulayarak; öncelikle ilgili kişinin KVKK'nın 13. maddesi kapsamında kişinin taleplerini yazılı şekilde ya da KVK Kurulu'nun belirleyeceği yöntemlerden biri ile iletmesi gerekliliğine değinmiştir. Bununla birlikte, Veri Sorumlusuna Başvuru Tebliği'nin 5. maddesinde sayılan başvuru kanallarından biri ile başvurunun yapılmasının yanı sıra söz konusu Tebliğ'in 6. maddesine göre, veri sorumlusunun bu başvuruyu hukuka ve dürüstlük kuralına aykırı olmadan cevaplandırmakla yükümlü olduğundan söz etmiştir. Bu doğrultuda KVK Kurulu, kimlik teyidi için ilgili kişinin farklı şekilde yönlendirilerek uygun bir başvuru yapmasının önüne geçilmeye çalışılmasının Veri Sorumlusuna Başvuru Tebliği'nin 5. ve 6. maddelerine uygun olmayacağını belirterek; operatör şirketin gerekli dikkat ve özeni göstermesi gerektiğini hatırlatmıştır.[466]

İlgili karar doğrultusunda görülmektedir ki; elektronik haberleşme sektöründe, özellikle iletişim hizmeti verilmesi nedeniyle kimlik teyidi aşaması, bu sektörde abone ile işletmeci arasında yapılan tüm işlemlerde olduğu gibi veri sahibinin bilgi talebine cevap verilmesi sürecinde de büyük önem taşımaktadır. Veri sahiplerine verilen cevabın kişisel veri içermesi sebebiyle kimlik teyidi yapılmadan veri sorumlusundan cevap vermesi beklenemeyeceğinden; Kurul'un vermiş olduğu kararın yerinde olduğu düşünülmektedir. Diğer sektörlerden farklı olarak; elektronik haberleşme sektöründeki işletmeciler, yeni abonelik tesisi veya başvurusu için kullanmaya başladıkları kimliğin

[466] KVK Kurulu'nun 01.10.2019 tarihli ve 2019/296 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6557/2019-296 , Erişim Tarihi: 14 Ekim 2022.

uzaktan doğrulanması yöntemleri sayesinde, bilgi talep eden veri sahibinin kimliğinin doğrulanması aşamasını bu yöntemlerden biri ile gerçekleştirmeye başlayacakları düşünülmektedir. Böylece bu sürecin belki de en önemli ve zor kısmı olan kimlik teyidi aşaması daha hızlı ve doğru şekilde tamamlanabilecektir.

1.4. TALEP EDİLEN BİLGİYE CEVAP VERME SÜRECİ

Veri sahibinin kişisel verileriyle ilgili bilgi taleplerini veri sorumlusuna yönlendirmesi hususunda mevzuatta bir usul öngörüldüğü gibi veri sorumlusu tarafından bu taleplerin karşılanması aşamasında da izlenmesi gereken bir usul vardır. Veri Sorumlusuna Başvuru Tebliği'nin 6. maddesinde veri sahibinin yaptığı başvuruya nasıl yanıt verilmesi gerektiği belirtilmiştir. İlgili hükümde ilk vurgulanan husus, veri sahibi tarafından yapılan başvurulara karşı hukuka ve dürüstlük kuralına uygun şekilde işlem gerçekleştirilebilmesi için veri sorumlusu tarafından teknik ve idari tedbirlerin alınması gerekliliğidir. Bahsi geçen ikinci husus ise veri sahibi tarafından kişisel verileriyle ilgili bilgi talep edilmesi halinde veri sorumlusunun cevap verme zorunluluğuna ilişkin olup; bu cevap, başvuruyu reddetmeye yönelik olumsuz bir cevap olsa da ilgili kişiye bununla ilgili bir dönüş yapılmalıdır.[467] Ayrıca ilgili hükmün 3. fıkrasında, veri sorumlusu tarafından verilecek olan cevap, başvurunun şekline göre yazılı olarak veya elektronik ortamda gönderilebilecek olup; genellikle başvuru sahibine cevabın kendisine nasıl gönderilmesini istediği sorularak bu konuda da başvuru sahibinin talebinin uygun şekilde karşılanması sağlanmaktadır.

Cevap yazısında bulunması gereken temel unsurlar, Veri Sorumlusuna Başvuru Tebliği'nin 6/4 maddesinde belirtilmiş olup; veri sorumlusuna ilişkin bilgiler, başvurucuya ilişkin kimlik ve iletişim bilgileri, talep konusu ve veri sorumlusunun konuya dair cevaplarının neler olduğu cevap yazısında bulunmalıdır.

Aynı Tebliğ'in 6/5 maddesinde yer verildiği üzere, veri sorumlusuna bilgi talebinde bulunan başvurucunun talebinin olabildiğince kısa sürede cevaplanması gerekirken; bu süre en fazla otuz gün olarak belirlenmiştir. Tebliğ'de bu süre azami olarak belirlenmiş olup; veri sorumlularının bu süreye uyması beklenmektedir.

---

[467] KVK Kurulu'nun 16.02.2021 tarih ve 2021/1262 sayılı kararında, veri sorumlusu tarafından veri sahibine bilgi verilemeyecek bile olsa buna ilişkin gerekçeyi belirten bir cevap verilmesi gerektiği belirtilmiştir. https://www.kvkk.gov.tr/Icerik/7287/2021-1262 , Erişim Tarihi: 14 Ekim 2022.

Elektronik haberleşme sektöründe, abonelerin bilgileri elektronik ortamda ve BTK mevzuatına uygun şekilde tutulmakta olduğundan; ayrıca abone bilgilerinin işlenme ve saklanmasına yönelik yine Kurum tarafından planlı ve plansız birtakım denetimlerin yapılması ve özellikle yargı makamlarından abone bilgilerinin talep edildiği yazıların cevap sürelerinin kısa olması sebebiyle; genellikle elektronik haberleşme sektöründeki işletmeciler bilgi talep edilen yazılara ivedilikle cevap vermek durumunda kalmaktadır. Bu nedenle elektronik haberleşme sektöründeki işletmeciler için otuz günlük azami sürede cevap vermek sorun teşkil etmemektedir.

Veri sahibi, talepte bulunduğu bilgilerin veri sorumlusu tarafından yazılı olarak cevaplanmasını istediği takdirde; istenen bilginin yazılı halde sunulması elektronik ortamda sunulmasına göre daha fazla maliyetli olabilmektedir. Özellikle elektronik haberleşme sektöründe, aboneliğe ilişkin belirli tarihler arasındaki CDR kayıtları veya hangi internet sayfalarının ziyaret edildiğine ilişkin bilgilerin yazılı olarak kağıt ortamında sunulabilmesi için veri sorumlusunun sayfalarca kağıt maliyetine katlanması gerekmektedir.

Kişisel verileriyle ilgili bilgi talep etme hususu, ilgili kişinin hakkı, veri sorumlusunun ise yükümlülüğü olsa da talep edilen bilginin veri sorumlusu tarafından maliyetine katlanılmasını beklemek adil bir durum olmayacağından; Veri Sorumlusuna Başvuru Tebliği'nin 6/5 ve 7. maddesinde, başvuru sahibinden alınabilecek ücrete ilişkin ayrıntılı bir düzenlemeye yer verilmiştir. Bu hükümler uyarınca, başvuruya yazılı olarak cevap verilmesi halinde, veri sorumlusu tarafından onuncu sayfadan sonraki her bir sayfanın 1-TL olarak ücretlendirilebileceği belirtilmiştir. İlgili hükümler çerçevesinde, değinilen bir diğer husus ise veri sorumlusunun hatası sebebiyle veri sahibinin başvurma durumu hasıl olmuşsa, alınan bu ücretin veri sahibine iade edilmesi gerekmektedir. Ayrıca ilgili Tebliğ'in 7. madde hükmünde, cevabın CD veya flash bellek benzeri bilgiyi depolamaya yönelik araçlar vasıtasıyla gönderilmesi halinde ise başvuru sahibinden en fazla söz konusu kaydı almaya yarayan aracın maliyetine tekabül eden ücretin alınabileceğine yer verilmiştir.

2. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN SAKLANMASI

Kişisel verilerin hukuka uygun işlenmesi, verilerin hukuka uygun şekilde toplanması, saklanması, diğer işleme faaliyetleri gerçekleştirildikten sonra ise yine hukuka uygun şekilde ve zamanda imhasını kapsamaktadır.[468]

Veri toplama ve işleme kriterlerinin artık daha katı olduğu herkesçe bilinmektedir. Dolayısıyla kişisel verileri saklamanın getirdiği riskler de genellikle eskisinden daha fazladır.[469] Veri sorumluları ve işleyenler de verilerin korunamaması veya yanlış işlenmesinin ciddi sonuçlar doğurabileceğinin farkında olması gerekmektedir. Verilerin korunamaması veya yanlış işlenmesi gibi durumların ortaya çıkması halinde, işletmecilerin iş kaybı yaşamaları, itibarlarının zedelenmesi, satışların azalması, ticari faaliyetlerinin durdurulması gibi ciddi işletmesel sorunların yanı sıra idari para cezalarıyla karşı karşıya kalmaları mümkündür.[470]

2.1. AB MEVZUATI VE 2006/24/EC SAYILI VERİ SAKLAMA DİREKTİFİ ÇERÇEVESİNDE KİŞİSEL VERİLERİN SAKLANMASI

2.1.1. 2006/24/EC Sayılı Veri Saklama Direktifi'nin Ortaya Çıkışı

Avrupa'da teröre ilişkin güvenlikle ilgili endişeler, Madrid ve Londra'da gerçekleşen terör eylemleri[471] sonrasında artış göstererek, güvenlik zafiyeti doğuran suçların soruşturulması, tespit edilmesi ve kovuşturulması amacıyla kullanılabilmesi adına verilerin korunmasının yanı sıra saklanmasının da ayrıca düşünülmesi gerektiği fikri yaygınlaşmaya başlamıştır.[472]

---

[468] Determann, *KVK Uygulama Kılavuzu*, XV.
[469] Paul Lambert, *The Data Protection Officer Profession, Rules, and Role*, (Boca Raton: CRC Press - Taylor & Francis, 2017), 119.
[470] Lambert, *Data Protection Officer*, 120.
[471] BBC News, Madrid Train Attacks, http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/. Erişim Tarihi: 16 Ekim 2022; BBC News, Bomb Attacks on London, http://news.bbc.co.uk/onthisday/hi/dates/stories/july/7/newsid_4942000/4942238.stm . Erişim Tarihi: 16 Ekim 2022.
[472] Arianna Vedaschi, Valerio Lubello, "Data Retention and Its Implications for the Fundamental Right to Privacy A European Perspective," *Tilburg Law Review* 20, (2015): 18.

AB üyesi devletlerde verilerin saklanmasına ilişkin farklılık teşkil eden bağlayıcı nitelikteki düzenlemelerin, kolluk kuvvetlerinin verilere erişimini sınırlayarak; organize suç ve terörizmi önleme ve bunlarla mücadeleyi sekteye uğrattığı gerekçesiyle, veri saklamaya ilişkin düzenlemelerin AB genelinde birbirleriyle uyumlu hale getirilmesi gerektiği savunulmuştur. 2002/58/EC sayılı Direktif sonrasında AB'nin elektronik haberleşme sektörüne olan ilgisinin her geçen gün artması, internet ve telekomünikasyon hizmet sağlayıcılarının veri toplamaya ilişkin yükümlülüklerinin de 95/46/EC sayılı Direktif ile uyumlu hale getirilmesi, belirli verilerin muhafaza edilmesinin sağlanması, güvenlik ve terör suçlarının soruşturulması, tespit edilmesi ve kovuşturulması açısından verilerin erişilebilir kılınması dolayısıyla güvenlik endişesiyle AB'nin yaklaşımında değişiklikler meydana gelmiştir. Kişisel verilerin işlenmesi ve mahremiyet hakkının korunmasını konu alan 95/46/EC sayılı Direktif'in, bahsi geçen elektronik haberleşme sektörü işletmecilerinin saklamaya ilişkin faaliyetlerinin de uyumlaştırılması amacıyla yeni bir düzenleme yapılması ihtiyacı doğmuştur.[473] Bunun üzerine Avrupa Komisyonu, Eylül 2005'te veri saklamaya ilişkin bir Direktif önerisinde bulunmuş olup; 2006/24/EC sayılı Veri Saklama Direktifi[474], 2006 yılında kabul edilmiştir.[475]

2.1.2. Veri Saklama Direktifi'yle Düzenlenen Hususlar

Veri Saklama Direktifi ile, hizmet sağlayıcılara telekomünikasyon verilerini saklama yükümlülüğü getirilerek; yetkili ulusal makamların haberleşmeye ilişkin verilere erişim sağlayabilmesine imkan tanınmıştır. Böylece AB üyesi devletlerin, gereklilik ve orantılılık unsurlarına riayet ederek saklanan haberleşme verilerine erişebilmesini mümkün hale getiren çalışmalar yapması gerektiği düzenlenmiştir.[476]

Direktifin özü, veri saklama yükümlülüğüne ilişkin olup; ISS'ler ve telekom operatörlerine önemli bir süre boyunca, çeşitli miktarda verileri toplama ve saklama yükümlülüğü getirilmiştir. Bu yükümlülük ve belirlenen kurallar birçok yönden problem teşkil etmektedir.[477]

---

[473] Vedaschi, "Data Retention," 18.
[474] Directive 2006/24/EC of the European Parliament and of the Council, EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=en . Erişim Tarihi: 16 Ekim 2022.
[475] Barbara Grabowska-Moroz, "Data Retention in the European Union," iç. *European Constitutional Courts towards Data Retention Laws*, ed. Marek Zubik, Jan Podkowik, Robert Rybski, (Switzerland: Springer Nature, 2021), 3-4.
[476] Grabowska-Moroz, "Data Retention," 4.
[477] Vedaschi, "Data Retention," 19.

Veri Saklama Direktifi'nin 5/1 maddesinde, bir haberleşmenin kaynağını izleme ve tanımlama, haberleşmenin hedefini belirleme, haberleşmenin tarihini, saatini ve süresini belirleme, haberleşmenin türünü belirleme, kullanıcıların haberleşme ekipmanlarını belirleme ve mobil haberleşme ekipmanının yerini belirlemek için gerekli veriler olmak üzere altı başlık halinde veri kategorileri oluşturulmuştur. Buna göre, sabit şebeke ve mobil telefonla ilgili olarak; arayan telefon numarası, abonenin ya da kayıtlı kullanıcının adı ve adresi, haberleşmenin kaynağını izlemek ve tanımlamak için gerekli verilerdir. İnternet erişimi, e-posta ve VoIP arama ile ilgili olarak; tahsis edilen kullanıcı kimlikleri, haberleşme sırasında IP adresi, kullanıcı kimliği ya da telefon numarası tahsis edilen abonenin ya da kayıtlı kullanıcının adı ve adresi haberleşmenin kaynağının takibine yönelik gerekli olan verilerdir. Haberleşmenin hedefini belirlemek için gerekli veriler, sabit şebeke ve mobil telefon ile ilgili aranan telefon numarası, çağrı yönlendirme ya da çağrının aktarıldığı numaralar; e-posta ve VoIP arama ile ilgili internet üzerinden yapılan aramanın hedeflenen alıcılarının kullanıcı kimliği ya da telefon numarası ile abonelerin ya da kayıtlı kullanıcıların isimleri ve adresleri gerekli veriler olarak ifade edilmiştir.

İlgili hükmün devamında, bir haberleşmenin tarihini, saatini ve süresini belirlemek için, sabit şebeke telefonu ve mobil telefon ile ilgili olarak haberleşmenin başladığı ve bittiği tarih ve saat bilgisine ihtiyaç olduğuna yer verilmiştir. İnternet erişimi, e-posta ve VoIP arama ile ilgili ise abonenin ya da kayıtlı kullanıcının kullanıcı kimliği ve internet erişim hizmeti sağlayıcısı tarafından tahsis edilen dinamik ya da statik IP adresine ihtiyaç duyulmaktadır. Ayrıca belirli bir saat dilimine dayalı olarak internet erişim hizmetinin oturum açma ve oturum kapatma tarihi ve saati yanında belirli bir saat dilimine göre e-posta hizmeti ya da internet üzerinden telefon hizmetinin oturum açma ve oturum kapatma tarihi ve saatini içeren verilere ihtiyaç vardır.

Veri Saklama Direktifi'nin 5/1 madde hükmünde ayrıca haberleşmenin türünü belirlemek için, sabit şebeke ve mobil telefon ile ilgili kullanılan telefon hizmeti; e-posta ve VoIP arama ile ilgili kullanılan internet hizmetine ilişkin verilerin gerekli olduğu belirtilmektedir. Kullanıcıların haberleşme ekipmanlarının ne olduğunu belirlemek için, mobil telefon ile ilgili olarak arayan ve aranan telefon numaraları, arayan tarafın Uluslararası Mobil Abone Kimliği (IMSI), arayan tarafın Uluslararası Mobil Cihaz Kimliği (IMEI), aranan tarafın IMSI'si, ön ödemeli anonim hizmetler söz konusu

olduğunda, hizmetin ilk etkinleştirildiği tarih ve saat ile hizmetin etkinleştirildiği konum etiketi olarak adlandırılan hücre kimliği verisinin gerekli olduğuna yer verilmiştir. Bunun dışında, internet erişimi, e-posta ve VoIP arama ile ilgili, çevirmeli erişim için arayan telefon numarası ve dijital abone hattı (DSL-digital subscriber line)[478] veya haberleşmenin başlatıcısının diğer uç noktası verisine ihtiyaç olduğu vurgulanmaktadır. Veri Saklama Direktifi'nin 5/1 maddesinde son olarak, mobil haberleşme ekipmanının yerini belirlemek için, haberleşmenin başlangıcındaki konum etiketi olarak adlandırılan hücre kimliği verisi ve haberleşme verilerinin tutulduğu süre boyunca konum etiketleri olarak adlandırılan hücre kimliğine atıfta bulunarak hücrelerin coğrafi konumunu tanımlayan verilerin gerekli olduğuna yer verilmiştir.

2.1.3. Veri Saklama Direktifi'ne Getirilen Eleştiriler

Veri kategorileri ile ilgili olarak Veri Saklama Direktifi, iletişim ve coğrafi konum verilerinin kaynağı ve alıcısı, türü, tarihi, saati ve süresi ile ilgili verilerin toplanmasını ve saklanmasını düzenlemiştir. Bu tür kayıtların toplanması ve saklanması, hizmet sağlayıcıların, büyük miktardaki verileri otomatik şekilde toplama ve bu verileri, veri bankalarında saklama yeteneğine sahip olan teknolojilere itimat ederek teslim olmasını gerektirmektedir. Bu verilerin, anlamlandırılabilir veriler olmasa dahi bir arada bulunduklarında anlamlı bir bütün oluşturma riski ve muazzam bir profil oluşturma potansiyelinin olması göz ardı edilmemelidir.[479] Dolayısıyla söz konusu meta verilerin saklanması, verilerin kötüye kullanılması ya da yetkisiz erişim ihtimalleri nedeniyle gizlilik ihlallerinin yaşanabilmesi riski Veri Saklama Direktifi'nin sorgulanmasına sebep olmuştur.[480]

Veri Saklama Direktifi'nin 7. maddesinde elektronik haberleşme hizmeti sağlayıcılarının verilere ilişkin gerekli güvenlik tedbirlerini alması, yalnızca yetkili kişiler tarafından erişim sağlanabilmesi ve saklama süresinin sona ermesi halinde imha edilmesi gerektiği belirtilmiştir. İlgili Direktif'in 8. maddesinde ise üye devletlerin yetkili

[478] Dijital abone hattı anlamına gelen DSL (digital subscriber line), multimedya ev video gibi yüksek bant genişliğine sahip verileri hizmet verdiği abonelerine ulaştırmak için mevcut telefon hatlarını kullanan bir modem teknolojisidir. Ayrıca DSL, ayrılmış, noktadan noktaya genel ağ erişimini sağlar. xDSL terimi, ADSL (asimetrik DSL) de dahil olmak üzere, bir dizi DSL terimini kapsar. (Cisco, "Digital Subscriber Line (DSL)," cisco.com, https://www.cisco.com/c/en_uk/solutions/routing-switching/dsl.html , Erişim Tarihi: 16 Ekim 2022.)
[479] Vedaschi, "Data Retention," 20.
[480] Vedaschi, "Data Retention," 21.

makamları tarafından talep edilmesi halinde Direktif'in 5. maddesinde yer verilen haberleşen kullanıcı numaraları, haberleşmenin gerçekleştiği zaman gibi verilerin iletilmesi gerektiğine değinilmiştir.

Veri Saklama Direktifi'nin amacı, ilgili Direktif'in 5/2 maddesinde yer verilen iletişimin içeriği hariç olmak üzere iletişime ilişkin tüm verileri, ciddi suçların araştırılması, tespiti ve kovuşturulması amacıyla erişilebilir kılmaktır.[481]

Söz konusu Direktif'in bir diğer olumsuz yanı ise "ciddi suç" ve "yetkili makamlar" kavramlarını tanımlamaması ve toplanacak verileri sınırlandırmaması, dolayısıyla hükümleri kabul edilemez şekilde genel nitelikte bırakmasıdır.[482] Bununla birlikte, Direktif'in, verilerin Avrupa yargı yetkisinin haricinde bir bölgede tutulmasına imkan verecek düzenlemelere yer vermesi, herhangi bir coğrafi sınırlama olmaksızın farklı ülkelerde tutulan verilerin bu ülkelerin mevzuatlarına tabi olabilmesinin boşluk oluşturabileceği düşünülmektedir.[483]

Devletlerin güvenlik ve terör gerekçesiyle küresel bir gözetim sistemi geliştirme gayesi, bu doğrultuda vatandaşların haberleşmeleri ve çevrimiçi davranışlarının takibinin yapılması yönünde sergiledikleri tutum, mahremiyet hakkının ihlaline sebep olabilecek durumlar ortaya çıkarmaktadır. Bu durumun bireyleri savunmasız bıraktığı düşünülmektedir. Veri Saklama Direktifi, AB vatandaşlarının verilerinin saklanması, terörle mücadele çalışmaları ile mahremiyet ve veri koruma hakları arasında bir denge kurmayı amaçlamış olup; herkese şüpheli muamelesi yaptığı, herkesi izleyerek, gözetim altına aldığına dair yaklaşım ile vatandaşların mahremiyet haklarına müdahale ettiği yönünde eleştirilmiştir.[484]

2.1.4. Veri Saklama Direktifi'ne İlişkin Değerlendirme İçeren Bazı Yargı Kararları

Veri Saklama Direktifi, elektronik haberleşme sektöründeki işletmecileri e-postalar ve telefon görüşmelerine ilişkin veriler de dahil olmak üzere haberleşmeye ilişkin verileri iki yıla kadar toplamak ve saklamakla yükümlü kılmıştır. Bu durumun

[481] Nora Ni Loideain, "The EC Data Retention Directive: Legal Implications for Privacy and Data Protection," iç. *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, Christina Akrivopoulou, Athanasios- Efstratios Psygkas, (New York: Information Science Reference, 2011), 260.
[482] Vedaschi, "Data Retention," 27.
[483] Vedaschi, "Data Retention," 30.
[484] Vedaschi, "Data Retention," 14.

vatandaşların özellikle özel hayatının gizliliğine ilişkin temel hakkına ciddi bir müdahale teşkil ettiği gerekçesiyle, bu doğrultuda çeşitli mahkeme kararları verilmeye başlanmış olup; ABAD mahremiyet hakkının ve kişisel verilerin korunması hakkının ihlal edildiği gerekçesiyle 2006/24/EC sayılı Veri Saklama Direktifi'nin geçersiz olması gerektiğine ilişkin düşüncesini vermiş olduğu kararlarında belirtmiştir.[485]

Veri Saklama Direktifi ile 2002/58/EC sayılı Elektronik Haberleşme Direktifi'ndeki genel veri koruma kurallarından uzaklaşılarak; Direktif'in, özel hayatın gizliliği hakkına karşılık toplumun güvenliği açısından açıkça bir muafiyet oluşturduğu düşüncesi, AİHM tarafından geliştirilen içtihat ile pekiştirilmiştir. Bu doğrultuda, kamu güvenliğinin yanında haberleşmenin gizliliği, özel hayatın korunması hakkının da gözetilerek orantılı önlemler alınması bakımından Veri Saklama Direktifi tartışılmaya başlanmıştır.[486]

Veri Saklama Direktifi'nin yasal gelişimi, veri koruma yetkilileri ve ISS sektörü de dahil olmak üzere rahatsızlığa sebep olmaya başladıktan sonra, söz konusu Direktif'in oluşturulması esnasında vurgulanan veri koruma ve mahremiyete ilişkin endişeler, veri koruma konusunda taahhütlerin orantılı ve etkili bir mevzuatın geliştirilmesine yönelik olmadığı hususunda yoğunlaşmaktadır.[487]

AİHM, Veri Saklama Direktifi'nin verilerin saklanması konusunda yalnızca üye devletlerdeki hizmet sağlayıcıların iç pazardaki faaliyetlerini kapsadığını, kamu makamlarının faaliyetlerini düzenleyen herhangi bir kural içermediğinden kolluk kuvvetlerinin verilere erişimini ya da kullanımını öncelikli olarak amaçlamadığını belirtmiştir. Dolayısıyla veri saklama yükümlülüklerinin getirilmesinin ulusal güvenliği etkilediği kabul edilse de doğrudan özel sektördeki hizmet sağlayıcıların bundan etkilediğinin kabulünün gerektiği vurgulanmıştır.[488]

Avrupa mahkemelerinin içtihatlarında yer alan telekomünikasyon verilerinin saklanmasına ilişkin hususlar, verilerin korunması için bir standart oluşturmamıştır. Tartışma konusu olan kararlar, yalnızca bir başlangıç noktası olmuştur.[489]

---

[485] Vedaschi, "Data Retention," 15-17.
[486] Grabowska-Moroz, "Data Retention," 4.
[487] Loideain, "Data Retention Directive," 268-269.
[488] Grabowska-Moroz, "Data Retention," 4-5.
[489] Jan Podkowik, Robert Rybski, Marek Zubik, "Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?," *International Journal of Constitutional Law* 19, no.5 (2021): 1599–1600, https://academic.oup.com/icon/article/19/5/1597/6498025 , Erişim Tarihi: 18 Ekim 2022.

AİHM ve ABAD'ın Veri Saklama Direktifi'ne ilişkin vermiş olduğu kararlardan dört tanesine çalışmada yer verilmiştir.

2.1.4.1. S. ve Marper - Birleşik Krallık Kararı

2011 yılında Avrupa Komisyonu tarafından Veri Saklama Direktifi'nde değişiklik yapılarak; veri saklamaya ilişkin yükümlülüklerin yalnızca iç pazarı uyumlu hale getiren bir araç olarak değil, bir güvenlik önlemi olarak düzenlenmesi tavsiye edilmiştir. Komisyon bunun yanında, zorunlu veri saklama sürelerini kısaltarak, veri erişimi ve saklamaya yönelik taleplerin bağımsız denetiminin sağlanmasını; bu sayede saklanacak veri kategorilerinin azaltılmasını, telekomünikasyon verilerinin korunması planı dahilinde kişisel verilerin korunmasına yönelik atılacak adımların da güçlendirilmesi ihtiyacını belirtmiştir. Ayrıca Komisyon, AİHM'in S. ve Marper - Birleşik Krallık kararıyla[490] birlikte, bireyin veri toplama konusundaki endişelerini kamu güvenliğine karşı dengeleyen nitelikte bir standart oluşturulması gerektiği kanaatine varmıştır.[491]

İlgili AİHM kararında, işlediği bir suç sebebiyle parmak izi ve DNA örneği alınan başvuruculaların, haklarında başlatılan ceza davaları, beraat ya da uzlaşma sebebiyle davanın düşmesiyle ceza almadan sona erdikten sonra da ilgili Veri Saklama Direktifi gereğince parmak izleri gibi kendilerini tanımlayıcı özel nitelikli kişisel verilerin üye devlet tarafından saklanmaya devam edilmiştir.[492] Başvurucular bu verilerin silinmesini talep etmesine rağmen; üye devletin iç hukukunda, gelecekte işlenecek olan suçlarla ilgili yapılacak soruşturmalarda karşılaştırma yapılabilmesi amacıyla süresiz şekilde saklanabileceğine ilişkin düzenleme olması sebebiyle talebinin reddedilmesi konusunda AİHM, kişinin söz konusu verilerinin yalnızca kendisiyle ilgili değil, tüm akrabalarıyla ilgili bilgi edinilmesini sağlayacak düzeyde olması ve bireyin kınanma ihtimalinin önüne geçilebilmesi amacıyla süresiz şekilde saklanmasının uygun bir önleyici uygulama olmadığı, kişilerin masumiyet karinelerini ihlal edeceğini, dolayısıyla söz konusu uygulamanın AİHS'yi ihlal edeceğini belirtmiştir.[493]

---

[490] AİHM, 30562/04 ve 30566/04 Başvuru numaralı, 04.12.2008 tarihli Karar, https://rm.coe.int/168067d216 , Erişim Tarihi: 18 Ekim 2022.
[491] Grabowska-Moroz, "Data Retention," 5.
[492] Songül Atak, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler," *Türkiye Barolar Birliği Dergisi*, no.87 (2010): 118.
[493] Rıza Saka, "Kişisel Verilerin Korunması ve İmhasına İlişkin Genel Açıklamalar," iç. *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası*, Rıza Saka, Ramazan Çağlayan, Mahmut Koca, (Ankara: Seçkin Yayıncılık, 2020): 242-243.

AİHM, beraatle ya da ceza davasının düşmesiyle sonuçlanan davalarda parmak izi gibi hassas verilerin saklanmaya devam edilmesinin kamunun ve bireylerin arasındaki menfaatlerinin çatışması ile devletin takdir yetkisinin sınırlarının aşılarak, özel hayata ilişkin orantısız müdahale teşkil ettiğini böylelikle AİHS'in 8. maddesinin ihlal edildiğini vurgulamıştır.

Söz konusu karar, Veri Saklama Direktifi'nin uygulanabilirliği konusunda sorunlar olduğuna işaret edilmesi açısından önem taşımaktadır. AİHM, İlgili Direktif doğrultusunda üye devletler tarafından bireyin hakları ile kamu güvenliği arasında denge gözetilmeden gerçekleştirilen uygulamaların hukuka aykırı olacağı endişesini dile getirmiştir.

2.1.4.2. İrlanda - Avrupa Parlamentosu Kararı

İrlanda - Avrupa Parlamentosu kararı[494], Veri Saklama Direktifi'ndeki veri saklama yükümlülüklerine itiraz edilen ilk örneklerinden biri olup; İrlanda Hükümeti'nin ve ardından ABAD'ın esasa ilişkin inceleme yapmadan, yalnızca şekil yönünden inceleme yapması sebebiyle başarısız olarak değerlendirilmektedir. Bununla beraber söz konusu karar, Veri Saklama Direktifi'ne ilişkin itirazların ilerleyen süreçte artacağının işaretlerini vermiştir. Veri Saklama Direktifi'nin uygulanması, çeşitli kontrol mekanizmaları ve Direktif'e sirayet eden belirsiz orantılılık standardının değişkenlik göstermesi nedeniyle, üye devletlerin Veri Saklama Direktifi'ne yönelik yaklaşımları da farklılık arz etmiştir. Nihayetinde, ABAD'ın verdiği İrlanda - Avrupa Parlamentosu kararı, Veri Saklama Direktifi hakkındaki tartışmaları sona erdirememiştir.[495]

Söz konusu süreci, Veri Saklama Direktifi'ne dair ulusal anayasa mahkemeleri tarafından kendi anayasalarına uygun olarak verilen Veri Saklama Direktifi'nin uygulanmasına ilişkin kararlar takip etmiştir. Genel anlamda ulusal mahkemeler, kolluk kuvvetlerinin endişeleri ile bireylerin veri koruma konusundaki talepleri arasında bir denge kurmaya çalışmıştır. Veri Saklama Direktifi'nin yükümlülükleri çerçevesinde veri saklamaya ilişkin yapılan üye devletlerin ulusal anayasal incelemelerinin artmasıyla, mahkemeler arasında adli konularda iletişim kurulması tetiklenmiştir. Böylece ABAD

[494] ABAD, Case C-301/06 numaralı, 10.02.2009 tarihli Karar, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62006CJ0301&from=en , Erişim Tarihi: 18 Ekim 2022.
[495] Grabowska-Moroz, "Data Retention," 5.

üye devletlerin ulusal kararlarını göz ardı edemeyerek; dikkate almak durumunda kalmıştır.[496]

ABAD'ın İrlanda - Avrupa Parlamentosu kararı, üye devletlerin anayasa mahkemelerinin saklanan telekomünikasyon verilerine yetkili makamların erişimini sağlayan ulusal düzenlemelerinin anayasalarına uygunluğunu özerk bir şekilde değerlendirmesi ve bu düzenlemelerin AİHS ve ulusal anayasalarına uygunluğunu değerlendirmesi gereken alanların haritasını çıkarmıştır.[497]

Ulusal mahkemeler bu karardan önce AB mevzuatının geçerliliğini sorgulama eğiliminde olmamıştır. Fakat 2006/24/EC sayılı Veri Saklama Direktifi, elektronik haberleşme verilerinin saklanmasına ilişkin mekanizmalarının uygunluğu ve özel hayatın korunması hakkıyla ilgili çekincelere yol açmıştır.[498] Söz konusu karar, üye devletlerin bazıları tarafından Direktif'in hükümlerinin uygulanabilir olmadığına ve geçersiz olması gerektiğine dair kanaat getirildiğini göstermesi açısından önem taşımaktadır.

2.1.4.3. İrlanda Dijital Haklar Kararı

2014 yılına gelindiğinde ABAD, İrlanda Dijital Haklar kararıyla[499] anayasal çerçevede Veri Saklama Direktifi'ne ilişkin argümanları tartışmaya başlamıştır. Veri Saklama Direktifi'nin mahremiyet ve kişisel verilerin korunması hakları da dahil olmak üzere AB Temel Haklar Şartı'nda ifade edilen insan haklarına ilişkin temel değerler ile ilişkisi ABAD tarafından incelenmiştir.

AB'de temel hakların düzenlenmesini sağlayan AB Temel Haklar Şartı, 2009 tarihli Lizbon Antlaşması'yla bağlayıcılık kazanmış olup; söz konusu metin bireylerin kişisel, sosyal, ekonomik gibi haklarını düzenleyerek aynı çatı altında birleştirmiştir. Bu haklar, AB hukukunda düzenlenmiş olan mevcut hakların ABAD'ın insan haklarına saygı çerçevesindeki yaklaşımı ile tekrar gözden geçirilmiş ve mahkemelerin karşılaştıkları hukuki problemlerde göz önünde bulundurdukları bir hukuki metin olarak dikkat çekmektedir. AB Temel Haklar Şartı'nın 8. maddesi, kişisel verilerin korunması hakkına yer vermekte olup; bu madde temelde AİHS, 108 sayılı Sözleşme ve 95/46/EC sayılı

[496] Grabowska-Moroz, "Data Retention," 6.
[497] Podkowik, "European Constitutional Courts?," 1627.
[498] Podkowik, "European Constitutional Courts?," 1626-1627.
[499] ABAD, Case C-293/12 numaralı, 08.04.2014 tarihli Karar, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=4 , Erişim Tarihi: 21 Ekim 2022.

Direktif doğrultusunda oluşturulmuş ve AİHS'den ayrı şekilde özel hayatın gizliliği hakkı içerisinde değerlendirilmemiştir.[500]

ABAD, gizlilik ve kişisel verilerin korunması haklarına müdahalenin temelde Direktif tarafından düzenlenen iki unsurdan kaynaklandığını belirtmiştir. Bunlardan birincisi, kişinin özel hayatına ve haberleşmesine ilişkin verilerin zorunlu olarak saklanması, ikincisi ise ulusal makamlar tarafından verilere erişimin mümkün olmasıdır. ABAD, söz konusu müdahalenin, bilhassa bireylerin sürekli izlenmesine yol açabileceği endişesiyle ciddi nitelikte olduğunu tespit etmiştir. Bununla beraber, kamu güvenliğini sağlamak adına ciddi suçlarla mücadele anlamına gelen önemli sayılabilecek müdahalelerin meşru olabileceği sonucuna vararak; elektronik haberleşmenin kullanımına ilişkin verilerin önem arz ettiğini ve Veri Saklama Direktifi'nin 1/1 maddesinde yer verildiği üzere, ciddi suçların önlenmesi ve suçlarla mücadele edilmesinde kıymetli bir araç olduğuna yer vermiştir. Ancak ABAD, telekomünikasyon verilerinin saklanması ve kullanılmasına dair yasal çerçeveyi tam olarak belirlemeyerek, veri saklamanın meşru amacına ilişkin ayrıca bir açıklamada bulunmamıştır. Bunun haricinde, Avrupa Komisyon'un 2011 yılındaki değerlendirmelerine ve veri saklama sisteminin etkililiğine ilişkin herhangi bir kaynağa da atıfta bulunmamıştır.[501]

Bir bireyin mahremiyet hakkına yönelik olarak "ciddi müdahale" kavramı, ABAD'ı katı bir inceleme standardı uygulamaya yöneltmiştir. Bu çerçevede ABAD, verilerin hem saklanmasına hem de erişilmesine müdahale edilmesi, veri saklama ile ciddi suçlar arasında ilişki olmaması, bütün Avrupa nüfusunu kapsayan çok sayıda verinin tutulması, saklanan verilere erişimle ilgili usule ilişkin güvencelerin olmaması, "ciddi suç" kavramının muğlak tanımı ve tutulan verilerin güvenliği ile ilgili duyulan endişeler doğrultusunda Veri Saklama Direktifi'nin eksiklikler içerdiğini ifade etmiştir. İrlanda Dijital Haklar kararı, ABAD'ın kişisel verilerin korunması hakkına müdahale edilmesine ilişkin ayrıntılı bir analiz yapmamasına ve genel olarak çoğunlukla mahremiyet hakkına atıfta bulunmasına rağmen, AB Temel Haklar Şartı'nın önemini ortaya koymuştur.[502]

---

[500] Sezen Kama Işık, Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış, (İstanbul: On İki Levha Yayıncılık, 2020),108-109.
[501] Grabowska-Moroz, "Data Retention," 6.
[502] Grabowska-Moroz, "Data Retention," 7.

2.1.4.4. Tele-2/Watson Kararı

ABAD'ın Tele-2/Watson davasındaki kararı[503], zorunlu olarak veri saklamaya ilişkin ABAD'ın yaklaşımının değişiklik gösterdiğinin görülmesi sebebiyle önem arz etmektedir. İrlanda Dijital Haklar davasında ABAD daha çok AB mevzuatını incelerken; Tele-2/Watson davasında ise açıkça üye devletlerin ulusal mevzuatına atıfta bulunmuştur. İnceleme konuları arasında farklılık teşkil eden hususlara rağmen, Tele-2/Watson davası, İrlanda Dijital Haklar davasının devamı niteliğindedir. ABAD, Tele-2/Watson davasında veri saklanmasına ilişkin yeni bir yaklaşım sunarken; kolluk kuvvetlerinin verilere erişimine ilişkin olarak, İrlanda Dijital Haklar davasındaki benzer argümanları kullanmıştır. Tele-2/Watson davası, Veri Saklama Direktifi'ni tamamıyla geçersiz kılan bir karar ile sonuçlanmıştır. ABAD, üye devletlerin elektronik haberleşme hizmeti sağlayıcılarına verilerin saklanması konusunda genel bir yükümlülük getirmesinin söz konusu olamayacağına karar vermiştir. Tele-2/Watson kararı ve İrlanda Dijital Haklar kararı ile, Veri Saklama Direktifi'nin mahremiyet hakkına ciddi bir müdahale oluşturan, bireysel profillemenin oluşturulmasına olanak sağlayan yapıda olduğuna kanaat getirilmiştir. Ayrıca her iki kararda da belirtildiği, verilerin saklanmasının yalnızca kesinlikle gereklilik olan durumlarda, sınırlandırılarak gerçekleştirilmesi konusunda ulusal mevzuatlarda düzenlemeler yapılması hususu vurgulanmıştır.[504]

Sonuç olarak Tele-2/Watson davasında ABAD, İrlanda Dijital Haklar kararının önemini teyit etmenin yanında, ulusal düzeyde veri saklama mevzuatının hem Avrupa hem de uluslararası insan hakları hukukuna uygun olması gerektiğine dair düşüncesini genişletmiştir.[505]

Veri Saklama Direktifi'nin iptal edilmesi ile mahremiyet hakkının daha iyi şekilde korunmasına yönelik bir adım atılmış olup; özel hayatın gizliliğinin, toplumun güvenlik çıkarlarından daha önce geldiği kanıtlanmıştır.[506]

---

[503] ABAD, Case C-203/15 numaralı, 21.12.2016 tarihli Karar, https://privacyinternational.org/sites/default/files/2019-08/CELEX_62015CJ0203_EN_TXT.pdf Erişim Tarihi: 21 Ekim 2022.
[504] Grabowska-Moroz, "Data Retention," 11.
[505] Grabowska-Moroz, "Data Retention," 12.
[506] Vedaschi, "Data Retention," 32-33.

2.2. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN SAKLANMASINA YÖNELİK TÜRK HUKUKUNDAKİ DÜZENLEMELER

Kişisel verilerin korunmasına yönelik hazırlanan uluslararası düzenlemelere uyum sağlayabilmek için, kişisel verilerin işlendiği alanları düzenleyen kanunlara bu konuya ilişkin hüküm eklenmesi gerektiği fark edilmiş ve bu doğrultuda çeşitli düzenlemeler yapılmıştır.

Elektronik haberleşme sektörünün temelini oluşturan ve sektöre ilişkin uyulması gereken kuralların belirlendiği temel kanun olan 5809 sayılı EHK'da kişisel verilerin korunmasına ilişkin yer alan tek hüküm 51. madde hükmüdür. EHK'nın yayımlandığı tarih olan 2008 yılında kişisel verilerin korunmasına yönelik düşüncenin ve aynı zamanda uluslararası düzenlemelerin bugünkü kadar gelişmiş olduğu söylenemeyeceğinden; ilgili 51. maddenin ilk halinde, bu sektördeki kişisel verilerin korunmasına ilişkin usul ve esasları BTK'nın belirleyeceğine dair tek bir cümle yer almaktaydı. İlgili maddenin bu halinin Anayasa'nın bazı maddelerine aykırı olduğu gerekçesiyle iptal edilmesinin ardından; kişisel verilerin korunmasına yönelik daha kapsamlı hükümler ile yeniden düzenleme yapılmıştır.

2.2.1. Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Başlıklı EHK'nın 51. Maddesinin Değerlendirmesi

Anayasa'nın 13. maddesinde temel hak ve özgürlüklerin yalnızca kanun ile sınırlandırılabileceğine ilişkin hüküm yer almaktadır. Hukuk devleti olabilmenin şartlarından biri olan hukuki belirlilik ilkesi de yine temel hak ve özgürlüklerin yalnızca kanunla sınırlı olması hususuyla bağdaşmaktadır.[507]

Kanunla sınırlama ölçütü, sınırlamanın öngörülebilir şekilde çerçevesinin belirli olmasını ve kesinliğini ifade etmektedir. Bu ölçüt, yürütme organının keyfiyeti doğrultusunda değişkenlik gösterebilecek olan davranışlarının önüne geçilmesi ve kişilerin hukuku bilerek davranmalarını; diğer bir ifadeyle hukuk güvenliği teminatını sağlamaktadır.[508]

---

[507] Abdurrahman EREN, *Anayasa Hukuku Dersleri*, (Ankara: Seçkin Yayıncılık, 2021), 582.

[508] AYM, 2013/1789 Başvuru numaralı ve 11.11.2015 tarihli Kararı, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/1789 , Erişim Tarihi: 22 Ekim 2022.

Yasama organının asli yetki, yürütme organının ise tali bir yetkiye sahip olduğu; yasama organı tarafından kanunla belirlenmemiş hiçbir konuda yürütmenin düzenleme yapamayacağından hareketle;[509] kanun ile temel esaslar doğrultusunda çerçeve belirlendikten sonra belirlenen kuralların uygulamaya dair ayrıntılarına kurumların kendilerinin çıkardıkları yönetmeliklerde yer verilmesi, temel hakların korunması konusunda önem taşımaktadır.

Elektronik haberleşme sektöründe kişisel verilerin korunması hususunda temel nitelikteki düzenleme olan 5809 sayılı EHK'nın 51. maddesinin 2008 yılında yayımlanan ilk halinde *"Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir."* denilmektedir.

Danıştay İdari Dava Daireleri Kurulu tarafından iptali istenen EHK'nın 51. maddesinin, Anayasa'nın 2., 7., 13. ve 20. maddelerine aykırı olduğu iddiasında bulunulmuştur. Anayasa Mahkemesi, ilgili istemin üzerine vermiş olduğu kararda ilk olarak; elektronik haberleşme sektöründe teknolojinin yardımıyla normalden çok daha fazla veri toplanabildiği, veri madenciliğiyle bir veriden birden fazla yeni veri üretilebilmesinin mümkün olduğu, veri aktarımının eskiye göre daha kolay olduğu gibi hususlar göz önünde bulundurulduğunda; kişisel verilerin korunmasının günümüzde zorunlu hale geldiğinin açık olduğu belirtilerek; Anayasa'nın 20/3 maddesinde yer verilen kişisel verilerin korunmasına ilişkin esasların ancak kanunla belirlenmesi gerektiği kuralının, kişisel verilerin korunması hakkının kamu makamlarının keyfi davranışlarına karşı korunması amacıyla güvence altına alındığını belirtmiştir. Ayrıca Anayasa'nın 7. maddesinde yer verilen TBMM'ye ait yasama yetkisinin devredilemezliği ilkesi doğrultusunda, kanunla düzenlenmesi gereken bir hususun yürütmenin keyfiyetine bırakılamayacağına değinilmiştir. Bununla birlikte, Anayasa'nın 20/3 maddesiyle korunmak istenen temek hak olan kişisel verilerin korunması hakkına ilişkin hususlar yine Anayasa'nın 13. maddesinde belirtilen hüküm gereğince ancak kanunla sınırlandırılabilecektir.[510]

---

[509] Yasin Söyler, *Yeni Başkanlık Sisteminde Cumhurbaşkanlığı Kararnamesi*, (Ankara: Seçkin Yayıncılık, 2018), 78; Adnan Küçük, *Türkiye'de Başkanlık (Cumhurbaşkanlığı) Sistemi*, (Ankara: Adalet Yayınevi, 2021), 278-281.

[510] AYM, 09.04.2014 tarih ve E. 2013/122, K. 2014/74 sayılı Kararı, https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf , Erişim Tarihi: 23 Ekim 2022.

Belirtilen Anayasa hükümleri doğrultusunda; elektronik haberleşme sektöründeki kişisel verilerin işlenmesi ve korunmasına yönelik esasların belirlenmesi yetkisinin TBMM yerine BTK tarafından kullanılmasını sağlayarak; kişisel verilerin korunması hakkına müdahalede bulunacak olan EHK'nın 51. maddesinin uygulanmaya devam etmesi, Anayasa'nın 2. maddesinde belirtilen hukuk devleti ilkesine de aykırı olduğundan, Anayasa Mahkemesi tarafından iptal edilmesine karar verilmiştir.

İlgili Anayasa Mahkemesi kararı ile yürürlükten kalkan EHK'nın 51. maddesi, 27 Mart 2015 tarihinde yeniden düzenlenerek yürürlüğe girmiştir.[511] Bu kez, on üç fıkra halinde düzenlenen kanun maddesinde, kişisel verilerin işlenmesine yönelik temel hususlara yer verilmiş; BTK'ya ise yalnızca ilgili maddenin uygulanmasına yönelik usulü belirleme görevi verilmiştir.

EHK'nın söz konusu 51. maddesinin ilk fıkrasında, verilerin belirli amaçlar çerçevesinde hukuka uygun şekilde işlenmesi gibi KVKK'nın 4/2 maddesinde yer alan kişisel verilerin işlenmesine ilişkin temel ilkelerden bahsedilmiştir.

EHK'nın 51/10 maddesinde, elektronik haberleşme sektöründe sunulan hizmetlerle ilgili saklanan kişisel verilerin saklama sürelerine ilişkin olarak; soruşturmaya ya da uyuşmazlığa konu herhangi bir durum olması halinde ilgili süreç sonuçlanana kadar, verilere ya da verilerle ilgili olan sistemlere erişimi gösteren kayıtların iki yıl boyunca saklanması gerektiğine yer verilmiştir. Ayrıca ilgili hükmün devamında, aboneler tarafından kendi kişisel verilerinin işlenmesine verilen rızaların ise en az abonelik süresi kadar saklanması gerektiğine yer verilmekle birlikte; gerçekleşen haberleşmeye ilişkin kayıtların ise en az bir yıl en fazla iki yıl olacak şekilde saklanmasına ilişkin düzenlemenin yönetmelikle belirlenmesi öngörülmüştür.

EHK'nın 51. maddesinde belirtilen kuralların usul ve esaslarını belirlemek üzere BTK tarafından yayımlanan Kişisel Verilerin İşlenmesi Yönetmeliği'nde saklama sürelerine ilişkin bulunan tek hüküm, işletmecilerin kişisel veri ve bu verilerle ilgili olan sistemlere gerçekleştirilen erişim faaliyetleri hakkında oluşturulan işlem kayıtlarının iki yıl boyunca saklanmasını emreden 6/4 maddesidir.

[511] R.G. 15.04.2015, S.29327. Söz konusu 6639 sayılı Kanun'un 32. maddesiyle değiştirilen EHK'nın 51. maddesi, 26 Ocak 2015 tarihinden itibaren geçerli olacak şekilde yürürlüğe girmiştir.

2.2.2. Abonelik Tesisi Esnasında Alınan Kişisel Verilerin Saklanması ve Saklama Sürelerine İlişkin Değerlendirme

Elektronik haberleşme sektöründe abonelik tesisi sırasında abonelik sözleşmesi yapma zorunluluğundan çalışmanın Birinci Bölümü'nde, abonelik sözleşmesine ek olarak alınması gereken evraktan ise çalışmanın İkinci Bölümü'nde bahsedilmiştir.

Tüketici Hakları Yönetmeliği'nin 7/7 maddesinde yer verildiği üzere; abonelik sözleşmesi ve sözleşmenin kurulmasıyla ilgili belgelerin elektronik haberleşme hizmetini sunan işletmeciler tarafından saklanması gerekmektedir. İlgili hükümde değinilen bir diğer husus da söz konusu belgelerin saklanma süresine ilişkin olup; bu süre abonelik süresince ve abonelik iptalinden itibaren otuz yıl olarak belirlenmiştir. Söz konusu süre, 18 Ocak 2022 tarihinde Tüketici Hakları Yönetmeliği'ne getirilen değişiklik ile güncellenmiş olup; bu tarihten önce ilgili belgelerin saklama süresi, abonelik süresince ve abonelik iptalinden itibaren on yıl olarak belirlenmişti. Bu sürenin on yıldan otuz yıla çıkartılması hususundaki gerekçe, haberleşme sektörünün ceza soruşturmaları ve devamındaki süreçte adli vakaların aydınlatılmasında önemli bir yardımcı sayılmasıdır. 5237 sayılı Türk Ceza Kanunu'ndaki dava zamanaşımı ve 5352 sayılı Adli Sicil Kanunu'nda belirtilen kesinleşmiş ceza ve güvenlik tedbirlerine ilişkin verilerin saklanmasına ilişkin süreler en fazla otuz yıl olarak belirlendiğinden; bunlarla uyumlu olacak şekilde abonelik sözleşmesi ve sözleşmenin kurulmasıyla ilgili belgelerin saklanması süresi otuz yıl olarak belirlenmiştir.[512]

Elektronik haberleşme sektöründe abonelik sözleşmesi ve ilgili diğer belgelerin abonelik süresince ve iptalinden sonra da otuz yıl boyunca saklanması hususunun, Adli Sicil Kanunu'nun 12/1-(b) maddesinde belirtilmiş olan maddeden kaynaklandığı düşünülmektedir.[513]

---

[512] 5352 sayılı Adli Sicil Kanunu'nda adli sicil ve arşivdeki kişisel verilerin imhası konusu ele alınmıştır. İlgili kanunun 1. ve 2. maddeleri uyarınca, kesinleşmiş ceza ve güvenlik tedbirlerine ilişkin veriler Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü'nde bulunan Merkezi Adli Sicil'de tutulmaktadır. Adli Sicil Kanunu'nun usul ve esasları ile ilgili birimlerin görev dağılımını belirlemek üzere Adli Sicil Yönetmeliği yayımlanmıştır. Söz konusu Kanun'un 12. maddesinde ve ilgili Yönetmeliğin 13. maddesinde adli sicil kayıtlarına ilişkin verilerin silinme süreleri belirlenmiştir.

[513] Söz konusu Adli Sicil Kanunu'nun 12/1-(b) maddesinde, Anayasa'nın 76. maddesi ve TCK dışında hak yoksunluğuna sebebiyet teşkil edecek mahkumiyetlerin arşivde kaydının alınmasından itibaren yasaklanmış hakların geri verilmesi kararı alınması şartıyla on beş yıl geçtiğinde kayıtların silinmesi gerekmektedir. İlgili hükümde yer alan bu şart aranmaksızın otuz yıl geçtiğinde ise arşiv kayıtları tamamıyla silinecektir. Ayrıca TCK'nın 66. maddesinde ağırlaştırılmış müebbet hapis cezasını gerektiren suçlar için otuz yıllık ceza zamanaşımı süresi öngörülmektedir.

Adli Sicil Kanunu'nda bahsi geçen sürelere uyum açısından abonelik sözleşmesi ve ilgili evrakın da otuz yıl saklanması, adli süreçlerin yönetimi açısından önem arz etmektedir. Saklama sürelerinin bu denli artırılmasının işletmeciler açısından risk teşkil ettiği ise aşikardır. Elektronik ortamda abonelik tesisi ile belgeler elektronik ortamda tutulabilmeye başlamış olsa bile; ıslak imzalı abonelik sözleşmelerinin yapılmaya devam edilebilmesi ve elektronik ortamda abonelik tesisi imkanından önce kurulan aboneliklerin ıslak imzalı sözleşmeleri ve ilgili diğer belgelerinin arşiv ortamında saklanmaya devam edilmesi durumu düşünüldüğünde; işletmecinin kişisel verileri saklama yükümlülüğü çerçevesinde arşiv kayıt sisteminin sağlıklı şekilde işliyor olması gerekmektedir. Bu durum, her şirketin elektronik haberleşme sektöründe işletmeci olma yeterliliğini kolaylıkla sağlayamayacağının göstergelerinden biridir.

Abonelik kuruluşunda kimlik belgesinin işletmeciye sunulmasındaki amaç ise abonelik başvurusunda bulunan kişi ile kimlik belgesindeki kişinin aynı kişi olduğunun doğrulanmasıdır. Tüketici Hakları Yönetmeliği'nin 7/8 maddesinde kimlik niteliğine haiz belgelerdeki bilgilerin doğruluğunun kontrolünün belgenin türüne göre farklılık gösteren servisler vasıtasıyla yapılması gerektiğine değinilmiştir. Yapılan bu doğrulama işlemine ilişkin alınan ekran görüntülerinin ise elektronik ortamda saklanması gerektiği belirtilmiştir. Abonelik tesisi esnasında alınan belgelerin doğrulama ekran görüntüleri de Tüketici Hakları Yönetmeliği'nin 7/8 maddesinde abonelik sözleşmesinin ayrılmaz bir parçası olarak görüldüğünden; abonelik sözleşmesiyle birlikte abonelik iptalinden itibaren otuz yıl daha saklanması gerekmektedir.

Elektronik haberleşme sektöründeki işletmecilerin, KVKK'nın 5/2 maddesinde belirtilen ilgili kişinin açık rızası olmaksızın kişisel verilerinin işlenebilir olması hallerinden olan sözleşmenin kurulması ya da ifasıyla ilgili olması ve veri sorumlusunun kendi hukuki mükellefiyetlerini sağlamak için kişisel verileri işlemesinin gerekmesi nedeniyle, abonelik tesisi esnasında kişiden kişisel verilerin bir kısmı alınmakta ve saklanmaya başlanmaktadır. Fakat abonelik tesisi denilen süreç anlık bir süreç olmadığından; belgelerin işletmeciye teslimi ve işletmecinin belgelerin doğruluğunu kontrolünden sonra aboneliğin aktivasyonunun sağlanması aşamaları tamamlandıktan sonra abonelik tesisi gerçekleştirilmiş olduğundan ve ancak bu halde abonenin hizmetleri kullanıma başlayabildiği düşünüldüğünde; ortalama birkaç gün süren bu süre zarfında abone tarafından vazgeçilmesi veya işletmeci tarafından belgelerin uygun olmaması

sebebiyle aboneliğin başlatılmama durumuyla karşılaşılabilmektedir. Bunun gibi durumlarda abone tarafından işletmeciye evrak sunularak veya beyanla verilen birtakım kişisel veriler olabilmektedir. Abonelik tesis edilmemesine rağmen işletmeci tarafından abonenin kişisel verilerinin işlenmesi ve saklanması hallerinde işletmecilerin nasıl hareket etmesi gerektiği KVK Kurulu tarafından incelenmiştir.

KVK Kurulu, 26.08.2021 tarihli ve 2021/859 sayılı kararında; internet aboneliği hizmeti almak isteyen şahsın adresine gelerek abonelik tesisi işlemlerini yürütmek isteyen veri sorumlusunun çalışanı tarafından, abonelik başlatmak isteyen kişinin abonelik sözleşmesi vasıtasıyla tüm bilgilerinin alınmış olmasına rağmen kimlik belgesinin fotoğrafı çekilmek istendiği belirtilmiştir. KVK Kurulu, veri sorumlusu işletmecinin Tüketici Hakları Yönetmeliği'nin 7/6-(a) maddesi uyarınca kimlik belgesinin örneğinin asılları üzerinden uygun şekilde alarak elektronik ortama aktarılması gerektiğine yönelik yükümlülüğü olduğundan bahisle, ilgili kimlik belgesi fotoğrafının KVKK'nın 5/1-(c) ve 5/1-(ç) maddeleri uyarınca işlendiğine ilişkin yapmış olduğu savunmanın yerinde olduğuna yer vermiştir. Abone olmak isteyen kişi tarafından kimlik belgesi fotoğrafının üzerine "müstenidattır" ifadesinin not düşülmesini istemesine rağmen veri sorumlusu çalışanı tarafından bunun yapılamayacağı bilgisi kendisine iletilmiştir. Bu nedenle şahıs, ilgili firmadan abonelik başlatmaktan vazgeçtiğini bildirerek veri sorumlusu tarafından alınan kişisel verilerinin de derhal silinmesini talep etmiştir. İlgili kişinin bu talebine karşılık KVK Kurulu, veri sorumlusunun ilgili kişinin sadece abonelik sözleşmesi kurulabilmesi için asgari düzeyde bilgilerini aldığı, kimlik fotoğrafı çekilmesi aşamasına geçilmediğini, ileride yaşanabilecek ihtilaflarda veri sorumlusunun savunma hakkını kullanılabilmesi için asgari düzeydeki kişisel verilerin amaçla uyumlu olacak şekilde yine asgari süre boyunca saklanabileceğini belirtmiştir. Veri sorumlusunun bu konuda talimatlandırılmasına, idari yaptırım kararı uygulanacak bir veri ihlalinin ise gerçekleşmemiş olduğuna karar vermiştir.[514]

İlgili kararda, veri sorumlusu işletmecinin en azından savunma hakkını kullanabilmesi amacıyla abonesi olmayan kişinin asgari düzeyde verisini saklaması uygun görülmüştür. Her ne kadar söz konusu kararda savunma hakkının korunabilmesi amacıyla veri işleme faaliyeti hukuka uygun olarak nitelendirilse de uygulamada

[514] KVK Kurulu'nun 26.08.2021 tarihli ve 2021/859 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7135/2021-859 , Erişim Tarihi: 25 Ekim 2022.

elektronik haberleşme sektöründeki işletmecilere yargı makamları veya kolluk kuvvetleri tarafından kişilerin işletmecide herhangi bir abonelik kaydının olup olmadığı dahi sorulabilmektedir. Bu durumda işletmeciler, kişi henüz abonesi olmasa da abone olma talebinde bulunduğuna ilişkin tutulan kayıtlarını ilgili makama sunmakla yükümlüdür. Diğer bir deyişle, kişiler henüz işletmecinin abonesi olmasa da bu kişiler hakkında işletmecilerden bilgi talep edilebildiği için işletmecilerin savunma hakkının yanı sıra hukuki yükümlülüğünü yerine getirebilmek amacıyla da ilgili kişinin verisini işlediği söylenebilir.

Kimlik Doğrulama Yönetmeliği hükümlerine uygun olarak uzaktan abonelik yapılması durumunda ise ilgili Yönetmeliği'nin 9/3 maddesinde belirtildiği üzere, işletmeci tarafından abonelik sürecindeki doğrulamaların işlendiği işlem belgesinin uzun süreli saklamaya olanak sağlayan PAdES-LTV formatına dönüştürüldükten sonra mevzuatta belirlenen süre boyunca saklanması öngörülmüştür. Bu süre, Tüketici Hakları Yönetmeliği'nde bahsedilen abonelik sözleşmesi ve sözleşmeyle ilgili diğer belgelerin saklanması için öngörülen abonelik süresi boyunca ve devamında otuz yıldır. İlgili 9. madde hükmünün 4. ve 5. fıkrasında belirtildiği üzere, kimlik doğrulamaya ilişkin yapılan tüm işlemlerin kayıt altına alınarak saklanması gerekmektedir. Ayrıca ilgili hükümde işlem kayıtlarının da mevzuatta yer verilen sürelere uygun olarak saklanması gerektiği belirtildiğinden; söz konusu kayıtların da abonelik süreciyle ilgili olması sebebiyle yine abonelik süresi boyunca ve devamında otuz yıl boyunca saklanması uygun olacaktır.

2.2.3. Aboneliğin Kullanımıyla Ortaya Çıkan Trafik ve Konum Verilerinin Saklanması

Saklama fiili aynı zamanda işleme davranışının içerisinde kabul edildiğinden[515] ve trafik ve konum verilerine dair diğer işleme faaliyetleri hakkında ayrıntılı bilgilere İkinci Bölüm'de yer verilmiş olduğundan; bu bölümde yalnızca bu verilerin saklanması ve saklanma süreleri konusuna değinilecektir.

Kişisel Verilerin İşlenmesi Yönetmeliği'nde, kişinin gerçekleştirdiği haberleşmenin iletilmesi ve iletişimle ilgili arabağlantı veya faturalama amacıyla işlenen veriler olarak adlandırılan trafik verileri ile terminal cihazının konumunun tespitiyle birlikte bireyin konumunun tespit edilebilmesini sağlayan veriler olarak adlandırılan

[515] Saklama da dahil olmak üzere veriye yapılan her türlü faaliyet işleme olarak adlandırılmaktadır. (Determann, *KVK Uygulama Kılavuzu*, XXIX.)

konum verileri, Anayasa'nın 22. maddesiyle de ayrıca korunan haberleşmenin gizliliği ilkesiyle bağlantılı olduğundan; işletmeciler tarafından işlenirken ve saklanırken daha dikkatli olunması gereken veri grubudur. Nitekim EHK'nın 51/9 maddesinde de trafik ve konum verilerinin ancak kullanıcı şikayeti olması durumunda ya da BTK'nın denetim faaliyetleri kapsamında işlenebileceğine yer verilmiş olup; söz konusu trafik ve konum verilerinin nasıl saklanabileceğine ilişkin ayrıntılara, ilgili 51. madde hükmünün 2., 7. ve 8. fıkralarında yer verilmiştir.

Elektronik haberleşme sektöründe trafik verilerinin saklanmasına ilişkin temel düzenleme EHK'nın 51. maddesinin 2. ve 7. fıkralarıdır. EHK'nın 51/2 maddesinde; haberleşmenin gizliliğinin esas olduğu, haberleşmenin taraflarının rızası olmadan kesintiye uğratılamayacağı, takip edilemeyeceği, dinlenemeyeceği, kayıt altına alınamayacağı ve saklanamayacağı belirtilerek; bunun istisnasının ancak mevzuat veya yargı kararları olabileceğine yer verilmiştir.

EHK'nın 51/9 hükmünde abone şikayetleri olması veya denetimlerin varlığı halinde trafik verilerinin işlenebileceği hususu çerçevesinde, EHK'nın 51/7 hükmünde trafik verilerinin, abone veya kullanıcıyla işletmeci arasında fatura, haberleşme vasıtasıyla hukuka aykırı eylemler, arabağlantı gibi hususlardan doğan anlaşmazlıkların çözümünde, yalnızca işletmeci tarafından yetki verilen kişiler tarafından işlenebileceği ve uyuşmazlığa konu süreç tamamlanana kadar saklanması gerektiği belirtilmektedir. Hizmetlerin pazarlamasının yapılması veya katma değerli hizmetlerin sunumu için trafik veya konum verileri işlenmek istendiği takdirde ise bu veriler anonimleştirilmeli ya da iletişimi gerçekleştiren tarafların rızalarının bulunması kaydıyla, bilgilendirmesi yapılan konularda ve sürede işleme faaliyetinin gerçekleştirilmesi gerekmektedir.

Konum verilerinin işlenmesi konusu ise EHK'nın 51/8 maddesinde düzenlenmiştir. Buna göre, mevzuatın öngördüğü haller veya yargı kararları doğrultusunda kişinin konum verilerinin işlenebileceği, bunun dışında ise acil durumların varlığı halinde 5902 sayılı Kanun'da belirtilen afet hali veya acil durumlarda kişilerin rızası olmadan da yalnızca konum verisi ve kişinin kimlik bilgilerinin yine yalnızca yetkilendirilmiş kişiler tarafından işlenebileceğine yer verilmiştir.

EHK'nın 51/8 maddesinde belirtildiği üzere, 5902 sayılı Kanun'da yer verilen afet ya da acil durumlar halinde kullanıcının rızası olmasa bile konum verilerinin işlenebileceğine yer verilmiş olup; konunun ayrıntısına ve işleme süresine Acil Yardım

Yönetmeliği'nin 5/2 maddesinde değinilmiştir. İlgili madde uyarınca, elektronik haberleşme sektöründeki işletmeciler, Acil Yardım Merkezleri'ne göndermiş oldukları konum bilgisini 1 yıl saklamakla yükümlü kılınmıştır.

Trafik ve konum verilerinin saklanmasına ilişkin EHK ve Kişisel Verilerin Korunmasına İlişkin Yönetmelik'te çeşitli hükümlere yer verilmiş olsa da saklama sürelerine ilişkin ayrıntılı bir bilgi bulunmamaktadır. EHK'nın 51/7 maddesinde yer alan hüküm gereğince, abone veya kullanıcının rızasının bulunduğu hallerde trafik ve konum verileri, rıza alınmadan önce kişiye bildirilen süre kadar işlenebilecek, dolayısıyla da bu süre boyunca saklanabilecektir. Bununla birlikte, kişinin rızasının bulunmadığı hallerde bu verilerin işletmeciler tarafından ne kadar süre boyunca saklanabileceğine dair kesin bir süre belirten herhangi bir hüküm bulunmamaktadır.

EHK'nın 51/10 maddesinde, veri kategorileri çerçevesinde haberleşmenin gerçekleştiği andan başlayacak şekilde en az bir yıl en fazla ise iki yıl olacak şekilde söz konusu trafik verilerinin saklanabileceği anlaşılsa da ilgili kesin sürenin yönetmelik ile belirleneceğine yer verilmesine rağmen Kişisel Verilerin İşlenmesi Yönetmeliği'nde bu konuya dair herhangi bir süreye yer verilmemiştir. Bununla birlikte, bahsi geçen veri kategorisi ifadesi de mülga olan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik'in[516] 13. maddesinde belirtilen veri kategorileridir. İlgili Yönetmeliğin yürürlükten kaldırılmış olması ve halihazırda uygulanan Kişisel Verilerin İşlenmesi Yönetmeliği'nde ise veri kategorisi olarak adlandırılan bir terim bulunmamasına rağmen; EHK'nın söz konusu 51/10 hükmünde henüz herhangi bir değişiklik yapılmamıştır.

Ayrıca mülga Yönetmeliğin 14. maddesinde trafik verilerine ilişkin haberleşmenin başlangıç - bitiş zamanı ve süresi, iletişimi gerçekleştiren telefon numaraları veya kişiye özgülenen kullanıcı kimlikleri gibi ayrıntılı kategorilerin, iletişimin gerçekleştiği andan başlayacak şekilde bir yıl boyunca, gerçekleşmeyen aramalara ilişkin verilerin ise üç ay boyunca saklanması gerektiğine dair bir hüküm olmasına rağmen; Kişisel Verilerin İşlenmesi Yönetmeliği'nde mülga Yönetmelik'in aksine yalnızca kişisel verilere ve bununla alakalı sistemlere ilişkin işlemlerin kayıtlarının

[516] 24 Temmuz 2012'de Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, Kişisel Verilerin İşlenmesi Yönetmeliği'nin Resmi Gazete'de yayımlandığı tarih olan 4 Aralık 2020 tarihinde mülga olmuştur.

iki yıl boyunca saklanmasına ilişkin süreden bahsedilmiş olup; trafik ve konum verisine dair herhangi bir süreye rastlanılmamaktadır.

Keza EHK'daki 51/10 hükmünde belirtildiği gibi kişisel verilere veya bu verilerle ilgili olan sistemlere erişildiğini gösteren kayıtların ise iki yıl boyunca saklanması gerektiğine yer verilmişken; ilgili mülga Yönetmelik'te bu süre 14/3 maddesi gereğince dört yıl olarak belirlenmişti. İlgili hükümler incelendiğinde ve EHK'nın 51. maddesinin 2014 yılında iptal edilerek yeni düzenlemenin 2015 yılında yürürlüğe girdiği ve Kişisel Verilerin İşlenmesi Yönetmeliği'nin 16. maddesinde belirtildiği üzere ilgili mülga Yönetmeliğin, Kişisel Verilerin İşlenmesi Yönetmeliği'nin yürürlüğe giriş tarihi olan 4 Aralık 2020'ye kadar uygulanmaya devam ettiği göz önünde bulundurulduğunda; bu süre zarfında mülga Yönetmelik hükmünün 5809 sayılı Kanun'da belirtilen sınırı aştığı gözlemlenmektedir.

2.3. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK ALINAN TEKNİK VE İDARİ TEDBİRLER

Elektronik haberleşme sektöründe abone desen yapısıyla başlayan ve milli güvenliğin korunması amacına hizmet eden BTK kurul kararlarının yanı sıra bilgi ve iletişim güvenliğinin sağlanması adına, verilerin dijital ortama taşınması ve verilerin saklandığı altyapıların dijital hale gelmesiyle birlikte güvenlik açıklarının oluşması ihtimali göz önünde bulundurularak; 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır.[517]

Bu doğrultuda, "Bilgi ve İletişim Güvenliği Rehberi"[518] oluşturularak; bahsedilen risklerin en aza indirilmesi ve hukuka aykırı şekilde erişilebildiğinde milli güvenliği tehdit edebilecek ya da kamu düzeninin bozulmasına sebep olabilecek nitelikteki verilerin güvenliğinin sağlanabilmesi için birtakım tedbirler alınması gerekliliği vurgulanmıştır.[519]

Bilgi ve iletişim güvenliğinin temel kuralları; geliştirilen sistemlerin tasarım aşamasından başlayarak tüm sistemin ve özellikle kişisel verileri içeren bölümlerin güvenli olmasının sağlanması ve verileri işleyecek olan personelin güvenlik konusunda

[517] R.G. 06.07.2019, S. 30823.
[518] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, Temmuz 2020, https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf , 11, Erişim Tarihi: 28 Ekim 2022.
[519] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, IV.

gerekli eğitimlerden geçmiş olmasıdır. Bununla birlikte, sistemlerde saldırı olabileceği düşünülen alanların güvenlikli hale getirilmesi, sistem açıklarının tespit edilerek en az güvenlikli olduğu düşünülen bölge hakkında güçlendirme çalışmalarının planlanması, saldırılara karşı birden fazla savunma ekipmanı sağlanması ve yurtdışı menşeili ürün kullanarak verilerin yurtdışına aktarılmasını en aza indirebilmek için yerli ve milli ürünlerin kullanılması da güvenliğe ilişkin temel hususlardan diğerleridir.[520] Tüm teknik ve idari tedbirlerin bu prensipler doğrultusunda gerçekleştirilmeye çalışılması halinde daha etkin sonuçlar alınabilecektir.

Türk hukukunda kişisel verilerin korunması mevzuatının temeli olan KVKK'da bu konuya ilişkin olarak 12/1-(c) maddesinde veri sorumlularının, gerekli tedbirler alarak kişisel verilerin güvenliğinin sağlanmasından sorumlu olduğu belirtilmiştir. İlgili hükmün yanı sıra elektronik haberleşme sektöründe ise kişisel verilerin korunmasına yönelik olarak tedbir alınması gerektiğine EHK'nın 51/4 maddesinde yer verilmiş olup; işletmeciler, verdikleri elektronik haberleşme hizmetlerinin güvenliğini temin etmek ve bu hizmetlerden faydalananların kişisel verilerini koruyabilmek için gerekli teknik ve idari tedbirleri almakla yükümlü kılınmıştır.

Söz konusu iki hüküm doğrultusunda, Kişisel Verilerin İşlenmesi Yönetmeliği'nin 6/5 maddesinde işletmecilerin abone veya kullanıcılarına sundukları hizmetler dolayısıyla elde ettikleri verilerin güvenliğinden sorumlu olduklarına yer verilmiştir.

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 6. maddesinin devamında ise EHK'nın 51/4 maddesi uyarınca işletmecinin alması gereken tedbirlerin nasıl uygulanabileceğine yer verilmiştir. Bu doğrultuda, işletmecinin elde ettiği kişisel verileri KVKK'ya uygun şekilde işleyebilmesine yönelik teknik ve idari önlemleri alması gerektiği belirtilmiştir. Burada bahsedilen tedbirlerin en azından hangi düzeyde olması gerektiğine, ilgili 6. madde hükmünün 2. fıkrasında yer verilmiş olup; öncelikle, kişisel verilerin korunmasına yönelik ilkeler kapsamında olacak şekilde işletmeci tarafından güvenlik politikalarının belirlenmesi gerekmektedir. Bununla birlikte, işletmeci tarafından aslında gerçekleştirilmek istenmeyen işleme faaliyetlerinin gerçekleşmesi gibi durumlara karşı, veriye erişimi veya işleme yetkisi bulunmayan kimseler tarafından veriyi değiştirme, kaydetme, ifşa gibi çeşitli işleme faaliyetinin gerçekleşmesi ya da verilerle

[520] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 30-31.

ilgili hukuka aykırı birtakım faaliyetlere karşı kişisel verilerin korunmasını sağlayacak gerekli önlemlerin alınması gerektiği belirtilmiştir. Abonelere ait kişisel verilerin saklandığı ortamların güvenliğinin sağlanması ise ayrıca düzenlenmiştir.

Kişisel verilerin korunması ve hukuka aykırı şekilde işlenmesinin önlenmesi amacıyla işletmecilerin tedbir alması elzemdir. BTK tarafından, işletmecilerin gerekli tedbirleri alıp almadığı, alınan tedbirlerin uygun olup olmadığı konusunda denetleme, bilgi talep etme yetkisinin yanı sıra söz konusu incelemenin ardından BTK'nın uygun görmediği tedbirlerin değiştirilmesini isteme yetkisi bulunduğuna, Kişisel Verileri İşleme Yönetmeliği'nin 6/3 maddesinde yer verilmiştir.

2.3.1. Teknik Tedbirler

Kişisel verileri işleyen işletmecilerin öncelikli olarak dikkat etmesi gereken husus, sistem ve kullanılan ağların güvenliği konusunda gerekli ve ciddi teknik tedbirlerin alınmasını sağlamaktır. Bu doğrultuda, donanım elemanlarının güvenliği ile başlayan süreç, işletmede kullanılan yazılımların güvenliği ve ağ güvenliğinin sağlanmasıyla devam etmektedir.[521]

2.3.1.1. Donanım Elemanlarının Güvenliği

Donanım elemanları genel anlamda, işletmede kullanılan bilgisayar, sabit disk, taşınabilir disk gibi unsurlardan oluşmaktadır. Donanım elemanlarının güvenliğinin sağlanabilmesi için, söz konusu cihazların envanterinin çıkartılmasının ardından kullananların kim olduğunun ve denetiminin sağlanması amacıyla kimlik denetiminin yapılması gerekmektedir. Kullanım ömrü sona eren ve kişisel verileri depolamaya yarayan sabit disk, harici bellek gibi cihazların güvenli bir şekilde imha edildiğinden emin olunması gerekmektedir.[522]

Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin, güvenlikle ilgili alınacak tedbirler konusunda KVKK ve EHK'nın yanı sıra BTK tarafından yayımlanan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği[523] (Bilgi Güvenliği Yönetmeliği) hükümlerine uygun şekilde davranmaları gerekmektedir. Bu Yönetmelik'te öncelikle işletmecinin kullandığı donanım

[521] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 1.
[522] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 36.
[523] R.G. 13.07.2014, S.29059.

elemanlarının güvenliğinin sağlanması gerektiği anlaşılmakta olup; 19. maddesinde donanım elemanlarının su, havalandırma gibi sistemlerden etkilenmeyecek şekilde gerekli çevresel tehditlerin önlenmesine yönelik tedbir alınması gerektiği belirtilmiştir. Bununla birlikte; aynı Yönetmeliğin 20/3 hükmünde, taşınabilir cihazlar ya da mobil cihazlardan kaynaklanabilecek güvenlik zafiyetlerine karşı cihazlara yetkisiz erişimin engellenmesi gibi çeşitli tedbirlerin alınması gerektiği belirtilmiştir.

2.3.1.2. Yazılım Elemanlarının Güvenliği

Donanım elemanlarının yanı sıra işletme içerisindeki faaliyetlerin yürütülmesinin sağlanması konusunda temel unsurlardan bir başkası ise yazılım elemanlarıdır. Bilgi Güvenliği Yönetmeliği'nin 21. madde hükmünden işletmenin kullandığı şebekelerin ve geliştirmiş olduğu uygulamaların güvenliğini sağlamasına yönelik olarak işletme içerisinde kullandığı yazılımların güvenliğinin sağlanması gerektiği anlaşılmaktadır. İşletme içerisinde kullanılan yazılımların onaylı kütüphanelerden yüklenerek onaylı ve dijital imzalı yazılımların çalıştırılmasının sağlanması, otomatik yazılım güncellemelerinin bulunduğuna dikkat ederek otomatik olmayanların takibinin sağlanması ve risk tespiti yapılarak işletmenin teknik anlamda tehditlerinin neler olabileceğinin tespitinin yapılması, beyaz liste dışındaki yazılımların indirilmesini önleyici tedbirleri almak gibi önlemler ise yazılım elemanlarının güvenliğinin sağlanması adına alınabilecek teknik tedbirlerden bazılarıdır.[524] İşletmenin e-posta sunucularına gelen zararlı bağlantılara erişim yapılamamasının sağlanmasının ise e-posta yoluyla sistemlere sızılabilmesinin önüne geçebilmek için ilk aşama olduğu söylenebilir.[525] Bilgi Güvenliği Yönetmeliği'nin 26. maddesinde de işletmenin sistemlerine saldırıların önlenebilmesi için işletme içerisinde kullanılan yazılımların zararlı kodlara karşı korunabilmesi amacıyla alınacak tedbirlere örnek olarak; yazılımları koruyucu tedbirlerin alınması, lisanssız yazılım kullanılmaması, işletmenin ağı dışındaki bir ağdan yazılım indirilmesinin önlenmesi gösterilmiştir.

2.3.1.3. Ağ Güvenliğinin Sağlanması

Ağ güvenliğinin sağlanması ise alınması gereken teknik tedbirlerin en önemlilerindendir. İşletme içerisinde kullanılan ağlarda kara liste ve beyaz liste

[524] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 38-40.
[525] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 44.

uygulamasıyla erişilebilen internet sayfalarının sınırlandırılması, ağların güvenliği için kullanılan güvenlik ve antivirüs programlarının güncel sürümlerinin kullanılmasının sağlanması, işletme ağlarının DoS ve DDoS saldırılarına[526] karşı korunması için önlem alınması, ayrıca misafir ağı oluşturulması[527] gibi pek çok kişinin kişisel verisinin işlendiği elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin, ağ güvenliğini sağlayabilmesi için alabileceği tedbirler bulunmaktadır.

Bilgi Güvenliği Yönetmeliği'nin 20/1 maddesinde elektronik ortamda muhafaza edilen bilgilere yetkisiz erişimin engellenebilmesi için gerekli önlemelerin alınması gerektiğinden bahsedilmektedir. İşletme içerisinde kullanılan şifrelerin belirli sürelerde güncellenmesi ve güçlü şifreler belirlenmesinin sağlanması, önemli verilerin aktarılmasında VPN teknolojileri, SSL gibi güvenli protokollerin kullanılmasının sağlanması[528] ise yalnızca şirket içi elemanların güvenliğinin sağlanması için değil, işlenmekte olan kullanıcılara ait kişisel verilerin güvenliğinin sağlanması için de önem arz etmektedir. Nitekim Bilgi Güvenliği Yönetmeliği'nin 22. maddesinde belirtildiği üzere; işletmecinin abonenin bilgilerini koruyabilmek için abonenin bilinçlendirilmesinin yanı sıra işletmecinin kendisine tahsis edilmiş IP adresi kullanmak suretiyle dışarıdan gelecek saldırıları önlemeye yönelik tedbirleri alması gerektiği belirtilmiş olup; abonenin kendisine atanmamış bir IP adresi ile sistemlere zarar verebilecek işlem yapmasını da önlemeleri gerektiği belirtilmiştir.

2.3.1.4. Veri Güvenliğine İlişkin Alınan Teknik Tedbirler

İşletme içerisinde kullanılan sistemlere girişte oturum açarken kullanıcıların kimliğinin tespitini sağlayacak mekanizmaların kurulmasını sağlama ve söz konusu oturum açma mekanizmalarına saldırı olma ihtimali göz önünde bulundurularak IP

[526] Kamu kurumları ya da özel kuruluşların sistemlerine saldırı yaparak, bu sistemlerin yoğunluklarını artırarak ağ trafiğinin artması sonucunda hizmetlerin kullanılmasına engel olmaya yönelik faaliyetler DoS ve DDoS saldırıları olarak adlandırılmaktadır. (Haydar Yener Arıcı, *Adli Bilişim*, Ankara: Seçkin Yayıncılık, 2018), 246.
[527] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 49-50.
[528] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 57.

bloklama[529], CAPTCHA[530] gibi önlemlerin alınmasını sağlamak;[531] yaşanabilecek sızmaların önüne geçilebilmesi açısından elzemdir.

İnternet sayfalarının genel anlamda güvenliğinin sağlanabilmesinin başında gelen alınması gereken en önemli teknik tedbirlerden biri de internet sitesinin "HTTPS" protokolüne göre hazırlanmasıdır. "HTTP" protokolü, internet sitesini kullanan kişiler ile sitenin sunucusu arasında bilgi aktarımına ilişkin kuralları düzenleyen iletişim protokolü olarak adlandırılmaktadır.[532] Bir HTTP oturumunun tehlikeye girmesi halinde, aktarılan verilerin bütünlüğü ve kullanılabilirliğinin olumsuz şekilde etkilenmesi söz konusu olabilmektedir.[533] İnternet sitesine giriş yapmak isteyen kullanıcı, alan adının başına "HTTP" yazmasa bile otomatik olarak adresin başına bu protokol eklenmektedir, aksi halde sitedeki bilgilere erişim mümkün olmamaktadır. "HTTP", kişiye yalnızca veriyi sunmakla ilgilenmekte olup; sunulan verinin korunması veya üçüncü kişilerle paylaşılmaması gibi veri güvenliğine ilişkin durumlarla ilgilenmemektedir.[534] "HTTPS" ise "HTTP"nin SSL/TLS gibi kurallar vasıtasıyla şifrelenerek daha güvenli hale getirilmiş versiyonudur.[535] "HTTPS", güvenli bir kanal oluşturmayı amaçlayarak kullanıcılar ile internet sitesi arasındaki veri aktarımı esnasında şifreli bir kanal kullanılarak daha güvenli bir etkileşim yaşanmasını sağlamaktadır.[536]

"HTTPS" protokolünün kullanıldığı url adreslerine erişimin engellenmesi uygulanamadığından; bu protokolün kullanımının yaygınlaşmasıyla bir url'ye erişimin engellenmesi yöntemi de giderek azalacak; içeriğin yalnızca internet sitesinin sunucusu

---

[529] IP engelleme olarak da adlandırılan IP bloklama, erişimin engellenmesi talebinde bulunulan içeriğin IP bloklama yöntemiyle engellenebilmesi için içeriği yayınlayan sunucunun IP adresinin engellenmesi suretiyle gerçekleştirilmektedir. Bu yöntemle engelleme gerçekleştirildiği takdirde, o IP adresinden yapılan tüm yayınlar bu durumdan etkilenmekte olup; hepsi engellenmektedir. (Mehmet Bedii Kaya, *İnternet Hukuku*, (İstanbul: On İki Levha Yayıncılık, 2021), 79.)

[530] CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart - İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Test), insan ile bilgisayar arasında ayrım yapabilmek için soru-cevap şeklinde yapılan doğrulama testi olarak bilinen güvenlik önlemidir. CAPTCHA, kişiden bir test çözmesini talep ederek; bir hesaba izinsiz şekilde girmek isteyen bilgisayarın önlenmesi ve soruyu çözenin gerçek kişi olduğunun kanıtlanmasını sağlamaktadır. Bu yöntemde genellikle, parçalı şekilde bir fotoğraf gösterilerek; fotoğrafın içerisindeki bazı parçaların kişi tarafından bulunması ya da bozuk şekilde görünen harf ve sayı bütününün kişi tarafından bilinerek belirtilen alana yazılması istenilmektedir. (Google Workspace Yöneticisi Yardım, "CAPTCHA nedir?," https://support.google.com/a/answer/1217728?hl=tr . Erişim Tarihi: 28 Ekim 2022.)

[531] CB Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, 66-69.

[532] Kaya, *İnternet Hukuku*, 20.

[533] Henk C.A. van Tilborg, Sushil Jajodia, *Encyclopedia of Cryptography and Security*, (New York: Springer, 2011), HTTP Session Security, 568.

[534] Kent, *Erişimin Engellenmesi*, 68-69.

[535] Kaya, *İnternet Hukuku*, 20.

[536] Kent, *Erişimin Engellenmesi*, 69.

tarafından müdahale edilebileceğinden erişimin engellenmesinin gerektiği hallerde alan adının tamamının engellenmesi yoluna gidilmek zorunda kalınacaktır.[537] Bu sebeple "HTTPS" protokolüne sahip internet sitesinin tamamen kapanmaması amacıyla internet sitesinde yapılan yayınlarda daha dikkatli olunmak isteneceği açıktır.

"HTTPS" protokolüne göre hazırlanmış olan internet sitesinden ödeme yapılması, "HTTP" protokolüne göre hazırlanmış olan siteye göre daha güvenli olduğundan, elektronik haberleşme sektöründeki işletmeciler tarafından da bu protokol türü tercih edilerek kullanıcıların veri güvenliğinin sağlanması amaçlanmaktadır.

2.3.1.5. Güvenlik Denetimlerinin Gerçekleştirilmesi

İşletme içerisinde kullanılan elemanların genel olarak güvenliğinin sağlanmasına yönelik alınan tedbirler, verilerin tam anlamıyla korunabildiği anlamına gelmemektedir. Alınan tedbirlere rağmen herhangi bir sızıntının olup olmadığının tespiti amacıyla düzenli aralıklarla sızma testlerinin[538] yapılması, güvenlik açıklarının tespit edilmesi ve herhangi bir saldırı olmadan var olan eksikliklerin giderilmesi açısından önem taşımaktadır. Nitekim KVKK'nın 12/3 maddesinde de güvenliğin sağlanması amacıyla veri sorumlularının kendi işletmelerinde gerekli denetimleri yapması gerektiğine yer verilmiştir. Bununla birlikte, işletme sistemlerine herhangi bir saldırı veya sızıntı gerçekleşmesi sonucunda veri kaybı yaşanması halinde, işletmenin faaliyetlerine devam edebilmesi açısından verilerin yedeklenmiş olması da ayrıca önem arz etmektedir. Bilgi Güvenliği Yönetmeliği'nin 27. maddesinde yer aldığı üzere, bilgi ve yazılımların belirli periyotlarda yedeğini almak gerekmekte olup; işletmecinin hangi verilerin yedeğinin alınacağına ilişkin gerekli düzenlemeleri yapması gerektiği belirtilmiştir. Alınan yedeklerin test edilmesi gerekmekte olup; diğer bilgilerin maruz kalabileceği tehlikelerden uzak olacak şekilde başka bir yere kaydının yapılması gerekmektedir.

---

[537] Kent, *Erişimin Engellenmesi*, 70.

[538] Sızma testi, bilgi sistemlerindeki açıkların tespit edilmesinde kullanılan güvenlik testleri olarak adlandırılmaktadır. (BGA Security, "10 Soruda Sızma Testi Nedir?," bgasecurity.com, https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/ , Erişim Tarihi: 28 Ekim 2022.) Bu testler, bilgi teknolojileri güvenlik risk yönetiminin bir parçası olarak kabul edilmektedir. Bu testler, işletmenin güvenlik sorunlarına ilişkin gerçekçi sonuçlar ortaya çıkartmasına rağmen; bu testlerin işletmenin güvenliğinin değerlendirilmesi için yalnızca bir bileşen olduğu unutulmamalıdır. (Sean-Philip Oriyano, *Penetration Testing*, (Indianapolis: Sybex, 2017), 58.)

2.3.1.6. Elektronik Haberleşme Sektörüne Özgü Alınan Teknik Tedbirler

Örnekseme yoluyla yukarıda yer verilen ilgili tüm teknik tedbirler, aboneliğin yapılış şekli yüz yüze de olsa uzaktan da olsa elektronik haberleşme hizmetinin güvenli şekilde abonelere sunulmasını ve hizmeti kullanan abone veya kullanıcıların kişisel verilerinin yanlış kullanımlarının önlenerek korunmasını sağlayacağından; bu tedbirlerin yerine getirilmesi gereken temel nitelikteki tedbirler olduğu açıktır.

Genel anlamda sayılan bu teknik tedbirlerin yanı sıra elektronik haberleşme sektöründeki işletmeciler, toplu SMS gönderimi veya santrale dahili belirleme gibi aboneliklere ilişkin çeşitli işlem ve kullanım takiplerinin gerçekleştirilebildiği abonelik arayüzlerine giriş esnasında, aboneliklerin abonenin bilgisi dışında kullanımlarının önlenebilmesi amacıyla; genellikle tek şifre değil, iki aşamalı doğrulama sistemi kullanmaktadır. Söz konusu iki aşamalı doğrulama sistemiyle, ilk aşamada o hizmete ilişkin aboneye verilen şifrenin girilmesinden sonra ikinci aşamaya geçilmektedir. Abonenin işletmecinin sistemine kayıtlı cep telefonu numarasına gönderilen tek kullanımlık şifrenin sisteme girilmesiyle arayüze giriş yapılabilmesine imkan sağlanmaktadır. İkinci aşamada abonenin cep telefonuna gönderilen doğrulama kodu vasıtasıyla abonenin izni ve bilgisinin olmadığı kimseler tarafından aboneliklere giriş yapılarak abonenin rızası dışında işlemlerin gerçekleşmesinin önüne geçilebilmektedir.[539]

İki aşamalı doğrulmaya ilişkin KVK Kurulu ilke karar[540] yayımlamış olup; bu kararda Kişisel Veri Güvenliği Rehberi'nde[541] yer verilen iki kademeli doğrulamanın işletmeler ve kurumlar tarafından kullanılması gerektiğine yer verilmiştir. İlgili kararda tek kademeli doğrulama kişinin yalnızca bir tane kişisel verisisin sorgulandığı sistem, iki kademeli doğrulama ise ilk kademede sorulan, kişiye özel bilginin yanı sıra uygulama tarafından kişiye atanan özel şifre veya kişinin cep telefonuna gönderilen tek kullanımlık şifre vasıtasıyla giriş yapılması şeklinde tanımlanmıştır. KVK Kurulu söz konusu kararda, tek kullanımlık şifrenin kişisel verilerin korunması açısından yüksek riskli bir yöntem olduğunu, güvenliğin sağlanması açısından iki kademeli şifre sisteminin

[539] Turkcell İletişim Hizmetleri A.Ş., https://hizligiris.com.tr/hizligiris/generic/sms_otp , Erişim Tarihi: 28 Ekim 2022.
[540] KVK Kurulu'nun 21.04.2022 tarih ve 2022/388 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/7252/2022-388 , Erişim Tarihi: 28 Ekim 2022.
[541] KVK Kurumu, Kişisel Veri Güvenliği Rehberi, 2018, https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf , Erişim Tarihi: 28 Ekim 2022.

benimsenmesinin daha uygun olacağını bildirmiştir. Anayasa'ya göre haberleşmenin gizliliğinin esas olması ve söz konusu ilke karar doğrultusunda, elektronik haberleşme sektöründeki işletmecilerin de iki kademeli şifre sistemini benimsemeleri uygun bir teknik tedbir olarak adlandırılabilecektir.

Kimlik Doğrulama Yönetmeliği uyarınca uzaktan kurulabilen abonelik sözleşmelerinin yapılabilmesinden sonra bahsi geçen önlemlere ek olarak başka tedbirlerin de alınması gerektiği belirtilmiştir. İlgili Yönetmeliğin 7/1 maddesinde yer verildiği üzere, görüntülü kimlik doğrulamasında işletmecinin risklerin farkında olarak gerekli güvenlik tedbirlerini alması gerekmektedir. Aynı hükmün 2. fıkrasında ise görüntülü şeklide yapılan kimlik doğrulaması işleminde, işletmecinin görsel ve işitsel olan video kaydının bütünlüğü ve ortaya çıkan ve başvurucu tarafından paylaşılan verilerin gizliliğinin sağlanması amacıyla gerekli tedbirleri alması gerektiğine değinilmiştir. Bu doğrultuda, söz konusu doğrulama işlemi, uçtan uca güvenli iletişim[542] vasıtasıyla gerçekleştirilmektedir.

Kimlik Doğrulama Yönetmeliği uyarınca abonenin kimliğinin doğrulanması sonucunda elde edilen verilerin saklanmasına yönelik alınması gereken teknik tedbirlere ise ilgili Yönetmeliğin 5/3 maddesinde ayrıca yer verilmiştir. İlgili maddede, kimlik doğrulama yoluyla elde edilen bilgilerin şifreli şekilde ve matematiksel anlamda eski haline getirilemeyecek şekilde saklanmasına, üçüncü taraflara şifrelenerek gönderilmesine, yetkisiz kişilerin söz konusu kişisel verilere erişimlerine, verilerin ilgili kişiye bildirilen amaç dışında kullanılmasına karşı gereken tedbirlerin alınarak; yapılan işlemlerin kayıt altında tutulması gerektiğinden bahsedilmektedir.

Uzaktan kimlik tespiti yapılarak abonelik tesisi Kimlik Doğrulama Yönetmeliği ile mümkün kılınmış olsa da kimliğin doğrulanması esnasında kimlik sunan kişinin kimlikte adı geçen gerçek kişi olup olmadığının tespiti yükümlülüğü işletmecide bulunmakta olup; ilgili Yönetmeliğin 7/9 maddesinde, kimliği sunan şahıs ile kimlikte adı geçen kişinin uyuşmaması gibi durumlarda ya da belgenin geçerliliğine ilişkin başka bir durumun varlığı halinde veya dolandırıcılık, sahtecilik gibi hukuka aykırı bir halin varlığına dair şüphe oluşması halinde görüntülü kimlik doğrulama sürecinin işletmeci

[542] Uçtan uca şifreleme (End-to-end encryption-E2EE), standart metin karakterlerinin sadece iletişimin tarafları arasında okunabilir şekilde gizli hale getirilmesini sağlayan algoritma kullanma işlemidir. Amaç, iletişimi gizli şekilde dinlemek isteyen potansiyel dinleyicilerin, konuşmayı dinlemesinin engellenmesidir. (IBM, "What is end-to-end encryption?," ibm.com, https://www.ibm.com/topics/end-to-end-encryption , Erişim Tarihi: 28 Ekim 2022.)

tarafından derhal sonlandırılması gerektiği belirtilmiştir. Bahsi geçen kimlik avı veya sahtecilik hallerine karşı tedbirlerin işletmeci tarafından alınması beklenmektedir.

Kimlik Doğrulama Yönetmeliği'nin 10. maddesinde, işletmecilerin hizmetlerini sunarken güvenliği sağlamalarına yönelik olarak EHK, KVKK ve ulusal ve uluslararası alanda belirlenmiş olan standartlara uygun şekilde hizmet verebilmek için tedbir almaları gerektiğine yer verilmiştir. Bu doğrultuda elektronik haberleşme hizmeti sunan işletmecilerin Bilgi Güvenliği Yönetmeliği hükümlerine uygun şekilde davranmaları hüküm altına alınmıştır. Ayrıca ilgili hükmün 3. fıkrasında işletmecinin, kimlik tespitine ilişkin gerçekleştirilmek istenen sahtekarlık gibi suçların önlenebilmesi amacıyla teknolojideki gelişmeleri takipte kalarak devamlı olarak sisteminde gereken güncellemeleri yapması gerektiği belirtilmiştir.

2.3.2. İdari Tedbirler

Kişisel verilerin korunması konusunda idari tedbirler genel olarak, gerçekleşebilecek risklerin değerlendirilmesi, veri sorumlusunun personelinin eğitilmesi, veri işleyenler ile kişisel verilerin korunması ve işlenmesi konusunda ilişkilerin yürütülmesi, KVKK konusunda şirketin politika ve prosedürlerinin belirlenmesinin yanı sıra işlenen kişisel verilerin olabildiğince azaltılmasına yönelik alınan önlemler olarak adlandırılabilmektedir.[543] Diğer bir ifadeyle işletmeciler tarafından alınması gereken idari tedbirlerin, işletme faaliyetlerinin yürütülmesi kapsamında, kişisel verilerin işlenmesi konusunda takip edilen prosedürün hazırlanmasının yanı sıra elde edilen verilerin işletme içerisindeki erişimlerini ve verileri işleyen personel veya işletmenin çalışma gerçekleştirdiği iş ortağı gibi üçüncü kişilerle paylaştığı kişisel verilerin korunmasına yönelik alınan güvenlik tedbirlerini kapsadığı söylenebilir.

2.3.2.1. Risk Değerlendirmesinin Yapılması

İşletmeciler tarafından öncelikli olarak işlenen kişisel verilerin neler olduğunun tespitinin yapılarak; bu verilere ilişkin risklerin değerlendirilmesi ve bu doğrultuda izlenmesi gereken yollara ilişkin gerekli prosedürün oluşturulması gerekmektedir.[544] İşlenen verilerle ilgili gerçekleşebilecek risklerin tespitinin yapılması önemli olmakla birlikte; işletme tarafından olabildiğince az sayıda kişisel veri işlenmesiyle

[543] KVK Kurumu, Veri Güvenliği Rehberi, iv.
[544] KVK Kurumu, Veri Güvenliği Rehberi, 8.

karşılaşılabilecek ihlallerin de bir o kadar az olacağı unutulmamalıdır. Özellikle, işleme amacının ortadan kalktığı veya veri işleme süresi sona eren verilerin imha edilerek işletme bünyesinde tutulmaya devam edilmesinin önüne geçilmesi, işletmeci lehine olan bir durumdur.[545]

2.3.2.2. Çalışanlara ve Diğer Veri İşleyenlere Yönelik Alınan İdari Tedbirler

Risk değerlendirmesinin yapılması kadar önemli olan bir diğer husus ise risklerle karşı karşıya kalan çalışanlara yönelik alınması gereken idari tedbirlerdir. Veri sorumlusu adına verileri işleyen personelin eğitilmesi ve kişisel verilerin korunması konusunda bilinçlendirilmesi gerekmektedir. Nitekim KVKK'nın 12/4 maddesinde belirtildiği üzere, veri işleyenler, işleme sırasında bilgi sahibi oldukları verileri üçüncü kişilere açıklayamayacaktır. Bu kişilerin, görevleri bitse dahi sorumluluklarının devam edeceğine söz konusu hükümde yer verilmiştir. İlgili hükümden, veri işleyenlerin faaliyetlerine karşı da önlem alınması gerektiği sonucu çıkartılabilmektedir.

İşletme içerisinde gerçekleşebilecek veri kaybı veya üçüncü taraflardan karşılaşılabilecek veri müdahalelerine karşı çalışanlara eğitim verilerek hazırlıklı olmaları sağlanmalıdır. Yapılan bu farkındalık çalışmalarıyla tecrübesizlik veya dikkatsizlik gibi sebeplerle veri kaybına yol açılması hallerinin yaşanmaması hedeflenmektedir. Personelin işyerindeki görev tanımı belirlenerek sorumlu olduğu veri grubu konusunda bilinçlenmesi sağlanmalıdır. İşletme içerisinde gerçekleştirilen faaliyetlerin yasaklanmadığı müddetçe serbest olduğu düşüncesinin aksine, izin verilene kadar yasak olduğu kanaatiyle davranılması gerektiği konusunda kurum bilinci oluşturulmalıdır.[546]

Çalışanların yanı sıra veri sorumlusuyla birlikte verileri işleyen bir diğer grup ise işletmenin hizmet aldığı ve bu hizmetten faydalanabilmek için kendisinin işlemekte olduğu kişisel verileri aktarması gereken veri işleyen grubudur. İşletme içerisinde veri sorumlusunun kişisel verilerin korunmasına yönelik tedbir almasının yanı sıra hizmet aldığı başka bir işletme olan veri işleyenin de kendi içerisinde aynı özeni göstermesi gerekmektedir. Aksi takdirde veri sorumlusu ne kadar dikkatli davransa da kendisinin öncelikli olarak sorumlu olduğu kişisel verilerin korunmasının veri işleyen diğer işletme

[545] KVK Kurumu, Veri Güvenliği Rehberi, 12.
[546] KVK Kurumu, Veri Güvenliği Rehberi, 9.

tarafından ihlal edilmesi nedeniyle veri kaybı veya izinsiz kullanım gerçekleşebilmektedir.

KVKK'nın 12/2 hükmü gereğince, veri işleyen işletme, veri sorumlusu işletmeci ile müştereken sorumludur. Bu doğrultuda, veri işleyenin de sorumluluğunun bilincinde olarak işleme faaliyetlerini gerçekleştirebilmesi için alınabilecek idari önlemlerden biri de veri işleyen ile gizlilik ve kişisel verilerin korunmasına yönelik maddelerin bulunduğu sözleşme imzalanmış olmasıdır. Veri sorumlusu tarafından, veri işleyenin güvenlikle ilgili gerekli teknik ve idari tedbirleri aldığına yönelik rapor hazırlayarak gerekirse yerinde denetim yapması da alınması gereken bir diğer önlemdir.[547]

2.3.2.3. Kişisel Veri İşlemeye Yönelik Gizlilik Sözleşmesi Hazırlanması, Politika ve Prosedür Oluşturulması

KVKK'da bahsedildiği üzere önem verilen gizlilik sözleşmesi hazırlanmasına ilişkin tedbire, Bilgi Güvenliği Yönetmeliği'nin 32. maddesinde de yer verilmiş olup; elektronik haberleşme sektöründeki işletmecilerin çalışanları, mal ve hizmet tedarik ettikleri şirketler ile gizlilik hükümlerine yer verilen sözleşme yapmaları ve bu sözleşmeleri saklamaları gerekmektedir. Gizli bilginin tanımına, sözleşmenin ne kadar süre ile geçerli olduğuna, hangi hallerde tarafların gizli bilgiyi kullanabileceklerine, taraflara getirilen yükümlülüklere, gizliliğin ihlal edilmesi halinde yapılacak işlemlerin neler olduğuna ilişkin hususlara gizlilik sözleşmesi ya da gizlilik hükümlerini içeren sözleşmelerde yer verilmesi gerektiği bildirilmiştir. Bununla birlikte, ilgili hükmün 3. fıkrasında değinildiği üzere; söz konusu kişilerle yapılacak olan bu sözleşmeler, veri sorumlusu olan işletmecinin sorumluluğunu ortadan kaldırmamaktadır.

İşletme içerisinde verileri işleyen çalışanlara gerekli eğitimler verilse de veri kaybı yaşandığında veya izinsiz veri işleme faaliyetinin gerçekleştiği tespit edildiğinde nasıl davranılması gerektiğine ilişkin işletmenin politika ve prosedürlerinin olması gerekmektedir. Bu prosedürlerin, acil şekilde tedbir alınması ve gerekli bildirimlerin yapılabilmesi için henüz veri ihlali yaşanmadan işletmeci tarafından hazırlanmış olması gerekmektedir. Bununla birlikte, prosedürlerin bir diğer faydası ise işletme içerisinde rutin kontrollerin yapılarak kayıt altına alınması sağlanarak; veri ihlaline karşı risklerin

[547] KVK Kurumu, Veri Güvenliği Rehberi, 12-13.

farkında olunarak; bu sayede, muhtemel gerçekleşebilecek risklere karşı henüz veri ihlali gerçekleşmeden önlem alınabilmesine imkan sağlanmasıdır.[548]

2.3.2.4. Elektronik Haberleşme Sektörüne Özgü Alınan İdari Tedbirler

Kişisel Verilerin İşlenmesi Yönetmeliği'nin 6/4 maddesinde yer verilen kişisel verilere ve işletmecinin sistemlerinde gerçekleşen erişimlere yönelik yapılan işlem kayıtlarının iki yıl boyunca saklanması yükümlülüğünün işletmeci açısından idari tedbir alınması konusunda da yorumlanması gerekmektedir. İşletmecilerin personellerinin veya bayilerinin abonelik işlemlerini yürütebilmek amacıyla abonenin veya kullanıcının kişisel verilerine yapılan erişimlerin ve işleme faaliyetlerinin ne zaman ve işletmenin hangi personeli veya bayisi tarafından gerçekleştirilmiş olduğunun takibinin yapılması, verilerin güvenliği açısından önem arz etmektedir. Ayrıca KVKK'nın 12/2 maddesinde yer verilen veri sorumlusu ile verileri veri sorumlusu adına işleyenlerin, kişisel verilerin korunması ve gereken tedbirlerin alınması konusunda müştereken sorumlu olduğu doğrultusunda, kişisel verilerin güvenliğini tehlikeye atacak herhangi bir durum olması halinde, işletmeciler tarafından gerçekleştirilen işleme faaliyetlerine ilişkin saklanan kayıtların incelenmesi söz konusu olacaktır.

Uzaktan abonelik kurulması esnasında, kimliğin doğrulanması yöntemlerinden biri olan yetkili marifetiyle kimlik doğrulama yöntemine ilişkin işletmeciler tarafından alınması gereken idari tedbirlerden Kimlik Doğrulama Yönetmeliği'nin EK-3'ünde bahsedilmektedir. İlgili EK-3'ün 2. paragrafında, kimlik doğrulama işlemini yürütecek olan personele eğitim verilmesi ve her yıl bu eğitimin yenilenmesinin yanı sıra kişisel verilerin korunması mevzuatı da dahil olmak üzere kimlik doğrulama mevzuatında değişiklik olması halinde bu değişiklik sonrasında da eğitimin yenilenmesi gerektiği belirtilmiştir. Ayrıca ilgili mevzuatta belirtildiği üzere, işlemleri gerçekleştirecek olan yetkilinin, abonelik sürecini başlatan kişinin özgür iradesiyle işlemleri yürütüp yürütmediğini anlayabilme konusunda eğitimli olması şarttır. Personelin, görev tanımı çerçevesinde kişisel verilere erişiminin de işletmeci tarafından sınırlandırılmış olması gerekmektedir.

[548] KVK Kurumu, Veri Güvenliği Rehberi, 11.

Elektronik haberleşme sektöründe işlenmesi konusunda birçok özel hüküm bulunan trafik verilerinin aktarılması konusunda da özenli davranılması için gereken idari tedbirlerin alınması gerektiğine yönelik Anayasa Mahkemesi kararı bulunmaktadır.

Anayasa Mahkemesi'nin 2014/149 E. ve 2014/151 sayılı kararıyla 2 Ekim 2014 tarihinde iptal edilen 5651 sayılı Kanun'un 3/4 maddesinde yer alan trafik bilgisinin TİB tarafından işletmeciden alındıktan sonra bir hakim kararı olması halinde başka kurumlara ilgili trafik verilerinin aktarılabileceğine ilişkin hükmün iptal kararında karşı oy açıklamasında bulunulmuştur. Buna göre, gerekli tedbirlerin alınarak uygulanması halinde ilgili hükmün iptal edilmesine gerek olmadığına ilişkin yapılan açıklamada; ilgili Kanun hükmüyle kişisel verilerin korunması hakkına açıkça müdahale edildiğinin ortada olmasına karşılık, söz konusu işleme faaliyetinin Anayasa'da yer verilen amaçlardan biri olan suçların önlenmesi gibi amaçlar doğrultusunda işlenmesi sebebiyle işleme faaliyetinin hukuka uygunluk nedeninden yoksun olmadan gerçekleştirildiği ifade edilmiştir. Elektronik haberleşme sektöründe yetkili kurumların veya diğer yetkili kamu kurum ve kuruluşlarının görevlerini yerine getirebilmeleri amacıyla ihtiyacı olan bilgi ve belgeleri temin etmekte Anayasa'ya aykırılık olamayacağı belirtilmiştir. Karşı oy olarak; Anayasa Mahkemesi'nin 2 Haziran 2011 tarihli kararıyla BTK'ye 5809 sayılı Kanun'un 6/1-(ı) maddesi ile verilen ihtiyacı olan bilgi ve belgeyi temin etme yetkisinin özel hayatın ya da haberleşmenin gizliliğine aykırılık teşkil etmeyeceği düşüncesiyle ilgili hükmün iptali talebinin reddedildiği gerekçesinin, söz konusu iptali istenen ve TİB'e trafik verisinin aktarılması yetkisinin konu alındığı 5651 sayılı Kanun'un 3/4 maddesinde de geçerli olacağı karşı oy olarak belirtilmiştir. Ayrıca ilgili karşı oyda, suçların önlenebilmesi için trafik verilerinin ancak hakim kararı olması halinde TİB tarafından diğer kurumlarla paylaşılabileceği hususunun orantısız bir yetki olmadığı düşüncesi vurgulanmıştır. Bununla birlikte, ülkemizce de imzalanarak tarafı olunan Sanal Ortamda İşlenen Suçlar Sözleşmesi[549] 16. maddesinde, bilgisayar ortamında saklanan verilerin kaybolma ve değiştirilme gibi hallere karşı korunabilmesi için sözleşmeye taraf devlet tarafından acil şekilde yasal tedbir ve işletmeci tarafından ise idari tedbirlerin alınması gerektiğine yer verilmiştir. İlgili Sözleşme'nin 17. maddesiyle özellikle trafik verilerinin korunmasına ilişkin alınan idari ve yasal tedbirlerin yanı sıra devletin yetkili kurumları

[549] Sanal Ortamda İşlenen Suçlar Sözleşmesi, https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf , Erişim Tarihi: 28 Ekim 2022.

vasıtasıyla trafik verilerinin işletmecilerden kısa sürede temini için gerekli yasal tedbirlerin alınması gerektiği belirtilmiştir. Bu doğrultuda idari tedbirlerin temin edilmesi gerektiğine yer verilmiştir. Bahsi geçen sebeplerle karşı oyda, iptal edilen 5651 sayılı Kanun'un 3/4 maddesinin aslında ülkemizin uluslararası sözleşmelerde taahhüt ettiği hususları yerine getirmek amacıyla düzenlenmiş olduğu belirtilmiştir.[550]

3. KİŞİSEL VERİLERİN İMHASI

Kişisel verilerin korunması hukukunda, verilerin toplandıktan sonra hukuka uygun işlenmesinin yanı sıra işleme süresi veya amacı sona eren verilerin imha edilerek saklanmaya devam edilmemesi önem arz etmektedir.

Veriler herhangi başka bir işleme faaliyetine tabi tutulmasa bile KVKK'nın 3/1-(e) maddesinde belirtildiği üzere saklama faaliyeti de işleme faaliyeti kapsamında kabul edilmektedir. İmha zamanı gelen verinin imhasının gerçekleştirilmeden saklanmaya devam edilmesi halinde, veri işleme faaliyetinin hukuka uygunluk nedeni ortadan kalktığından; imhanın gerçekleştirilmemesi, hukuka aykırı olarak veri işlemeye devam edilmesi sonucunu ortaya çıkarmaktadır.

Verilerin imhası, tamamen ortadan kaldırılması veya erişiminin kısıtlanması şeklinde farklı şekillerde gerçekleştirilebilmektedir.[551] İmha kavramı, hukuk sistemlerinde farklı şekillerde adlandırılabilmekte olup; bu çalışmada, AB hukuku ve Türk hukukundaki ele alınış biçimlerine göre sınıflandırılarak bu kavram incelenmeye çalışılacaktır. Söz konusu incelemeden önce, imha kavramıyla bağlantılı olan ve dijitalleşmenin artmasıyla birlikte son zamanlarda sıkça adından söz edilen unutulma hakkına yargı kararları bağlamında yer verilecektir.

3.1. UNUTULMA HAKKI

Geçmişte, geleneklerin korunması ve toplumların gelişmesi bakımından hafıza, ilerlemenin temel bir unsuru olmuştur. Günümüzde ise geçmiş zamanların aksine,

---

[550] AYM, 02.10.2014 ve 2014/149 E., 2014/151 sayılı Kararı, https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-151-nrm.pdf , Erişim Tarihi: 29 Ekim 2022.

[551] Dülger, KVK Hukuku, 604.

internete yerleştirilen bir bilginin potansiyel olarak silinemez ve sonsuza dek hatırlanma yeteneğini haiz olması; insani ve hukuki açıdan, teknolojik ilerlemenin istenmeyen bir yönüdür.[552] İnsan hafızası, bir bilgiyi zaman geçtikçe unutma özelliğine sahipken; internete kaydedilen bilgi, silinmediği sürece sonsuza dek saklanabilmektedir. İnternet üzerinde verilerin bu şekilde sürekli saklanabilir olmasının yararlarının yanı sıra bireyler açısından unutulmama durumunun maddi ve manevi yönden yıkıcı etkileri olabilmektedir.[553]

AİHS'in 8. maddesinde düzenlenen özel hayatın gizliliğinin, unutulma hakkının temelini oluşturduğu düşünülmektedir.[554] Unutulma hakkı, günümüzde ağ teknolojilerindeki gelişmeler ve bilgilerin saklanma gerekliliği sebebiyle önem kazanan, kişinin özel yaşamını ilgilendiren ve gizlilik kavramıyla örtüşen kişiye sıkı sıkıya bağlı olan bir haktır.[555] Bu hak kısaca, kişilere ait dijital ortamlarda bulunan verilerinin tekrar geri getirilmeyecek şekilde imha edilmesidir. Tüm bu tanımlar doğrultusunda unutulma hakkının elektronik ortamlarda yayımlanan içeriklere ilişkin kullanılabilen bir hak olduğu açıktır.[556]

GDPR'ın 17. maddesinde unutulma hakkı, "silme hakkı (unutulma hakkı)" olarak adlandırılmıştır. Doktrinde bir yanda, silme hakkı ile unutulma hakkının bazen aynı anlamda, bazen ise farklı anlamlarda kullanıldığına ilişkin[557] ya da unutulma hakkı ile silme hakkının birbirinden farklı olduğuna[558] dair görüşler mevcuttur. Bir başka görüşte ise; unutulma hakkının, dijital çağın gereği olarak silme ve düzeltme haklarının daha işlevsel şekilde kullanılmasına yönelik bir hak olduğu, silme ve düzeltme hakkının bir uzantısı sayılabileceği düşünülmektedir.[559] Buna karşılık silme hakkı ile unutulma hakkının aslında aynı hak olduğuna, yalnızca GDPR'ın 17. maddesinde ifade ediliş

---

[552] Angelo Maietta, "The Right to be Forgotten," Revista de Estudos Constitucionais Hermenêutica e Teoria do Direito (RECHTD), 12(2): 208, https://revistas.unisinos.br/index.php/RECHTD/article/view/rechtd.2020.122.03 , Erişim Tarihi: 29 Ekim 2022.
[553] Yılmaz, *Kişisel Verileri Koruma Hukuku*, 62-63.
[554] Yılmaz, *KVK Hukuku*, 63.
[555] Maietta, "The Right to be Forgotten," 209.
[556] Seray Nalbantoğlu, "Bir Temel Hak Olarak Unutulma Hakkı," *Türkiye Adalet Akademisi Dergisi* 9, no.15 (2018): 589.
[557] Küzeci, *Kişisel Verilerin Korunması*, 257.
[558] Olgun Değirmenci, "Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler)," *Terazi Hukuk Dergisi* 13, no.144 (2018): 154.
[559] Çekin, *KVK Hukuku*, 133.

biçiminde farklılık olduğuna dair açıklamalar[560] da bulunmaktadır. Çalışmada bu kavramların farklılığına dair tartışmaya yer vermeden, ABAD ve Anayasa Mahkemesi kararları doğrultusunda unutulma hakkı incelenecektir.

3.1.1. Els Alfacs Kararı

1978'de kamp alanında kimyasal madde taşıyan kamyonun kaza yapması sebebiyle iki yüze yakın kişinin öldüğüne dair haberlere ilişkin olarak 2010 yılında bile Google'a kamp alanının adı yazıldığında şirketin adının bu haberle anılması üzerine, Google Spain'e yapılan başvurunun cevapsız kalması sonucunda şirket, unutulma hakkı, mahremiyet ve imajının korunması hakkına dayanarak; olayla ilgili bilgi almak isteyen kişilere gösterilecek haberle ile kamp alanı hakkında bilgi almak isteyen kişilere gösterilecek bilgiler arasında ayrım yapılması gerektiğini talep ederek dava açmıştır. Olay ilk yaşandığında dava sürecindeki gelişmeler hakkında halka bilgi verme amacıyla haberlerin yayınlanmış olması ve olayın üzerinden bir müddet geçtikten sonra da ülkede olayla ilgili çeşitli manevi ve ekonomik değerlere ilişkin zarar ortaya çıkmış olması nedeniyle yayınlanmaya devam edilmesinde kamuya bilgi verme amacı bulunduğu açık olsa da olayın üzerinden yaklaşık otuz yıl geçtikten sonra kamuyu ilgilendiren bir amaç kalmadığından; ilgili haberlerin Google'ın listesinde yayınlanmasını gerektiren durumun ortadan kalktığı iddia edilmiştir.[561]

İlgili kararda, veriyi işleme amacı ortadan kalktıktan sonra işleme faaliyetine devam edildiğinden; ABAD olayın üstünden uzun yıllar geçmesi sebebiyle olayın herkes tarafından görülebilir olmasını uygun bulmamıştır. Bu doğrultuda ilgili karar, unutulma hakkının ABAD tarafından açıkça tanındığını gösteren bir karar niteliğinde olmuştur.[562]

---

[560] Information Commissioner's Office (ICO), "Right to erasure," ico.org.uk, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ , Erişim Tarihi: 29 Ekim 2022.

[561] Ana Azurmendi, "Spain: The Right to Be Forgotten The Right to Privacy and the Initiative Facing the New Challenges of the Information Society," ed. Wolf J. Schünemann, Max-Otto Baumann, Privacy, Data Protection and Cybersecurity in Europe, (Cham, Switzerland: Springer, 2017), 23, https://link.springer.com/chapter/10.1007/978-3-319-53634-7_2 , Erişim Tarihi: 29 Ekim 2022; Dülger, *KVK Hukuku*, 494.

[562] Dülger, *KVK Hukuku*, 494.

3.1.2. Google - İspanya Kararı

Google-İspanya kararı[563], unutulma hakkının mahkeme kararları vasıtasıyla tanınmasının sağlanması açısından önemli bir karar niteliğindedir. Sosyal güvenlik borçlarının yapılandırılması amacıyla taşınmazını satmak durumunda kalan İspanyol avukat Mario Costeja Gonzalez, konuya ilişkin gazete haberlerinin gazetenin dijitalleştirilmesi sonrasında Google arama motoru üzerinden Mario Costeja Gonzalez adını arattığında güncelliğini yitirmiş kişisel ve finansal verileriyle karşılaşmıştır. Avukatın ismiyle yapılan haberlerin geçerliliğini yitirmesi sebebiyle halen Google'da yayınlanmaya devam etmesi üzerine, 95/46/EC sayılı Direktif doğrultusunda kişisel verinin işlenme amacını yitirmesi sebebiyle hukuka aykırı olduğu ileri sürülerek silinmesini talep etmesine rağmen; İspanyol Veri Koruma Otoritesi (SDPA) tarafından ifade özgürlüğü çerçevesinde ilgili haberlerin yayınlandığı gerekçesiyle avukatın talebinin reddedilmesine karar verilmiş; diğer yandan Google'a haberi silmesini değil, haberleri dizine eklemeyi bırakmasını söylemesine rağmen Google tarafından bu talebe itiraz edilmiştir. Bunun üzerine, İspanya Yüksek Mahkemesi'nde açılan davada, söz konusu olay ABAD'a ön soru olarak yöneltilmiştir.[564] ABAD, söz konusu davada 95/46/EC sayılı Direktif hükümlerini unutulma hakkını içerecek şekilde yorumlamıştır.

ABAD'ın kararı, vatandaşlar ile arama motorları arasındaki ihtilafların çözümünde bir araç olmuştur. Bundan böyle herkesin veriler yetersiz, ilgisiz veya güncel olmadığında arama motorundan verilerinin silinmesini isteme hakkı olduğuna yönelik toplum bilinci oluşmaya başlamıştır.[565]

3.1.3. Article 29 Çalışma Grubu'nun Google-İspanya Kararına İlişkin Rehberi

Article 29 Çalışma Grubu, Google-İspanya kararından sonra unutulma hakkına ilişkin rehber yayınlamıştır.[566]

---

[563] ABAD, Case C-131/12 numaralı, 13.05.2014 tarihli Karar, https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=155358 , Erişim Tarihi: 30 Ekim 2022.

[564] Azurmendi, "Right to Be Forgotten," 22; Dülger, *KVK Hukuku*, 493.

[565] Azurmendi, "Right to Be Forgotten," 29.

[566] Article 29 Çalışma Grubu, Guidelines on the Implementation of the Court Of Justice of the European Union Judgment on "Google Spain and Inc V. Agencia Española De Protección De Datos (Aepd) and Mario Costeja González" C-131/12, (2014), https://ec.europa.eu/newsroom/article29/items/667236/en , Erişim Tarihi: 30 Ekim 2022.

İlgili rehberde öncelikle bireyin mahremiyetinin arama motoru olan Google'ın ekonomik menfaatinden ve kullanıcıların bireyin kişisel verilerine erişme haklarından üstün olduğu belirtilmiştir. Unutulma hakkının kullanılabilmesi için menfaat dengesinin gözetilmesi gerektiğine değinilerek; kişisel verisi işlenen kişinin kamudaki yeri göz önünde bulundurularak bireyin menfaati ile toplumun bilgiye erişme hakkı arasında hangi yararın üstün olduğuna göre karar verilmesi gerektiği belirtilmiştir.[567]

Arama motorlarına gelen kişisel verilerin silinmesine yönelik taleplere, halkın çıkarları gözetilerek karar verilmesi gerektiği vurgulanmıştır. Toplumun çıkarları ön plandaysa, içeriklerin çıkartılmaması belirtilmiştir. Zaten içerik, kişisel veriye ilişkin aramaya yönelik sonuç listesinden çıkartılsa bile içeriğin halen kaynak internet sayfasında bulunmaya devam etmesi sebebiyle, ilgili içeriğe başka bir arama motoru vasıtasıyla erişilebilir olduğunun unutulmaması gerekmektedir.[568]

Article 29 Çalışma Grubu, arama motorlarına unutulma hakkıyla ilgili bir başvuru geldiğinde; başvuranın, verisi işlenen gerçek kişi olup olmadığına ilişkin kimlik tespitini yapmalarının uygun olacağını belirleterek; bu tespiti AB üye devletinin kendi yasalarına uygun şekilde gerçekleştirmeleri gerektiğine yer vermiştir. Bununla birlikte ilgili kişinin başvurusunda, unutulma hakkını kullanmak istediği verinin neden arama listesinden kaldırılmasını istediğini ayrıntılı şekilde açıklamasının uygun olacağından bahsedilmiştir.[569]

Arama motorunun listesinden yapılacak olan çıkartma işleminin yalnızca başvuranın bulunduğu ülkeden erişim sağlanabilen ulusal alan adları üzerinden değil, ".com" şeklindeki tüm ülkeleri kapsayacak şekilde yerine getirilmesi gerektiği yönünde Article 29 Çalışma Grubu görüşünü bildirmiştir. Yalnızca bu şekilde gerçekleştirilen işlemin bireyin menfaatini koruyucu etkide olacağına yer verilmiştir.[570]

Unutulma hakkı doğrultusunda bireyler tarafından arama motorlarına yapılan başvurular sonucu, arama motorlarının listelerinden yalnızca o kişiyle ilgili listeden çıkartma işleminin uygulanması gerekmekte olup; ilgili internet sayfasına arama motoruna başka bir terim yazılarak da ulaşılabiliyorsa bu durumun engellenmemesi önerilmektedir. Bununla birlikte ilgili Google-İspanya kararında, "isim" terimi

[567] Article 29 Çalışma Grubu, Google Spain Guidelines, 5-6.
[568] Article 29 Çalışma Grubu, Google Spain Guidelines, 6.
[569] Article 29 Çalışma Grubu, Google Spain Guidelines, 7.
[570] Article 29 Çalışma Grubu, Google Spain Guidelines, 9.

kullanıldığından; unutulma hakkının kişinin soy ismini de kapsadığı sonucuna varılabileceği belirtilerek; soy isim gibi çeşitli isim versiyonlarıyla da içeriğe erişimin mümkün olması sebebiyle söz konusu isimlerin de arama motoru listesinden çıkartılması gerektiği önerilmiştir.[571]

Arama motorlarına yapılan başvuruların değerlendirilmesi aşamasında, üye devletin kişisel verileri koruma otoritelerinin düzenlemelerinin bu konudaki AB düzenlemelerine uygun olup olmadığının değerlendirilebilmesi açısından Article 29 Çalışma Grubu tarafından çeşitli kriterler oluşturulmuş olup; üye devletlerin de veri koruma otoritelerinin bu kriterlere bakarak inceleme yapabileceğini belirtilmiştir. Söz konusu rehberde yayımlanan kriterlerden bazıları; başvuranın gerçek bir kişi olup olmadığı, başvuranın toplum içerisinde tanınır bir kimse olup olmadığı, içeriğin çalışma hayatına ilişkin olup olmadığı gibi hususlardır. Bu kriterler sınırlı sayıda olmayıp; üye devletler tarafından ulusal mevzuatlarına uygun olduğu ölçüde uygulanmaktadır. Bahsi geçen kriterlerden sadece birinin sağlanmış olması yeterli olmayıp, birkaç kriterin birlikte dikkate alınmış olması önerilmektedir. Bununla birlikte, Article 29 Çalışma Grubu tarafından kriterlerin özellikle toplumun bilgiye erişim hakkının sınırlanmayacak şekilde uygulanması gerektiği önerilmektedir.[572]

3.1.4. Anayasa Mahkemesi'nin N.B.B. Kararı

Başvuranın 1998 yılındaki uyuşturucu kullandığına ilişkin haberlerin 2013 yılında halen gazetenin internet arşivinde yayınlanmaya devam etmesi durumunun, itibarını zedelediği gerekçesiyle ilgili gazeteden haberlerin kaldırılmasına ilişkin erişimin engellenmesi talebiyle yargıya başvuran ilgili kişinin talebinin reddedilmesiyle birlikte; kişi, son olarak Anayasa Mahkemesi'ne başvurmuştur. Anayasa'nın 17. madde hükmünde yer verilen kişinin manevi bütünlüğünün korunması hakkı ve 20/3 maddesinde yer alan kişisel verilerin korunması hakkı birlikte değerlendirildiğinde; devletin bireye unutulma hakkı çerçevesinde yeni bir sayfa açma hakkı tanıması gerektiği belirtilmiştir. Söz konusu olayda başvuranın talebinin erişimin engellenmesiyle karşılanması halinin bu

[571] Article 29 Çalışma Grubu, Google Spain Guidelines, 9.
[572] Article 29 Çalışma Grubu, Google Spain Guidelines, 12.

hükümler doğrultusunda gerçekleştirilmesi gerektiği düşünüldüğünden; başvuranın talebi kabul edilmiştir.[573]

Görüldüğü üzere Anayasa Mahkemesi, her ne kadar Anayasa'da unutulma hakkına ilişkin herhangi bir hüküm yer almasa da manevi hakların korunması, özel hayatın gizliliği ve kişisel verilerin korunması gibi temel haklar doğrultusunda unutulma hakkının veri sahiplerine tanınması gerektiği doğrultusunda karar vermiştir.

3.1.5. KVK Kurulu'nun Unutulma Hakkında İlişkin Verdiği Kararlar

KVK Kurulu, 2020 yılında verdiği bir kararda, Anayasa Mahkemesi'nin N.B.B. kararına atıfta bulunarak; dijital hafızada tutulmaya devam eden gazete haberlerinin kişinin yaşamını olumsuz yönde etkiyebileceğini belirtmiştir. Ulusal kararların yanı sıra ABAD'ın Google-İspanya kararına da değinilerek; bireyin özel hayatının gizliliği hakkının kamunun bilgiye erişim hakkının üzerinde olduğuna yer verilmiştir. Bu kuralın ise yalnızca kamunun bilgiyi öğrenme konusundaki yararının bireyin menfaatinden daha üstün olduğuna karar verilmesi halinde uygulanmayacağının altı çizilmiştir. Her ne kadar iç hukukumuzda unutulma hakkı diye ayrıca belirtilmiş bir hak olmasa da Anayasa'nın 20/3 maddesi, KVKK'nın 4., 7. ve 11. maddeleri, Kişisel Verilerin Silinmesi Yönetmeliği'nin 8. maddesi gibi unutulma hakkını karşılayabilecek birçok hüküm bulunduğu belirtilmiştir. Bu doğrultuda, arama motorlarının arama listesinde içerikleri sınıflandırarak listelemesi faaliyetinin kişisel veri işleme faaliyeti olduğunun kabulüyle, ilgili kişilerin arama motorlarına kendi ad ve soyadıyla yapılan arama işlemi sonuçlarının listeden çıkartılmasına yönelik taleplerin, arama motorlarının kamu ve bireyin menfaatlerini gözetilerek karşılanması gerektiği belirtilmiştir.[574]

İlgili kararda, bireylerin unutulma hakkı doğrultusunda arama motorlarına başvurması halinde alınması gereken aksiyonların neler olduğuna ilişkin kriter listesi yayımlanmıştır.[575] İlgili kriterler, Article 29 Çalışma Grubu'nun Google-İspanya kararı

---

[573] AYM, 2013/5653 Başvuru numaralı, 03.03.2016 tarihli Karar, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 , Erişim Tarihi: 30 Ekim 2022.

[574] KVK Kurulu, 23.06.2020 tarih ve 2020/481 sayılı Kararı, https://www.kvkk.gov.tr/Icerik/6776/2020-481 , Erişim Tarihi: 30 Ekim 2022.

[575] KVK Kurulu, Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf , Erişim Tarihi: 30 Ekim 2022.

doğrultusunda hazırladığı rehberdeki kriterlere büyük oranda benzemektedir. Bahsi geçen kriterlerden bazıları; bilgilerin içeriğinin doğru olup olmadığı, başvuran kişinin toplumda önemli bir rolünün olup olmadığı, verilerin çalışma yaşamına yönelik olup olmadığı, arama sonuçlarındaki bilginin kişinin onurunu kırıcı hakaret içerip içermediği ve iftira niteliği taşıyıp taşımadığı ve arama sonuçlarının güncel bilgi niteliğinde olup olmadığı gibi hususlardır.

Her ne kadar KVK Kurulu tarafından yayımlanan ilgili kriterlerin adından ve içeriğinden arama motorları üzerinden yapılan aramalar için geçerli olduğu anlaşılsa da unutulma hakkıyla silme hakkının yalnızca farklı şekilde isimlendirildiği, içeriğinin aynı olduğu göz önünde bulundurulduğunda; söz konusu silme faaliyetine ilişkin kriterlerin yalnızca arama motorlarına yapılan başvurular için dikkate alınmaması gerektiği düşünülmektedir.

KVK Kurulu, yine aynı yıl içerisinde vermiş olduğu bir başka kararda ise atama işlemine ilişkin asılsız haberlerin yer aldığı haberlere arama listelerinde yer verilmemesi için arama motoruna başvuran ilgili kişinin talebinin reddedilmesi sonucunda; ilgili kişi tarafından KVKK'ya şikayet başvurusunda bulunulduğu belirtilmiştir. Arama motorunun listeleme işleminin kişisel veri işleme olduğu, Kurul tarafından yayımlanan kriterler kapsamında başvurunun değerlendirilmesi gerektiğine yer verilmiştir. Başvuran hakkında yayınlanan bilgilerin çalışma yaşamına yönelik olduğu, haberlerin 2020 yılı tarihli olması sebebiyle hala güncelliğini koruduğu, içeriğin gazetecilik faaliyeti kapsamında değerlendirilebileceği, ilgili kişi hala aynı işte çalıştığından bilginin kişiye bu anlamda zarar vermediğinin anlaşıldığı ve diğer kriterlere göre de yapılan değerlendirme sonucunda ilgili kişinin talebinin reddedilmesine karar verilmiştir.[576]

3.1.6. Elektronik Haberleşme Sektöründe Unutulma Hakkının Değerlendirilmesi

Unutulma hakkı, silme hakkıyla aynı işlevde olan bir haktır. Elektronik haberleşme sektöründe işlenen kişisel verilerinin silinmesini talep eden abone veya kullanıcılar, unutulma hakkı kapsamında işletmecilerden kişisel verilerinin silinmesini talep edebilmektedir. Fakat elektronik haberleşme sektöründeki işletmecilerin işledikleri çoğu veri işletmecinin yasal yükümlülüğünü yerine getirmesinden kaynaklı olduğu için

[576] KVK Kurulu, 08.12.2020 tarih ve 2020/927 sayılı Karar, https://www.kvkk.gov.tr/Icerik/6871/2020-927 , Erişim Tarihi: 30 Ekim 2022.

veri sahibi tarafından unutulma hakkı kullanılmak istendiğinde, her ne kadar işletmeci için artık o veri eski tarihte kalmış bir veri olsa da işletmeci, mevzuat uyarınca veriyi yalnızca saklama işlemine tabi tutmaktadır. Veri sorumlusunun abonelik sözleşmesi ve ek belgelerini saklama yükümlülüğü abonelik sona erdikten sonra otuz yıl daha devam ettiğinden; genellikle abonelerin bu talepleri karşılanamamaktadır.

3.2. AB DÜZENLEMELERİNE GÖRE İMHA

95/46/EC sayılı Direktif, "tanımlar" başlıklı 2. maddesinde kişisel verilerin işlenmesi açıklanırken, "silme ve yok etme kavramlarına" yer verilmiştir. Direktif'in "veri koruma ve veri güvenliği" başlıklı 7. maddesinde, "verilerin yok edilmesine" ilişkin uygun teknik ve idari tedbirlerin alınması gerektiği vurgulanmıştır. Son olarak, Direktif'in "denetim otoritesi" başlıklı 28. madde hükmünde, üye devletlerinin kamu makamlarının, izleme yükümlülüğünden söz edilerek, işleme faaliyetleri gerçekleşmeden önce görüş bildirmek ve bu görüşlerin yayınlanmasını sağlamak, verilerin silinmesini ya da yok edilmesini sağlamak gibi vazifelerinin olduğuna yer verilerek "verilerin yok edilmesi"nden söz edilmektedir. Direktif'in 6/e maddesinde, verilerin işlenme amaçları için gereken süreden daha uzun tutulmaması gerektiğine yer verilmiştir. Direktif'in 32/2 maddesinde, veri sahibinin talep etmesi halinde, erişim hakkını kullandığı sırada meşru amaçlar dahilinde uyumsuz olarak depolanmış bulunan verilerin düzeltilmesi, silinmesi ya da engellenmesi hakkının veri sahibine verilmesi gerektiği düzenlenmiştir.

2002/58/EC sayılı Direktif'te ise imha konusunda 6/1 maddesi bulunmakta olup; iletişim ağı ya da kamuya açık elektronik haberleşme hizmetinin sağlayıcısının işlediği trafik verilerinin iletişimin gerçekleştirilmesi için gerekli olmadığı zaman silinmesi ya da anonim hale getirilmesi gerektiğine yer verilmiştir.

GDPR'ın 4/2 maddesinde, kişisel verilerin işlenmesi tanımlanırken, "silme ya da imhanın" da kişisel verilerin işlenmesine dahil edildiğinden söz edilmiştir. Ancak burada geçen imha kavramıyla kastedilenin; KVKK'daki gibi silme, anonimleştirme veya yok etme kavramlarını kapsayan bir imha tanımı olmayıp; yok etmeyi karşılayan bir ifade olduğu anlaşılmaktadır.[577]

[577] Saka, "İmha," 45-46.

GDPR'ın 4/12 maddesinde, kişisel veri ihlalinin ne olduğuna ilişkin açıklama yapılırken; işlenen kişisel verilerin kazara ya da yasa dışı şekilde yok edilmesinden söz edilerek; bunun bir güvenlik ihlali teşkil ettiğine yer verilmiştir.

GDPR'ın 17. maddesinde unutulma (silme) hakkı doğrultusunda, kişisel verilerin toplanma ya da işlenme maksatlarıyla alakalı bundan böyle gereklilik teşkil etmemesi, veri sahibinin veri işlemeye ilişkin daha önce verdiği veri işlemeye ilişkin verdiği izni geri almış olması halinde ya da veri işlemenin gerçekleşmesine dair kanuni başka bir işleme koşulunun olmaması durumunda silme işleminin yerine getirilmesi gerekmektedir. Bununla birlikte, ilgili kişinin işleme faaliyetine itirazının olması ve bunun karşısında işleme faaliyetinin yapılmasına ilişkin meşru bir sebep olmaması, veri işleme faaliyetinin kanuna aykırı olarak yapılması veya daha önce işlenmiş olan kişisel verilerin silinmesinin kanuni olarak zorunlu olması gibi durumlarda da silinmeye ilişkin gereklilikler yerine getirilmelidir. Hükmün devamında, veri sorumlusu tarafından işlenen kişisel verilerin kamuya açıklanmış olması ve üçüncü kişilere aktarılması durumunda verilerin silinmesi, halihazırdaki teknoloji ve maliyetler dikkate alınarak; verilerin diğer veri sorumlularından veya veri sorumlusu adına veri işleyenlerden de verilerin silinmesinin sağlanması gerekliliği vurgulanmıştır.

GDPR'da anonimleştirmeye doğrudan yer verilmemiş olsa da 4/5 maddesinde "takma ad verme" şeklinde yapılan tanım incelendiğinde; kişisel verilerin ilgili kişiyle ilişkilendirilmeyecek şekilde işlenebileceğine yer verildiği görülmektedir. Takma isim verilmesi yoluyla bir veri tam olarak anonimleştirilememekte; veri anonimleştirilerek değil veri sahibine takma ad verilerek veriyle veri sahibi arasında ilişki kurulmasının önüne geçilmek amaçlanmaktadır.[578]

3.3. TÜRK HUKUKUNDA KİŞİSEL VERİLERİN İMHASI

Kişisel verilerin imhasına ilişkin Türk hukukunda bulunan temel düzenleme Anayasa'nın 20/3 maddesinde yer almaktadır. Bu düzenlemede imha kavramını karşılayacak şekilde kişisel verilerin silinmesi ifadesine yer verilmiştir. TCK'da verilerin imhası kavramı ise yok etme şeklinde geçmektedir.

[578] Saka, "İmha," 55-56.

Kişisel verilerin korunmasına ilişkin esasların yer aldığı KVKK'da imhaya ilişkin ise silme, yok etme ve anonim hale getirme hallerinden bahsedilmiş olup; imhaya ilişkin usule yer verilen Kişisel Verileri Silme Yönetmeliği'nde de aynı şekilde imhanın silme, yok etme ve anonimleştirme şeklinde yapılabileceği görülmektedir.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in[579] (Kişisel Verileri Silme Yönetmeliği) 4/1-(c) maddesinde imhanın kişisel verilerin silinmesi, anonimleştirilmesi ya da yok edilmesi anlamına geldiği belirtilmiştir.

Veri sorumluları KVKK'nın 5. veya 6. maddesinde belirtilen hukuka uygunluk nedenlerinin varlığı halinde kişisel verileri işleyebilmektedir. Söz konusu hukuka uygunluk hallerinin ortadan kalkması veya ilgili kişiden açık rızası alınmadan önce verisini işlemeye yönelik olarak yapılan bilgilendirme metninde belirtilen veri işleme süresinin dolması halinde ise veri sorumlusu, ilgili verileri işlemeye devam edemeyecektir. Saklama faaliyeti de kişisel veriyi işleme anlamına geldiğinden; veri sorumlusunun ilgili veriyi değiştirmeden veya kullanmadan yalnızca saklamaya devam etmesi hali de veri işleme faaliyeti olarak kabul edilmektedir. Bu sebeple hukuka uygunluk nedenlerinin ortadan kalkması veya işleme süresinin sona ermesi halinde veri sorumlusunun bu kişisel verileri imha etmesi gerekmektedir.

Veri sorumlusuna getirilen imha yükümlülüğü ile ilgili kişinin belirlenebilir olmasının önüne geçilmeye çalışılmaktadır.[580] Nitekim Kişisel Verileri Silme Yönetmeliği'nin 7/1 maddesinde de bu konuya değinilerek; veriyi işleme şartlarının ortadan kalkması halinde verisi işlenenin talebi doğrultusunda ya da veri sorumlusunun resen söz konusu verileri imha etmesi gerektiğine yer verilmiştir.

Kişisel Verileri Silme Yönetmeliği'nin 7/2 maddesinde belirtildiği üzere; kişisel verilerin imhası, silerek, anonimleştirerek ya da yok ederek nasıl yapılırsa yapılsın; veriyi işlerken dikkat edilen KVKK'nın 4. maddesinde yer verilen ölçülü, hukuka ve dürüstlük kuralına uygun olma gibi ilkelere riayet edilerek; imhanın gerçekleştirilmesi gerekmektedir. Bununla birlikte, KVKK'nın 12. maddesinde yer verilen veri güvenliğine ilişkin hususlara imha sürecinde de dikkat edilmesi gerekmektedir. İmha sürecinde, KVK

[579] R.G. 28.10.2017, S.30224.
[580] Dülger, KVK Hukuku, 598.

Kurulu tarafından verilen kararlar da dikkate alınarak; işletmenin imhaya ilişkin prosedürü çerçevesinde imha faaliyetinin gerçekleştirilmesi gerekmektedir.

Kişisel Verileri Silme Yönetmeliği'nin 7/3 maddesinde, veri sorumlusu tarafından gerçekleştirilen imha faaliyeti esnasında yapılan işlemler kayıt alınarak veri sorumlusunun uymakla yükümlü olduğu başka bir mevzuat hükmü bulunmadığı hallerde en az üç yıl boyunca saklanması gerektiği belirtilmiştir.

İmha yöntemlerinden hangisinin seçileceğine ise Kişisel Verileri Silme Yönetmeliği'nin 7/5 maddesinde yer verilmiş olup; silme, yok etme ya da anonimleştirmeden hangi yolla verinin imha edileceğine veri sorumlusunun karar vereceği belirtilmiştir. İmha işlemi resen olduğunda veri sorumlusu uygun yöntemi belirleyebilirken; veri sahibinin talebiyle imha gerçekleştirilmesi halinde ise yine veri sorumlusu tarafından uygun yöntem belirlenmekte olup; bu sefer veri sahibine seçilen yöntemin açıklaması yapılmaktadır.

İmha edilmesi gereken kişisel verilerin vaktinde veya hiç imha edilmemesi halinde veri sorumlusuna karşı uygulanacak yaptırım, KVKK'nın 17/2 hükmü gereğince, TCK'nın 138. maddesi uygulanacak olup; ilgili hüküm uyarınca, veri sorumlusuna bir yıldan iki yıla kadar hapis cezası verilebilecektir. CMK hükümleri uyarınca yok edilmesi veya ortadan kaldırılması gereken bir suçun varlığı halinde ise cezanın bir kat artırılacağı düzenlenmiştir. Söz konusu hükümde yalnızca yok etmeme haline karşılık ceza öngörülmüş olup; silme ya da anonimleştirmeme hallerine yönelik olarak herhangi bir hüküm bulunmadığı görülmektedir. Ancak TCK'nın KVKK'dan yaklaşık on iki yıl önce yayımlandığı düşünüldüğünde; henüz kişisel veri ve bu verilerin korunması kavramı ülkemizde yerleşmediğinden; imhanın yalnızca yok etme şeklinde gerçekleşebileceğine ilişkin düşünce ve ilgili cezai hükmün fazla uygulama alanı bulamamış olması nedeniyle hükmün lafzının yok etme şeklinde oluşturulduğu düşünülmektedir.[581]

Kişisel verilerin imhasına yönelik olarak hukukumuzda kavram birliği olmadığı açıktır. Kişisel Verileri Silme Yönetmeliği'nin 13. maddesinde belirtildiği üzere, uygulamada bu farklılığın neden olacağı durumlarda KVK Kurulu'nun verdiği kararların yol gösterici olduğu anlaşılmaktadır.

İmha edilmesi gereken verilerin süresinde veya hiç imha edilmemesi halinin veri sorumlusu açısından cezai sorumluluğunun yanı sıra özellikle elektronik haberleşme

[581] Saka, "İmha," 45.

sektöründeki işletmecilerin işlemiş oldukları verilerin diğer sektörlere nazaran daha fazla olduğundan işletmelerin bu çok sayıdaki verilerin saklanmasına ilişkin işletmesel problemleri bulunmaktadır. Elektronik haberleşme hizmeti kullanıldıkça veri yığınlarının giderek artması sebebiyle, işletmeci açısından imha zamanı gelmiş olan verilerin imhalarının gerçekleştirilmesi, işletmecinin veri saklama maliyeti ve sorumluluğundan kurtulması anlamına gelmektedir.

3.3.1. İmha Politikası

Kişisel Verileri Silme Yönetmeliği'nin 5. maddesinde, KVKK'nın 16. madde hükmü kapsamında VERBİS'e kayıt zorunluluğu olan veri sorumlularının işlemekte olduğu kişisel verileri nasıl sakladığına ve ne şekilde imha edeceğine dair veri sorumluları, saklama ve imha politikası oluşturmakla yükümlü kılınmıştır.

Kişisel verileri saklama ve imha politikası, KVK Kurumu'nun hazırladığı Veri Güvenliği Rehberi'nde idari tedbirler arasında sayılmaktadır.[582]

Kişisel Verileri Silme Yönetmeliği'nin 7/4 maddesinde veri sorumlusunun imhaya ilişkin uyguladığı yöntemleri açıkladığı bir imha politikası olması gerektiği yer almaktadır. Aynı Yönetmeliğin 6. maddesinde imha politikası içerisinde; en azından politikanın amacının ne olduğuna ve verilerin kaydedildiği kayıt ortamlarının hangileri olduğuna, işletmeci tarafından alınan teknik ve idari tedbirler hakkında bilgilendirmeye yer verilmesi gerektiği bildirilmiştir. Bununla birlikte, politikada bahsedilen terimlerin ne anlama geldiğine ilişkin tanımlar bölümüne, verilerin saklanması veya imha edilmek istenmesinin hukuki ve teknik gerekçeleri de ilgili bilgilendirmede yer almalıdır. Bilgilendirmede bulunması gereken diğer hususlar ise imhaya yönelik olarak alınan tedbirlerin neler olduğu, imha sürecinde yer alan personele ve görevlerine ilişkin bilgilendirme, verilerin saklanmasına ve imhasına yönelik olarak belirlenen süreler, periyodik olarak hangi dönemlerde imhanın gerçekleştirildiğine ilişkin bilgilendirme ve politikada güncelleme yapıldığında buna ilişkin bilgilerdir.

3.3.2. İmha Süreleri

Kişisel verilerin resen imha edilmesi gerektiği hallerde veri sorumlusu, Kişisel Verileri Silme Yönetmeliği'nin 11. maddesinde yer alan sürelere uygun olarak imha işlemlerini yürütür. İlgili madde hükmü gereğince, imha sürelerini neler olduğuna ilişkin

[582] KVK Kurumu, Veri Güvenliği Rehberi, 12.

bakılması gereken ilk kaynağın veri sorumlusunun imha politikası olduğu anlaşılmakta olup; veri sorumlusu, imha politikasında yer verdiği sürelere uygun olarak işleme faaliyetine ilişkin hukuka uygunluk nedeni sona eren kişisel verileri imha eder. Her ne kadar politikada belirlenen süreye uygun imha yapılması uygun sayılsa da ilgili Yönetmeliğin 11/2 maddesinde bu sürenin en fazla altı ay olması gerektiğine yer verilmiştir. İmha politikası olmayan veri sorumlularının ise veriyi hukuka uygun şekilde işleyebilmesine ilişkin hallerin ortadan kalktığı tarihi takip eden üç ay içerisinde gerekli silme, anonimleştirme veya yok etme faaliyetlerinin yerine getirilmesi gerektiğine yer verilmiştir. Söz konusu 11. maddenin 4. fıkrasında ise verinin hukuka aykırı şekilde işlendiğinin tespiti ve telafi edilmesi zor hallerin ortaya çıkma ihtimalinin bulunması ya da zararların doğması durumunda KVK Kurulu'nun imhaya ilişkin süreleri kısaltabileceğine yer verilmiştir.

KVKK'nın 11. ve 13. maddelerinde belirtilen ilgili kişinin verilerinin silinmesi veya yok edilmesi talebiyle veri sorumlusuna başvurması halinde uygulanacak usule Kişisel Verileri Silme Yönetmeliği'nin 12. maddesinde yer verilmiştir. İlgili kişinin böyle bir talebine karşılık, veri işlemesine ilişkin herhangi bir yükümlülüğü veya hukuka uygun sebebi kalmadıysa, veri sorumlusu tarafından ilgili verilerin imha edilmesi sağlanır. Söz konusu imha süreci, talebin gelmesinin ardından otuz gün içerisinde tamamlandıktan sonra veri sahibine bilgi verilir. İmhası istenen veriler üçüncü kişilere aktarılmışsa; veri sorumlusu tarafından bu kişilere de bilgi verilerek onların da bilgiyi imha etmesi sağlanır. İlgili kişiden imhaya ilişkin talep gelmesine rağmen; veri sorumlusunun veriyi işlemesine yönelik sebepleri hala mevcutsa; veri sorumlusu, KVKK'nın 13/3 maddesinde belirtildiği üzere yazılı olarak veya elektronik ortam üzerinden gerekçesini bildirerek talebi reddettiğine ilişkin cevabını yine otuz gün içerisinde veri sahibine iletmelidir.

İşlenen verilerin saklama sürelerine ilişkin mevzuatta ayrıntılı bir hüküm yer almaması halinde, öncelikle verinin KVKK'nın 28. madde kapsamında sayılan istisnai hallerden biri olup olmadığının kontrol edilmesi gerekmektedir. Bu tespitin ardından veri sorumlusunun veriyi işlemeye ilişkin hukuka uygunluk nedenlerinin ya da yasal yükümlülüğünün sona erip ermediğine bakıldıktan ve ilgili kişinin vermiş olduğu rızanın geçerliliği kontrol edildikten sonra, verinin meşru işlenme amacının ortadan kalktığına karar verilirse; veri sorumlusu tarafından verilerin imha edilmesi gerektiğine karar

verilmelidir. Bu durumda Kişisel Verileri Silme Yönetmeliği'nin 11. ve 12. maddelerinde yer alan sürelere göre verilerin imhası gerçekleştirilmektedir.[583]

3.3.3. Silme

Silme faaliyetinin ne anlama geldiği, Kişisel Verileri Silme Yönetmeliği'nin 8. maddesinde belirtilmiş olup; kişisel verilerin ilgili kullanıcılar tarafından yeniden ulaşılamayacak ve kullanılmayacak hale getirilmesi işlemi silme olarak tanımlanmıştır. Veri sorumlusu, bu doğrultuda gereken tedbirleri almakla yükümlü kılınmıştır.

İlgili kişi ve ilgili kullanıcı kavramları birbirinden farklı kavramlar olup; ilgili kişi, verileri işlenen gerçek kişi iken, ilgili Yönetmeliğin 4/1-(b) maddesinde düzenlenen ilgili kullanıcı ise kişisel verileri teknik anlamda saklayan, yedekleyen ya da koruyan kişiler dışında, genel anlamda veri sorumlusunun verdiği yetki ve talimat ile kişisel verileri işleyen kişidir. Bu doğrultuda şirket çalışanları ya da doğrudan şirket çalışanı olmasa da şirket adına örneğin; muhasebe ya da marka veya patent tescili alanında danışmanlık hizmeti veren şirketler ilgili kullanıcı olarak değerlendirilmektedir.

Kişisel Verileri Silme Yönetmeliği'nde silme işleminin açıklaması incelendiğinde; verilerin ilgili kullanıcılar tarafından erişilememesinden bahsedildiği, verinin varlığının tamamen ortadan kaldırılması anlamına gelmediği anlaşılmaktadır. Bu doğrultuda, ilgili silme işleminin ardından; veri sorumlusunun meşru bir menfaatinin doğması ya da yasal bir yükümlülüğünü yerine getirme amacının ortaya çıkması halinde ilgili silinen veriler veri sorumlusu tarafından yeniden işlenebilecektir.[584]

Silme işlemi, ilgili kullanıcının veriye erişiminin engellenmesi anlamına geldiğinden; verilerin ilgili kullanıcı tarafından erişilemediği her durum silme olarak adlandırılabilmektedir. Kağıt ortamında saklanan veriden söz ediliyorsa, imha edilecek evrakın ilgili kullanıcının erişemeyeceği şekilde kilitli olarak muhafaza edilerek; elektronik ortamda saklanan veri ise kişinin veriye erişebilmesine yönelik yetkisinin kaldırılarak, taşınabilir disklerde muhafaza edilen veriler, diskin şifresi değiştirilerek ve veri tabanında kayıtlı bulunan verilerin ise veri tabanı komutları vasıtasıyla silinebilmektedir.

---

[583] Ramazan Çağlayan, "İdare Hukuku Açısından Kişisel Verilerin İmhası ve Denetim," iç. *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası*, Rıza Saka, Ramazan Çağlayan, Mahmut Koca, (Ankara: Seçkin Yayıncılık, 2020): 259.
[584] Saka, *İmha*, 48.

Bulut ortamında saklanan verilere ilişkin, kişisel güvenlik duvarları, parola yöneticileri, anahtar kelime uyarıları gibi pek çok ürün geliştirilerek kullanıcıların çevrimiçi gizliliklerinin ilave güvenlik önlemleri sağlanarak korunması amaçlanmaktadır.[585] Bahsi geçen şekilde güvenlik önlemleri alınarak korunan verilerin saklandığı uygulama vasıtasıyla ve uygulamanın sunucusundan da silinecek şekilde erişimin kaldırılması veya ilgili kullanıcının erişiminin kısıtlanması yoluyla silinme işlemi gerçekleştirilebilir.[586]

3.3.4. Yok Etme

Kişisel verilerin yok edilmesi, Kişisel Verileri Silme Yönetmeliği'nin 9. maddesinde belirtildiği üzere, verilerin kimsenin ulaşamayacağı ve kullanamayacağı hale getirilmesi olarak tanımlanmaktadır. Silme faaliyetinde yalnızca ilgili kullanıcıların erişmesi engellenmek istenirken; yok etme işleminde verilere kimse erişememektedir. İlgili hüküm incelendiğinde, yok edilmenin silme işleminden farkının yok edilen verinin artık ilgili kullanıcı dışındaki kişiler de dahil olmak üzere kimse tarafından bir daha ulaşılamamasıdır.

Bilgi Güvenliği Yönetmeliği'nin 20/2 maddesinde, kullanılmayan ya da yeniden kullanabilmek için temizlenmesi gereken taşınabilir bellek, sabit disk gibi ekipmanların geri dönüştürülemez şekilde silinmesi ve silinemediği takdirde ise mümkün mertebe cihazın parçalarının kullanılamaz hale getirilmesi gerektiğine yer verilmiştir. İlgili hükümde cihazların ve bilgilerin geri erişilemeyecek şekilde imhasıyla yok etme faaliyeti kastedilmektedir.

Yok edilen kişisel veriye hiçbir türlü ulaşılması mümkün değildir. Kağıt ortamında saklanan bir verinin kağıdın yakılması gibi yok etme işlemlerinden sonra eski haline döndürülmesi mümkün değildir. Sabit disk gibi manyetik veri depolamaya olanak sağlayan cihazların yok edilmesi ise yakarak, eriterek mümkünken; çok küçük parçalara ayırarak yok etme işlemi sonrasında dahi bazı verilere ulaşılabilmektedir. CD ortamında kaydedilen veriler ise yine yakılarak veya üzerine yazma yöntemiyle yok edilebilmektedir. Bulut ortamında saklanan veriler silinebilirken; yok edilmesi pek

[585] Joris Claessens, Claudia Diaz, Caroline Goemans, Bart Preneel, Joos Vandewalle, Jos Dumortier, "Revocable Anonymous Access to the Internet," Computer Security and Industrial Cryptography (COSIC), Interdisciplinary Centre for Law and Information Technology (ICRI), (2002): 2, https://www.esat.kuleuven.be/cosic/publications/article-92.pdf , Erişim Tarihi: 30 Ekim 2022.
[586] Saka, "İmha," 49-51.

mümkün değildir. Bunun yerine veri sorumlusunun bulut ortamını kullandığı veri işleyen ile gizlilik sözleşmesi yapması ve verilerini şifreli olarak saklaması çözüm olarak gösterilebilir.[587]

3.3.5. Anonimleştirme

KVKK'nın 3/1-(b) maddesine göre anonimleştirme, verilerin hiçbir şekilde ilgili kişiyle bağlantı kurulamayacak hale getirilmesi olarak tanımlanmış olup; aynı tanıma Kişisel Verileri Silme Yönetmeliği'nin 10/1 maddesinde de yer verilmiştir. Aynı Yönetmelik hükmünün 2. fıkrasında, anonimleştirilen verilerin, teknik birtakım yollar vasıtasıyla dahi yeniden ulaşılamayacak hale veya başka verilerle eşleştirilse dahi ilgili kişinin tahmin edilemeyeceği hale getirilmesi gerektiğine yer verilmiştir.

Verilerin anonim olması, içeriğin herhangi tanımlanabilir bir bilgi içermemesi anlamına gelmektedir. Günümüzde özellikle haberleşme ağlarında ve internette, kullanıcıların mahremiyetlerinin sağlanması konusunda endişe duyulmaktadır. Bu ortamlarda işlenen verilerin anonimlik düzeyini artırmak teknik olarak kolay olsa da verilerin tam olarak anonim hale getirilmesi garanti edilememektedir.[588]

Veri sorumluları tarafından elde edilen kişisel verilerin kullanım ve işlenme amaçları sona erdikten sonra da istatistik oluşturma, planlama yapma gibi çeşitli amaçlarla verinin kime ait olduğu bilinmeden işlenmeye ihtiyaç duyulabilmektedir. Bunun gibi durumlarda, verinin işlenmesine ilişkin hukuka uygunluk nedeni ortadan kalksa dahi verinin anonimleştirilerek kullanılabilmesi tercih edilebilmektedir.[589] Verisi işlenen ilgili kişi ile veri arasındaki bağın ortadan kalkmasıyla birlikte, veriye bakıldığında ilgili kişi bilinir veya bilinebilir olmadığından; işleme faaliyeti de kişisel verinin işlenmesi anlamını terk etmektedir.

En bilindik anonimleştirme yöntemi, verinin içerisindeki harf veya sayıların yerine yıldız konularak yapılan maskeleme yöntemidir. Toplu şekilde sınıflandırılarak verinin yalnızca bir özelliğine göre sınıflandırma yapılması hali de anonimleştirme yollarından biridir.[590]

---

[587] Saka, "İmha," 52-54.
[588] Claessens, "Revocable Anonymous Access," 2, 18.
[589] Saka, "İmha," 55.
[590] Saka, "İmha," 56.

Herhangi bir telekomünikasyon ağında yapılmak istenen anonimleştirme faaliyetinde ise kullanıcıların haberleşme sırasında bir ağ adresine sahip olması gerektiğinden ve internet için bu ağ adresi IP adresi olarak tanımlandığından; internette iyi bir gizlilik düzeyi elde etmek için, bütün IP trafiği anonimleştirilmelidir.[591]

4. VERİ TAŞINABİLİRLİĞİ HAKKI

Veri taşınabilirliği hakkı, 95/46 sayılı Direktif'te yer almamakta olup; ilk kez GDPR'nin 20. maddesinde; ilgili kişinin verilerini bir veri sorumlusundan diğerine taşıyabileceği şeklinde tanımlanmıştır.[592] Diğer bir deyişle veri taşınabilirliği, bir kullanıcının verilerinin halihazırda hizmet aldığı bir platformdan alınarak başka birine aktarılmasına olanak tanınmasıdır.[593] Veri taşınabilirliği genellikle bulut bilişim, akıllı cihaz uygulamaları, web hizmetleri ve diğer otomatik veri işleme faaliyetleri için geçerlidir.[594]

GDPR'nin 20. madde hükmü çerçevesinde veri sahibi, veri sorumlusunda bulunan kişisel verilerini makine tarafından okunabilir bir formatta edinebilme hakkına sahip olmasının yanı sıra bu verileri herhangi bir yükümlülüğe tabi olmadan başka bir veri sorumlusuna iletme hakkına sahiptir. Veri taşınabilirliği hakkı ile veri sahibinin kendi verileri üzerinde daha fazla söz sahibi olması ve konumunun güçlenmesi hedeflenmiştir.[595]

Veri taşınabilirliği ile veri sahibinin taleplerine uygun şekilde kişisel verileri alma ve bunların işlenmesi garanti edildiğinden, GDPR 20. maddede belirtildiği üzere, veri taşınabilirliği taleplerini yanıtlayarak verileri ileten veri sorumluları, kişisel verileri alan kişi ya da başka bir şirket tarafından gerçekleştirilen işlemlerden sorumlu değildir. Bu doğrultuda, verileri başka bir alıcıya gönderenin veri sorumlusu olmadığı durumlarda, veri sorumlusu gereken önlemleri alması halinde başka bir sorumluluk ile karşı karşıya kalmayacaktır. Veri sorumlusu önlemler almak adına örneğin; iletilen kişisel veri

[591] Claessens, "Revocable Anonymous Access," 3.
[592] Akıncı, GVKT, 20.
[593] Sasha Hondagneu-Messner, "Data Portability: A Guide and a Roadmap," *Rutgers Computer Technology Law Journal* 47, no.2 (2021): 242-243.
[594] Hondagneu-Messner, "Data Portability," 249.
[595] Article 29 Çalışma Grubu, Guidelines on the Right to Data Portability, 3, https://ec.europa.eu/newsroom/article29/items/611233 , Erişim Tarihi: 28 Ekim 2022.

türlerinin gerçekten de ilgili kişinin iletmek istediği veri türlerinden olmasını sağlayan prosedürler oluşturarak; veri aktarımından öncesinde veri sahibinden onay alarak işlemlerini gerçekleştirmelidir.[596]

Veri taşınabilirliği hakkı, veri sahiplerinin kişisel verilerini kendilerinin yönetmesi ve yeniden kullanabilmesi için yol gösterici niteliktedir. Böylelikle, kişisel verilerin bu hak doğrultusunda kullanıcılar tarafından kontrollü ve güvenli olarak paylaşılması taleplerinin artmasıyla; işletmeciler tarafından hizmetlerin sunumu ve müşteri deneyimleri de zenginleşme eğilimi göstermektedir.[597]

Öte yandan, söz konusu veri taşınabilirliği hakkı sayesinde ilgili kişilere verileri üzerinde büyük bir egemenlik alanı tanındığı düşüncesine karşılık; bu hakkın kullanımına dikkat edilmediği takdirde, kişisel verilerin birden fazla veri sorumlusuyla paylaşılması mümkün hale gelmektedir.[598] Bu durum, verilerin güvenliği hakkında endişelerin artmasına neden olmaktadır.

Bireyler verilerine ilişkin bir onay vermesi ya da bir sözleşmenin imzalanmasından kaynaklı kullanılan verilerinin taşınabilirlik çerçevesinde iadesini ya da başka bir şirketle paylaşılmasını talep edebilmektedir.[599] Rekabet ve veri koruma uzmanları, karmaşık sorunlar olmasına rağmen; veri taşınabilirliğinin bireylerin verilerini kontrol etmesine yardımcı olduğu ve çevrimiçi hizmet sağlayıcılar arasında seçim yapmalarını kolaylaştırabileceği konusunda görüş birliği içerisindedir.[600] Veri taşınabilirliği hakkından kaynaklı kişisel verilerin taşınabilir olması AB'de kişisel verilerin serbest akışını destekleyerek rekabetin de artmasına yardımcı olmaktadır. Bunun yanında, veri sahibinin hizmet sağlayıcılar arasında geçiş yapabilmesi kolaylaşarak, rekabet kaynaklı hizmet sağlayıcıların yeni hizmetler geliştirmeleri de söz konusu olmaktadır.[601]

Örneğin, Facebook'un yıllar içerisinde kullanıcılarından edindiği veriler Facebook'a alternatif olabilecek bir rakibinin her şeye yeniden başlayarak zamanla bu

[596] Article 29 Çalışma Grubu Data Portability, 6.
[597] Article 29 Çalışma Grubu, Data Portability, 5.
[598] Akıncı, GVKT, 20.
[599] It's Your Data-Take Control, https://ec.europa.eu/info/sites/default/files/data-protection-overview-citizens_en_0.pdf . Erişim Tarihi: 28 Ekim 2022.
[600] Erin Egan, Charting a Way Forward Data Portability and Privacy, Facebook, 2019. https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf , 3, Erişim Tarihi: 28 Ekim 2022.
[601] Article 29 Çalışma Grubu, Data Portability, 3.

verileri elde etmesini gerektirecektir. Esasen Facebook'a alternatif olacak bir platform iki önemli sorun ile karşı karşıya kalacaktır. Bunlardan birincisi, uzun yıllar içerisinde elde edilen kişisel verilere dayalı olarak Facebook ile karşılaştırılabilir bir gelirin nasıl edileceği, ikincisi ise halihazırda Facebook kullanan çok sayıda kişinin Facebook aracılığıyla arkadaşlarıyla kurdukları bağlantıları kurmalarına nasıl izin verileceğidir. Rekabete aykırılık oluşturan bu iki temel sorunun, veri taşınabilirliği ile çözülebileceği düşünülmektedir. Bu süreç, doğru bir şekilde yönetilir ve düzenlenirse, veri taşınabilirliği sayesinde daha rekabetçi bir ortam sağlanabilir.[602]

Veri taşınabilirliği ile ilgili, bu aktarımı yapanların verileri fazla veya eksik dahil edeceğine ilişkin pratik kaygıların yanı sıra verilere yetkisiz erişimle ilgili güvenlik sorunlarına ilişkin risklerin olduğu düşünülmektedir.[603] Bununla birlikte, GDPR ile veri taşınabilirliği hakkının ilgili kişilere sağlanması ve dolayısıyla üye devletlerin ulusal gizlilik kanunlarında veri taşınabilirliği hakkına yer verilmesinin rekabeti destekleyici yanının aksine kişisel verilerin kolayca elde edilebilir hale getirilmesi ve platformlar arası hızlı bir şekilde aktarılmasıyla ortaya çıkabilecek güvenlik sorunları da göz ardı edilmemelidir.

Veri taşınabilirliğine yalnızca elektronik haberleşme sektörüne özgü olarak gösterilebilecek örnek ise numara taşınabilirliğidir.[604] Örneğin, telefon numarasını bir operatörden diğerine taşıyan kişi, halihazırda kullanmakta olduğu telefon numarası değişmeden numarasını taşıdığı operatörün hizmetlerin faydalanabilir hale gelmektedir. Böylece telefon numarası değişmesi gibi bir zorlukla karşılaşılmamış olmaktadır.

5. KİŞİSEL VERİLERİN YENİDEN DEĞERLENDİRMEYE TABİ TUTULMASI

Büyük miktarda verinin çok daha hızlı, ucuz ve ölçeklenebilir şekilde işlenmesini sağlayan bulut bilişimin yaygın ve düşük maliyetli kullanılabilirliği, makine öğreniminin artık geniş veri kümelerinden ve etkin bir şekilde sınırsız kaynaktan yararlanabileceği anlamına gelmektedir. Amazon, IBM, Google ve Microsoft gibi büyük bulut bilişim

[602] Hondagneu-Messner, "Data Portability," 242-243.
[603] Hondagneu-Messner, "Data Portability," 244.
[604] Hondagneu-Messner, "Data Portability," 246.

oyuncuları artık tahmine dayalı analitik verilere önemli ölçüde odaklanarak; bulut destekli makine öğrenimi hizmetleri ve araçları sağlamaktadır.[605]

Çevrimiçi faaliyetlerle ve nesnelerin interneti kullanılarak verinin yoğun olduğu ortamlarda, insan katılımının azalması ve makine kullanımının artış göstermesiyle birlikte profil oluşturma yaygınlaşarak makine öğrenimi ile değerli bilgiler keşfedilmesi sonucunda; bu bilgilere dayalı tahminler yapılmasıyla mevcut verilerin veri madenciliği yapılarak kullanılması mümkün hale gelmektedir.[606]

5.1. ABONENİN KİŞİSEL VERİLERİNDEN PROFİL OLUŞTURMA

GDPR'ın 4/2 maddesinde, kişisel verilerin işlenmesi faaliyetinin otomatik araçlarla olsun ya da olmasın toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama ya da değiştirme, alma, danışma gibi faaliyetlerin tümü işleme kapsamında değerlendirilmektedir. GDPR'ın 4/4 maddesinde profil oluşturma faaliyeti; kişisel verilerin, kişilerin ilgi alanları, sağlık, ekonomik, konum gibi hususların tespit veya analiz edilmesi için kullanılması olarak tanımlanmıştır. İlgili hükümlerden hareketle, profil oluşturma faaliyetinin de veri işleme faaliyeti olarak adlandırılacağı açıktır.

Profil oluşturma süreci temelde; veri toplama, makine öğrenimi algoritmalarının kullanımı yoluyla model geliştirme ve karar verme olmak üzere üç başlıkta incelenebilir. İlk olarak kişisel verilerin, veri koruma ilkelerine uygun olarak toplanması gerekmektedir. GDPR'ın "itiraz hakkı" başlıklı 21/1 maddesi kapsamında veri sahibi, kendi özel durumuna ilişkin gerekçelerle, herhangi bir zamanda, GDPR'ın 6/1 maddesinin (e) veya (f) bentlerine dayalı olarak kendisiyle ilgili kişisel verilerin işlenmesine itiraz etme hakkına sahip olup, söz konusu hüküm çerçevesinde profil oluşturmak da bu kapsamda değerlendirilmektedir. GDPR'ın 21/2 maddesinde, pazarlama amacıyla kişisel verilerin kullanılması halinde, profil işleme faaliyeti de dahil olmak üzere kişinin her zaman itiraz etme hakkının olduğu belirtilmiştir. GDPR'ın 21/3 maddesi kapsamında da veri sahibi doğrudan pazarlama amacıyla verilerinin işlenmesine itiraz etmesi durumunda, kişisel verileri artık bu amaçlar için işlenememektedir. İkinci olarak, bir makine öğrenimi algoritması ile farklı yollardan elde edilen verilerden bir

[605] Dimitra Kamarinou, Christopher Millard, Jatinder Singh, "Machine Learning with Personal Data," ssrn.com, Queen Mary School of Law Legal Studies Research Paper No. 247/2016, 2016, 4, https://ssrn.com/abstract=2865811, Erişim Tarihi: 4 Kasım 2022.
[606] Kamarinou, "Machine Learning," 6.

profil geliştirebilir. Bu işlem yapılırken, hesaplama gücü ya da depolama açısından bulut ortamından yararlanılabilir. Profil oluşturma sürecinin son aşaması, belirlenen profillere dayalı olarak veri sahipleri hakkında tespitler ve sonuçlar çıkarmaktır.[607]

Kişisel verilerin profil oluşturulması yolu ile sınıflandırılarak bireyler hakkında çıkarımlarda bulunulması, hizmetin veya ürünün satışının hedeflendiği topluluğa ulaşılabilmesinin daha hızlı ve az maliyetli olmasını sağlaması sebebiyle çoğu sektörde aktif olarak kullanılan bir yöntemdir.

5.2. BÜYÜK VERİ UYGULAMALARI

Büyük veri, büyük ölçekli bilginin toplanması, depolanması ve analiz edilebilmesine uygun nitelikteki bilgi anlamına gelmektedir.[608] Büyük veri genellikle, geleneksel istatistiksel yöntemlerin yanı sıra daha yenilikçi analitik araçlar kullanarak verilerin toplanmasına ve matematiksel olarak analiz edilmesine yardımcı olan yeni bir teknoloji olarak tanımlanmaktadır. Geçmişte, verilerin toplanması ve analiz edilmesi verilerin kullanılmasını zor, zaman alıcı ve maliyetli hale getirmekteydi. Bu durum, gerekli olduğu kadar verinin kullanılmasını öne çıkarmıştı. Dijitalleşmenin getirdiği teknolojik değişikliklerin verileri toplamak ve analiz etmek için gereken süreyi ve maliyeti önemli ölçüde azalttı.[609]

İşletmeciler, büyük verileri kullanarak belirsiz bağlantıları, davranışları, eğilimleri, kimlikleri ve pratik bilgileri öğrenebilmek adına karmaşık algoritmalar ve yapay zeka teknolojileri uygulayabilmektedir. Esasen, büyük verileri oluşturan bilgiler, tüketicilerin işlemlerinden, nesnelerin interneti ile dijital uygulamalardan elde edilebilmektedir. Kredi kartı ile yapılan bir alışveriş, hastanede görülen tedavi süreci, çevrimiçi ortamda yapılan iş başvurusu ya da en basit olarak Google'da bir konunun araştırılması gibi örnekler büyük verilerin oluşturulması ve kullanılmasına temel teşkil etmektedir. Büyük veri ile bireyler hakkında detaylı bilgiler toplanırken, kişisel bilgilere erişimi sınırlandırmak için yeni yöntemler keşfedilerek; kişisel verilere ilişkin bireylerin sorumluluğunun daha az olduğu bir hayatın sürdürülebilmesi sağlanabilir. Örneğin tıp alanında, büyük verinin mümkün kıldığı hastanın kendi kendini izlemesine yardımcı olan

[607] Kamarinou, "Machine Learning," 8-10.
[608] Anita L. Allen, "Law, Privacy & Technology Commentary Series Protecting One's Own Privacy In A Big Data Economy," *Harvard Law Review Forum*, no.130 (2016): 71.
[609] Mayer-Schönberger, "Big Data," 318.

yenilikçi yöntemler, önleyici tıbbın iyileştirilmesini sağlayarak, hastanelerin iş yüklerinin azalmasına yardımcı olmaktadır.[610]

Bahsi geçen olumlu etkilerine karşılık, büyük veri uygulamaları vasıtasıyla birtakım veriler bir araya gelerek başka bilgilere ulaşılabilmesini sağladığından, kişisel verilerin korunmasına ilişkin sorun teşkil etmesinin yanı sıra kullanıcıların profilleme işlemine maruz kalmalarına da neden olmaktadır.[611] Değerli bilgilerin ayırt edilebilmesi maksadıyla büyük miktarda analiz edilebilir veri toplama çabası olarak ifade edilebilen büyük veri,[612] kişisel verilerin işlenmesi ve mahremiyetin sağlanması bakımından bazı soru işaretlerini oluşturmaktadır. Kimlikle ilgili bilgiler, istihdam, barınma ya da finansal hizmetler gibi konularda elde edilen bilgiler, bireylerin dijital olarak gözetilmesi ve takibine neden olduğundan mahremiyetin kolaylıkla ihlal edilebileceği gerçekliğinin de göz ardı edilmemesi gerekmektedir. Bütün bu durumlardan korunabilmek adına, kullanılan cihazlara bir başkasının erişimini sınırlayabilmek, parolaların ve güvenlik yazılımlarının özenle kullanılmasının yanı sıra sosyal medya ve kredi kartlarının kullanımında da gereken özenin gösterilmesi ve söz konusu durumlarda ihtiyatlı davranmak önem taşımaktadır. [613]

Teknolojik gelişmeler, mahremiyet ve güvenliği tehlikeye atabilir fakat yeniliklerin gerçekleştirilmesindeki önemi sayesinde uzun vadede mahremiyetin korunmasına daha fazla katkısının olacağını gerçeği de yadsınamaz.[614]

Bulut bilişim ve sanallaştırma hizmetlerinin kullanıcılar, işletmeler ve resmi kuruluşlar nezdinde popülaritesi her geçen gün artış göstermekle birlikte, veri koruma, veri güvenliği, süreklilik, sorumluluk, kayıt tutma gibi konularda endişeler de söz konusudur. Bulut hizmetlerini kullanmayı düşünen herhangi bir kişinin ya da kuruluşun avantajları, dezavantajları ve sözleşme güvencelerini dikkatlice değerlendirmesi gerekir. Bunların yanı sıra hizmet veren operatörlerin de veri koruma uyumluluğunu nasıl sağladıklarına dair kendilerini güvence altına almaları önemlidir.[615]

---

[610] Allen, "Big Data Economy," 71, 74.
[611] Çekin, *KVK Hukuku*, 195.
[612] Mayer-Schönberger, "Big Data," 318.
[613] Allen, "Big Data Economy," 71-72.
[614] Allen, "Big Data Economy," 75.
[615] Paul Lambert, *Understanding the New European Data Protection Rules*, Chapter 4, Need For Updating Data Protection, 9.

5.3. VERİ MADENCİLİĞİ

Verilerin değeri, yalnızca çok sayıda veriye sahip olunarak ve bu verilerin analiz edilmesiyle değil, aynı zamanda verilerin başka veri kaynaklarıyla birleştirilmesiyle birlikte artış göstermektedir. Veriler, tek başına olduğunda değeri az olan tek bir yapboz parçası gibidir. Ancak diğer verilerle birleştirildiğinde bir görüntüyü tamamlamak adına değerli bir bütün haline gelmektedir.[616] Veri madenciliği, birden fazla farklı faaliyet sonucunda elde edilen bilgi yığınlarının sınıflandırılarak veya bir düzene bağlı şekilde saklanarak anlamlı bir bilgi topluluğu haline getirme işlemi olarak tanımlanmaktadır.[617]

Veri madenciliği, kamusal alanda ve özel sektörde yaygın olarak kullanılan veri tabanlarında bulunan kişisel veriler ile ilgili bir kavramdır. Kamusal alanda veri madenciliğinde, geniş bilgi depolarından istihbarat elde etmek için kullanılan bir dizi teknik uygulanmaktadır. Konu tabanlı veri madenciliği ve örnek temelli veri madenciliği olarak iki başlık halinde kamusal anlamda veri madenciliği kavramı ayrıştırılmaktadır. Konu tabanlı veri madenciliği, kolluk kuvvetlerinin ya da istihbarat görevlilerinin, halihazırda şüphelendikleri konular hakkında veri toplama süreçlerini hızlandırmaktadır.[618]

Örnek temelli veri madenciliği, belirli bir şüphe üzerine başlatılmaz.[619] Örnek temelli veri madenciliği, varsayım üzerine kurulu bir çalışma yapılarak; potansiyel olarak suç işleyebilecek kişilerin belirlenerek örnekseme yoluyla veri tabanlarının taranması ve sonuç elde edilmeye çalışılması anlamına gelmektedir. Bir başka deyişle, konu tabanlı veri madenciliği, olağan makul şüphe ile başlarken; örnek temelli veri madenciliği, şüpheli kişileri belirlemek için veri bağlantılarının tahmin gücü hakkındaki bir teoriye veya teorilere dayanmaktadır.[620]

Özel hayatın gizliliği açısından konu tabanlı veri madenciliği ile örnek temelli veri madenciliğini karşılaştırmak gerektiğinde; konu tabanlı veri madenciliği bir şüphe üzerine gerçekleştirilmekte olup; örnek temelli veri madenciliğinde ortada herhangi bir

---

[616] Mayer-Schönberger, "Big Data," 320.
[617] Yılmaz, *KVK Hukuku*, 170.
[618]
[619] Leslie Harris, "Balancing Privacy and Security: The Privacy Implications of Goverment Data Mining Programs," Hearing Before the Committee on the Judiciary United States Senate 110. Congress (2007): 106.
[620] Rubinstein, "Data Mining," 262-263.

şüphe bulunmamasına rağmen ihtimaller üzerine dayalı işlem gerçekleştirildiğinden, mahremiyet endişesi daha azdır.[621]

Özel şirketlerin de bireyler hakkında kapsamlı bilgiler toplaması için müşteri portföyündeki tüketicileri daha iyi tanıması sağlanarak satış tekniklerini, politikalarını ve kampanyalarını bu veriler doğrultusunda oluşturmaları gibi sebepleri bulunmaktadır.[622] İnternet tabanlı hizmetlerin yaygınlaşmasıyla başta reklam ve pazarlama amacıyla şirketler, kişilerin çevrimiçi etkinliklerini izleyerek; kişilerin kapsamlı olarak profillerini geliştirmektedir. Bu dijital verilerin söz konusu şirketler tarafından oluşturularak işlenmesi ve veri madenciliği yapması, gizlilik ihlali risklerini beraberinde getirmektedir.[623]

Hedefli reklamlar kullanılarak, aynı reklam ağına bağlı olan birden fazla internet sitesini ziyaret ederken kullanıcıların çevrimiçi davranışları hakkında bilgi toplamak için çerezler kullanılmaktadır. Kişilerin tanımlanarak elde edilen verilerin reklam amaçlı kullanımı, 1990'lı yıllardan itibaren yaygınlaşarak, elde edilen verilerin işlenmesi ve gizliliğin yeterince sağlanmaması konusunda bazı şikayetlerin ortaya çıkmasına neden olmuştur.[624] Örneğin DoubleClick, internet kullanıcılarının çevrimiçi etkinliklerini izleyerek; bu izleme verilerini büyük ve aynı zamanda ulusal bir pazarlamada kullanarak; ayrıntılı kişisel bilgiler sayesinde haksız ve yanıltıcı ticari uygulamalar gerçekleştirmiştir.[625]

İnternet kullanıcılarının profillerini geliştirmek için çerezler ile bilgi derleyen bir reklam hizmeti şirketi olan DoubleClick'in, 2000 yılında bir pazarlama firması olan Abacus Direct'i satın alma planı olduğunu duyurması ve kendi çevrimiçi profil önbelleklerini Abacus Direct'in çevrimdışı verileriyle entegrasyonunu sağlamak istemesi çok sayıda veri ihlalinin ortaya çıkabileceği endişesini doğurmuştur.[626]

Arama motorları ile yapılan aramalar, takvimlerin kullanımı, internet tabanlı elektronik postaların kullanımı gibi yollarla internet tabanlı olarak elde edilen veriler, hedefli reklamların yanında, sektörel olarak bu işi yapan şirketlerin daha çok bilgi

---

[621] Harris, "Data Mining Programs," 106.
[622] Yılmaz, *KVK Hukuku*, 170-171.
[623] Rubinstein, "Data Mining," 262-263.
[624] Rubinstein, "Data Mining," 270-271.
[625] Federal Trade Commission, "In the Matter of DoubleClick," "Online Profiling and Privacy," Hearing Before the Committee on Commerce, Science, and Transportation United States Senate 106. Congress, (2000): 64.
[626] Rubinstein, "Data Mining," 270-271.

toplayacakları, işleyeceklerini ve elde edilen verileri hangi amaçla kullanacaklarına karar vereceklerini göstermektedir. Google eski CEO'larından biri olan Eric Schmidt'in *"daha fazla kişisel veri toplamak Google'ın geleceğinin anahtarıdır. Algoritmalar daha iyi hale geldiğinde, kişiselleştirmede daha iyi olacağız. Google kullanıcılarının, yarın ne yapacağım?, hangi işe gireyim? sorularını sorabilmesini hedefliyoruz"* sözü şirketin veri toplamak üzere faaliyet gösterdiğini açıkça göstermektedir.[627]

5.4. ELEKTRONİK HABERLEŞME SEKTÖRÜNDE VERİ MADENCİLİĞİ VE HEDEFLEME KRİTERLERİ ÇERÇEVESİNDE ABONENİN VEYA KULLANICININ VERİLERİNİN YENİDEN DEĞERLENDİRMESİ

Çerezler ve internet tabanlı hizmetlerin kullanımı vasıtasıyla kullanıcılardan toplanan veri yığınlarının yanı sıra elektronik haberleşme sektöründe abonenin, haberleşme hizmetinden faydalanabilmek amacıyla veri sorumlusu işletmeciye verdiği kişisel ve iletişim bilgileri gibi temel nitelikteki veriler kampanyaların yapılandırılması amacıyla yeniden değerlendirmeye tabi tutulabilmektedir. Hedefleme kriterleri olarak adlandırılan bu işleme faaliyetiyle işletmeciler; yaş, cinsiyet, şehir, tarife kullanım kapasitesi gibi çeşitli özelliklere göre sınıflandırdığı kendi abonelerine özel hizmetlerini pazarlayarak çok daha hızlı ve kolay bir şekilde pazarlamasını yaptığı hizmetin satışını yapabilmektedir. İşletmeciler, abonelerini hedefleme kriterleri çerçevesinde değerlendirmeden tüm abonelerine karşı aynı pazarlamayı yaptığında hem reklam maliyeti daha fazla olmakta; hem de daha uzun bir sürede hizmetin hitap ettiği müşteri kitlesine ulaşılabilmektedir.

Elektronik haberleşme sektöründeki işletmecilerin kendi abonelerine hedefleme kriterleri çerçevesinde hizmet sunuyor olmasının yanı sıra özellikle bu sektörün işletmeciye getirmiş olduğu haberleşme hizmetinin hayatın her alanında kullanılması avantajı sayesinde işletmeciler, kendi abonelerinin yaş, cinsiyet, lokasyon gibi kriterlere göre verilerini ayrıştırarak giyim, gıda gibi çeşitli sektörlerde faaliyet gösteren işletmelere hedefli mesaj gönderme hizmeti sunabilmektedir.[628] Bununla birlikte, lokasyon bilgisi ve

---

[627] Rubinstein, "Data Mining," 272-273.

[628] Örneğin, Turkcell İletişim Hizmetleri A.Ş., "Hedefli Mesaj," https://www.turkcell.com.tr/kurumsal/dijital-is-servisleri/diger-kurumsal-cozumler/hedefli-mesaj , Erişim Tarihi: 8 Kasım 2022.

cihaz bilgisinin de hedefli mesaj hizmetine dahil edilmesiyle, bir şehir içerisinde alışveriş merkezine giriş yapan elektronik haberleşme hizmeti sunan işletmecinin abonelerinin tespit edilerek; hedefli mesaj hizmeti alan giyim firmasına bilgi verilmesiyle yalnızca o alışveriş merkezine giren kişilere reklam SMS'i gönderilmesi sağlanabilmektedir. Böylece potansiyel müşteriye daha hızlı ve daha az maliyetle ulaşmak mümkün olmaktadır.

Hedefleme kriterleri çerçevesinde veri sahibinin kişisel verilerinin işlenmesi, açık rıza dışındaki KVKK'da belirtilen hukuka uygunluk nedenleri arasında olmadığından; kişinin verilerinin bu doğrultuda işlenerek reklam içerikli ileti gönderilmesi veya kişisel verilerinin hedefleme kriterleri çerçevesinde yeniden değerlendirmeye tabi tutularak işletmeci tarafından kendisine haberleşme hizmetlerine ilişkin çeşitli hizmetlerin sunulmasının hukuka uygun olabilmesinin tek şartı, veri sahibinin açık rızasının bulunmasıdır. Elektronik haberleşme sektöründeki işletmeciler bu durumun bilincinde olduğundan; genellikle aboneliğin kurulması esnasında abonelik sözleşmesinde veya abonelik sözleşmesinin başında bulunan abone bilgi formuna yerleştirilen abone tercihleri bölümünde abonelerden, işletmecinin sunduğu bazı hizmetlerle erişebilmesi veya hizmetlere ilişkin sunulan avantajlardan faydalanabilmesi veya işletmeci dışında başka şirketlerin reklam içerikli iletilerini alabilmesi amacıyla kişisel verilerinin işlenmesine yönelik açık rızaları alınmaktadır.

SONUÇ

Elektronik haberleşme hizmetlerinden faydalanan abonelerin kendisinin veri sorumlusu olduğu verilerin, elektronik haberleşme sektöründeki işletmeciler tarafından veri işleyen sıfatıyla işlenmesinin yanı sıra bu abonelerin söz konusu elektronik haberleşme hizmetlerinden yararlanmaları sebebiyle işletmecilerin abonesi olmalarından kaynaklı kendilerine sunulan haberleşme hizmeti dolayısıyla abone bilgisi niteliğinde kişisel veriler açığa çıkmaktadır. Bu veriler de elektronik haberleşme sektöründeki işletmeciler tarafından işlenmektedir. Örneğin, müşterilerine toplu SMS göndermek isteyen şirketler, müşterilerinin iletişim ve kimlik bilgilerini almaları ve saklamaları nedeniyle veri sorumlusudur. Müşterilerine ait telefon numaralarını toplu SMS göndereceği elektronik haberleşme sektöründeki işletmecinin sistemine yükleyerek binlerce kişiye SMS gönderilmesi için işletmecinin aracılık yapması durumunda ise söz konusu işletmeci, veri işleyen sıfatını haiz olmaktadır. SMS gönderim talebinde bulunan şirket ise gönderimi sağlayan işletmecinin abonesi olmak zorundadır. Bu sebeple toplu SMS göndermek isteyen şirketin yetkilisi bazı kişisel verilerini, haberleşme hizmeti sunan işletmecinin abonesi olabilmek için işletmeciyle paylaşmak durumundadır. Bununla birlikte, gerçek kişi abonelerin hizmeti kullanımından kaynaklı ortaya çıkan trafik verisi gibi veriler de dahil olmak üzere tüm bu kişisel verilerin işletmeci tarafından işlenmesi halinde, elektronik haberleşme sektöründeki işletmeci, veri sorumlusu sıfatını haiz olmaktadır.

Elektronik haberleşme sektöründeki hizmetlerin kullanımının artmasıyla birlikte, işletmeciler tarafından işlenmek durumunda kalınan veriler de giderek artış göstermektedir. İşletmecilerin bu kadar çok verinin güvenliğini nasıl sağlayacağı ise başlı başına bir sorun teşkil etmektedir. İşletmeciler, sistemlerinde meydana gelebilecek bir saldırı veya veri ihlali durumunda sorumluluklarının büyüklüğü nedeniyle, her an ticari hayatlarının sona erebileceği ve ekonomik zorluklarla karşı karşıya kalma endişesini taşımaktadır. Öte yandan, işlenen verilerin çok sayıda olması ve saklanmasının güçlüğüne rağmen güvenlik sistemlerini geliştirerek, veri merkezlerinde gerekli olan önlemleri alan işletmeciler, elektronik haberleşme sektöründe öne çıkmaya devam edecektir.

Haberleşme hizmetlerinin kullanımından kaynaklı ortaya çıkan verilerin işlenmesi ve korunmasının yanı sıra işletmeciler tarafından aboneden doğrudan alınan kişisel

verilerin doğrulanması konusu ise işletmeciler açısından kişisel verilerin işlenmesi hususunda önem arz eden bir diğer konudur. Kimlik Doğrulama Yönetmeliği'nin yayımlanmasıyla birlikte kimliğin uzaktan doğrulanması mümkün hale gelmiştir. E-Devlet kapısı, ICAO 9303 standardına uygun yakın alan iletişimi özelliği olan belge ile birlikte yapay zeka veya yetkili marifetiyle görüntülü doğrulama, TCKK ile birlikte PAdES oluşturma, yüz yüze kanallarda başvuru sahibinin kimlik belgesi ile birlikte işleme özgülenecek video görüntüsü alma yöntemlerinden biri ile işletmeciler, abonelerinin kimliğini doğrulayarak gerekli işlemleri yürütebilmeye başlamıştır. Söz konusu yöntemler hem maliyet hem de işletmesel anlamda teknik işgücü gerektirdiğinden henüz elektronik haberleşme işletmecilerinin tamamının ilgili yapıları kurduğu söylenemese de bu sektörde tutunabilmek amacıyla zamanla tüm işletmecilerin ilgili yapıları kurmaları gereklilik haline gelecektir.

Uzaktan yapılabilen kimlik doğrulaması sayesinde ıslak imzalı sözleşme zorunluluğu ortadan kalkarak bayi ağı az olan işletmecilerin ülke genelinde hatta yurtdışından abonelik yapabilmelerinin önü açılmıştır. Bunun yanı sıra ıslak imzalı sözleşmelerin kağıt ortamında kurulması sebebiyle belgelerin saklanmasına ilişkin yangın, sel baskını gibi afetlerle karşılaşma riskinin yanı sıra abone sayısı arttıkça evrak sayısı da arttığından, evrakın kağıt ortamında muhafaza edilmesi güçleşmekteydi. Kağıt üzerinde gerçekleştirilen aboneliğin risklerinin yanında abone olmak isteyen kişinin kimlik kontrolünün işletmecinin personeli veya bayisi tarafından yapılması durumunda, kontrol işlemi kişinin inisiyatifine bırakılmak zorunda kalınmaktaydı. Söz konusu durum, abonenin bilgisi dışında abonelik tesis edilmesi riskini de barındırmaktaydı. Bununla birlikte, yüz yüze ortamda kişinin yalnızca kimliğinin ibrazı ile kimlik tespiti işlemi, göz ile kontrol yapılması nedeniyle kesinlik içermemektedir. Bu sebeple işletmeci tarafından abone olmak isteyen kişiden adına kayıtlı fatura, yerleşim yeri ve adres belgesi istenmekteydi. İşletmecinin haberleşme hizmeti sunmak için ihtiyacının olmadığı belgelerin de alınması durumuna neden olmaktaydı. İlgili ek belgeler her ne kadar veri sorumlusu olan işletmecinin kendi yükümlülüğünü yerine getirmesi için işlenmek zorunda olsa da bu belgeler vasıtasıyla elektronik haberleşme hizmetinin sunumu için gerekli olmayan bilgilerin de işletmeci tarafından işlenmesi durumunda kalınmaktaydı. Uzaktan kimliğin doğrulanarak abonelik yapılabilmesiyle, aboneden gerek olmayan evrakın alınmaması sağlanarak hem işletmeci gereksiz bilgileri saklama

yükümlülüğünden hem de abone fazladan kişisel verisini paylaşma zahmetinden kurtulmuştur.

Abonenin kimliğinin uzaktan doğrulanabilmesi yönteminin her ne kadar numara taşıma gibi işlemler için de gerçekleştirilebileceği konuya ilişkin mevzuattan anlaşılıyor olsa da henüz Numara Taşıma Sistemi ile video kaydı içeren bir kimlik doğrulama dosyasının kapasitesi kadar büyük dosyaların paylaşımına izin verilmediği göz önünde bulundurulduğunda; numara taşıma işlemi için uzaktan aboneliğin geçerli bir yöntem olmadığı tespit edilmiştir. Bununla birlikte, numara taşıma işleminin gerçekleştirilebilmesi için aboneden alınan talep formunun yanı sıra kişinin kimliğinin doğrulanması yükümlülüğü numarayı diğer işletmeciye taşıyacak olan verici işletmecide olduğunda; alıcı işletmeciler bu büyük veri içeren dosyaların kendilerine gönderilmesini istememekte, başka bir yöntem ile verici işletmecinin kişinin kimliğini doğrulamasını talep etmektedir. İşletmeciler hali hazırda kendi abonelerinden kaynaklanan büyük kişisel veri yığınlarının risklerini alırken; bir de numara taşıma işlemiyle kendilerine gelecek abonelerin kimlik doğrulamalarına ilişkin video kaydı gibi büyük verilerin sorumluluğunu almak istememektedir. Bu durum karşısında, uzaktan kimliğin doğrulanması işlemi, uygulanmaya yeni başlanması sebebiyle sektörde şimdilik bu şekilde ilerlese de ileride bu konuda da geliştirme yapılacağı düşünülmektedir.

Elektronik haberleşme sektörü, kişisel verilerin çokça işlendiği bir sektördür. İnternetin mobil cihazlarda da kullanılabilirliğinin artması ve haberleşmenin hayatın her anında var olması durumu, herkesin en azından bir haberleşme aboneliğinin olması gerekliliğini ortaya çıkarmaktadır. Artan abone sayısı, artan veri anlamına geldiğinden; gün geçtikçe işletmecilerin işledikleri büyük veri toplulukları oluşturmaktadır. Abonenin kişisel verisinin gizliliği esas olup; açık rızası bulunmadan veya KVKK'da belirtilen hukuka uygunluk nedenleri olmadığı sürece verilerin işlenmesi hukuka aykırı olmaktadır. Bununla birlikte, kişiden onay almadan ileti gönderilemeyeceği düşüncesi de kişilerden sürekli şekilde açık rızalarının alınmasına neden olmuştur. Veri sorumluları kendi yükümlülükleri sebebiyle veri işlemek zorunda olsalar bile veri sahibinin açık rızası olmadan işlediğinde hukuka aykırı olacağı düşüncesiyle gerek olmadığı halde rıza talep etmeye başlamıştır. Veri sahibinin rıza yorgunluğuna sebep olan bu durum, ilgili kişiler tarafından bilgilendirme metinlerini okumadan rıza vermeleri sonucunu ortaya çıkarmıştır. Bu durum, gizliliği önem arz eden verilerin işlenmesi yoluyla kişisel verilerin

korunması açısından tehlike oluşturmaktadır. Ayrıca veri sorumluları açısından düşünüldüğünde ise veri sorumluları yasal yükümlülüklerini yerine getirme amacıyla veri işleyebilmelerine rağmen veri sahiplerinden açık rıza da istediklerinden, gerçekte böyle olmasa da veri sahiplerinde verilerinin işlenmesinin yalnızca veri sahiplerinin kendi rızalarına bağlı olduğu düşüncesi ilgili kişilerde oluşmaktadır. Görülmektedir ki; veri işleme konusunda ilgili kişinin rızasının alınması kadar veri sorumlularının da hak ve yükümlülüklerini bilmesi önem arz etmektedir.

Abonelerden elde edilen verilerin işletmeci tarafından işlenerek saklanması, verilerin boyutunun giderek artmasıyla birlikte yük olmaktan çıkartılmak istenmektedir. Bu doğrultuda kişisel verilerin, işletmecilerin kendileri açısından olumlu sonuçlar elde edebilmelerine yönelik yeniden değerlendirilebileceği düşüncesi ortaya çıkmıştır. Veriler yeniden değerlendirmeye tabi tutularak kullanıcılara sunulabilecek yeni hizmetler oluşturmak istenmiştir. Çerezler vasıtasıyla kullanıcıların profillerinin belirlenebilmesinin yanı sıra işletmecilerde bulunan abone verilerinin yaş, cinsiyet, abonenin bulunduğu şehir gibi kriterlere göre sınıflandırılması suretiyle de kullanıcı profili belirlenebilmektedir. Kriterlere göre gruplandırılan abonelere özel hizmetler hazırlanarak; ürünün hitap ettiği müşteri kitlesine hızlı bir şekilde erişilebilmekte olup; hizmetten edinilen kar da bir o kadar hızlı şekilde artmaktadır. Hedefleme kriterleri vasıtasıyla işletmecilerin kendi abonelerine ek hizmetler sunabilmesinin yanı sıra kriterlere göre belirlenen müşteri kitlesine hedefli mesaj gönderimi gibi hizmetler ise işletmecilerin abonesi olan ve ticari elektronik ileti gönderimi yapan çeşitli sektörlerde faaliyet gösteren şirketlere pazarlanabilmektedir.

Çalışmanın genelinde yer verildiği üzere, elektronik haberleşme sektöründe işlenen kişisel verilerin korunması, başta işletmecinin sorumluluklarının bilincinde olarak abonenin kişisel verilerinin gizliliğini sağlamak amacıyla mevzuata uygun faaliyetler yerine getirmesi ve gerekli tedbirleri almasıyla mümkün olabilecektir. Abonenin ise her ne kadar mevzuat gereğince elektronik haberleşme aboneliği için bazı kişisel verilerinin işlenmesi zorunlu olsa da verilerinin işlenmesine yönelik vermiş olduğu rızaların bilincinde olarak; aboneliğine izinsiz girişleri önleyebilmek amacıyla veri gizliliğini sağlayacak şekilde kişisel bilgilerini başkalarıyla paylaşmaması gerekmektedir.

KAYNAKÇA

Açıkgöz, Osman. *Tüketicinin Korunması Çerçevesinde Mobil Haberleşme Abonelik Sözleşmesinde Genel İşlem Koşulları*. İstanbul: On İki Levha Yayıncılık, 2013.

Akıncı, Ayşe Nur. "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi." *Kalkınma Bakanlığı Çalışma Raporu* no.6 (2017):1-41. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf . Erişim Tarihi: 17 Mayıs 2022.

Akkurt, Sinan Sami. "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri." *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 60, no.1 (2011):19-46.

Aksoy, Hüseyin Can, Mesut Halıcıoğlu. "AB ve Türk Hukuklarında Çerezler: Kişisel Verilerin Korunması Açısından Karşılaştırmalı Bir Değerlendirme." *Kişisel Verileri Koruma Dergisi,* no.3 (2021): 61-88.

Aksoy, Hüseyin Can, Mesut Halıcıoğlu. "E-Gizlilik Tüzüğü Çalışmaları Işığında Türk Hukukunda Elektronik Haberleşmenin Gizliliğinin Korunması." *Kişisel Verileri Koruma Dergisi* 2, no.2 (2020): 1-18.

Aktan, Ertuğrul. "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu." Ankara Üniversitesi Bilgi Yönetimi Dergisi 1, no.1 (2018): 1-22.

Akyılmaz, Bahtiyar, Murat Sezginer, Cemil Kaya, *Türk İdare Hukuku*. Ankara: Savaş Yayınevi, 2021.

Aladeokin, Adeyemi, Pavol Zavarsky, Neelam Memon. "Analysis and Compliance Evaluation of Cookies-Setting Websites with Privacy Protection Laws." *2017 Twelfth International Conference on Digital Information Management (ICDIM),* (2017):121-126. https://ieeexplore.ieee.org/document/8244646 . Erişim Tarihi: 3 Temmuz 2022.

Aldridge. “IT Security Levels.” aldridge.com. https://aldridge.com/it-security-levels/ . Erişim Tarihi: 14 Eylül 2022.

Allen, Anita L. “An Ethical Duty to Protect One’s Own Information Privacy?.” *Alabama Law Review*, no:64 (2013): 845-866.

Allen, Anita L. “Law, Privacy & Technology Commentary Series Protecting One’s Own Privacy In A Big Data Economy,” *Harvard Law Review Forum*, no.130 (2016): 71-78.

Alongi, Elizabeth A. “Has The U.S. Canned Spam?.” *Arizona Law Review* 46, no.2 (2004): 263-290. https://arizonalawreview.org/pdf/46-2/46arizlrev263.pdf . Erişim Tarihi: 30 Mayıs 2022.

Altın, Aytuğ. “Kamu Hizmeti Anlayışında Değişim.” *Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (2013): 101-118.

Anayasa Mahkemesi. 2008/115 E., 2011/86 K. sayılı Kararı. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2011-86-nrm.pdf . Erişim Tarihi: 26 Eylül 2022.

Anayasa Mahkemesi. 2014/149 E., 2014/151 K. sayılı Kararı. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-151-nrm.pdf . Erişim Tarihi: 4 Ekim 2022.

Anayasa Mahkemesi. 09.04.2014 tarih ve E. 2013/122, K. 2014/74 sayılı Kararı. https://normkararlarbilgibankasi.anayasa.gov.tr/Dosyalar/Kararlar/KararPDF/2014-74-nrm.pdf . Erişim Tarihi: 23 Ekim 2022.

Anayasa Mahkemesi. 2013/5653 Başvuru numaralı, 03.03.2016 tarihli Kararı. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/5653 , Erişim Tarihi: 30 Ekim 2022.

Anayasa Mahkemesi. 2018/6161 Başvuru numaralı 28.06.2022 tarihli Karar. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/6161 , Erişim Tarihi: 21 Aralık 2022.

Anayasa Mahkemesi. 2013/1789 Başvuru numaralı ve 11.11.2015 tarihli Kararı. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/1789 . Erişim Tarihi: 22 Ekim 2022.

Andrew, Jonathan. "Locatian Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights." *European University Institute Department of Law PhD Theses*, (2018), https://cadmus.eui.eu/bitstream/handle/1814/51585/Andrew_2018_LAW_add_addendum.pdf?sequence=4&isAllowed=y . Erişim Tarihi: 2 Ekim 2022.

Arıcı, Haydar Yener. *Adli Bilişim*. Ankara: Seçkin Yayıncılık, 2018.

Article 29 Çalışma Grubu. Guidelines on Consent Under Regulation 2016/679 (2018). https://ec.europa.eu/newsroom/article29/items/623051 . Erişim Tarihi: 28 Mayıs 2022.

Article 29 Çalışma Grubu. Opinion 04/2012 on Cookie Consent Exemption , (2012). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf . Erişim Tarihi: 27 Temmuz 2022.

Article 29 Çalışma Grubu. Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies, (2013). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf . Erişim Tarihi: 21 Temmuz 2022.

Article 29 Çalışma Grubu. Guidelines on the Right to Data Portability, https://ec.europa.eu/newsroom/article29/items/611233 . Erişim Tarihi: 28 Ekim 2022.

Article 29 Çalışma Grubu. Guidelines on the Implementation of the Court Of Justice of the European Union Judgment on "Google Spain and Inc V. Agencia Española De Protección De Datos (Aepd) and Mario Costeja González" C-131/12, (2014). https://ec.europa.eu/newsroom/article29/items/667236/en . Erişim Tarihi: 30 Ekim 2022.

Aşıkoğlu, Şehriban İpek. "Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda-." *Kişisel Verileri Koruma Dergisi* 1, no.2 (2019): 41-65.

Atak, Songül. "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler." *Türkiye Barolar Birliği Dergisi*, no.87 (2010): 90-120.

Atar, Eray Aksın, Ertuğrul Erzengin. "Mukayeseli Hukukta Standart Sözleşme Hükümlerinin Çatışması ve Bu Duruma Bağlanan Hukuki Sonuçlar," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 26, no.1 (2020):339-381.

Atay, Ender Ethem. *İdare Hukuku* (Ankara: Seçkin Yayıncılık, 2022).

Avrupa Birliği Adalet Divanı. Case C-131/12 numaralı, 13.05.2014 tarihli Karar, https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=155358 . Erişim Tarihi: 30 Ekim 2022.

Avrupa Birliği Adalet Divanı. Case C-203/15 numaralı, 21.12.2016 tarihli Karar. https://privacyinternational.org/sites/default/files/2019-08/CELEX_62015CJ0203_EN_TXT.pdf . Erişim Tarihi: 21 Ekim 2022.

Avrupa Birliği Adalet Divanı. Case C-293/12 numaralı, 08.04.2014 tarihli Karar. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=4 . Erişim Tarihi: 21 Ekim 2022.

Avrupa Birliği Adalet Divanı. Case C-301/06 numaralı, 10.02.2009 tarihli Karar. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62006CJ0301&from=en . Erişim Tarihi: 18 Ekim 2022.

Avrupa İnsan Hakları Mahkemesi. 30562/04 ve 30566/04 Başvuru numaralı, 04.12.2008 tarihli Karar. https://rm.coe.int/168067d216 . Erişim Tarihi: 18 Ekim 2022.

Ayenson, Mika D, Dietrich James Wambach, Ashkan Soltani, Nathan Soltani, Chris Jay Hoofnagle. "Flash Cookies and Privacy II: Now with HTML5 and ETag

Respawning." ssrn.com (2011):1-21. http://dx.doi.org/10.2139/ssrn.1898390 . Erişim Tarihi: 12 Temmuz 2022.

Azurmendi, Ana. "Spain: The Right to Be Forgotten The Right to Privacy and the Initiative Facing the New Challenges of the Information Society." ed. Wolf J. Schünemann, Max-Otto Baumann, Privacy, Data Protection and Cybersecurity in Europe. Cham, Switzerland: Springer, 2017:17-30. https://link.springer.com/chapter/10.1007/978-3-319-53634-7_2 . Erişim Tarihi: 29 Ekim 2022.

Bal, Yakup. *6502 sayılı Tüketicinin Korunması Hakkında Kanun Kapsamında Abonelik Sözleşmeleri*. Ankara: Seçkin Yayıncılık, 2020.

Balaban, Mahmut Furkan. "İleti Yönetim Sisteminin Kurulması ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in Değerlendirilmesi." *Bilişim Hukuku Dergisi* 2, no.2 (2020): 181-219.

BBC News. Madrid Train Attacks. http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/. Erişim Tarihi: 16 Ekim 2022.

BBC News. Bomb Attacks on London. http://news.bbc.co.uk/onthisday/hi/dates/stories/july/7/newsid_4942000/4942238.stm . Erişim Tarihi: 16 Ekim 2022.

Berghel, Hal. "Toxic Cookies." *Computer* 46, no.9 (2013): 104-107. http://ww.berghel.net/col-edit/out-of-band/sept-13/oob_9-13.pdf . Erişim Tarihi: 5 Temmuz 2022.

BGA Security. "10 Soruda Sızma Testi Nedir?," bgasecurity.com, https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/ . Erişim Tarihi: 28 Ekim 2022.

Bianco, Ginevra. "An Empirical Analysis Of Consumer Response To Google's Decision Of Phasing Out Third Party Cookies." *Luiss Guido Carli University Department of Economics and Finance Course of Marketing*, (2020): 1-64.

https://www.researchgate.net/publication/345253989_An_empirical_analysis_of_consumer_response_to_Google's_decision_of_phasing_out_third_party_cookies/link/5fa191f0299bf1b53e5d1a98/download . Erişim Tarihi: 10 Temmuz 2022.

Bilgi Teknolojileri ve İletişim Kurumu. AB Elektronik Haberleşme Düzenlemeleri. https://www.btk.gov.tr/ab-elektronik-haberlesme-duzenlemeleri . Erişim Tarihi: 28 Şubat 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Yetkilendirme Yönetim Sistemi. https://yetkilendirme.btk.gov.tr/Yetkilendirme/isletmeci-arama.xhtml;jsessionid=3UGcwEIkVM3KfxvHMeVfdxgurRAyEVYtNxF5uCm4.be1 . Erişim Tarihi: 4 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 16.05.2017 tarih ve 2017/DK-YED/163 sayılı Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/yetkisiz-hizmet-sunumu-sazak-haberlesme.pdf . Erişim Tarihi: 2 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 24.03.2020 tarih ve 2020/İK-YED/085 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-izinsiz-hisse-devri-ve-mevzuata-aykiri-islemler-lodosnet/85-2020-web.pdf . Erişim Tarihi: 3 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 31.03.2016 tarih ve 2016/DK-YED/195 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/yetkilendirme-yonetmeligi-degisikligi.pdf . Erişim Tarihi: 3 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 16.03.2021 tarih ve 2021/DK-YED/80 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorune-iliskin-yetkilendirme-yonetmeligi-nde-degisiklik-yapilmasina-dair-yonetmelik-ile-yetkilendirme-basvurusu-sartlarina-ve-surelerine-iliskin-duzenlemeler/80-2021-web.pdf . Erişim Tarihi: 5 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Mobil İletişimde Yeni Teknoloji 4.5G Broşürü. https://www.btk.gov.tr/uploads/pages/slug/45g-brosur.pdf . Erişim Tarihi: 5 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 04.05.2021 tarih ve 2021/İK-SDD/120 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/inceleme-sebeke-ve-bilgi-guvenligine-acentelik-faaliyetlerine-abonelik-sozlesmelerine-ve-cli-a-iliskin-mevzuat-yukumlulukleri-bir-telekom-alfa-iletisim-regnum-nehir-telekom/120-2021-web.pdf . Erişim Tarihi: 6 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Yetkilendirme İçin Başvuru Adımları, https://www.btk.gov.tr/yetkilendirme-icin-basvuru-adimlari . Erişim Tarihi: 3 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 11.08.2014 tarih ve 2014/DK-THD/395 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/abonelik-sozlesmesi-olmaksizin-hizmet-sunulmasi.pdf . Erişim Tarihi: 6 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 25.05.2021 tarih ve 2021/İK-THD/134 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-abonelik-sozlesmesinin-tesisine-iliskin-mevzuat-ihlali-turknet/134-2021-web.pdf . Erişim Tarihi: 7 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 16.03.2021 tarih ve 2021/İK-THD/76 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-tuketici-haklarina-iliskin-mevzuat-ihlali-katlama-kampanyasi-turkcell/76-2021-web.pdf . Erişim Tarihi: 25 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.05.2018 tarih ve 2018/DK-THD/162 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/tuketici-ve-kullanici-sikayetlerinin-isletmeciler-ve-posta-hizmet-saglayicilari-tarafindan-cozumlenmesine-iliskin-usul-ve-esaslar/162-2018-web.pdf . Erişim Tarihi: 12 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 01.09.2016 tarih ve 2016/DK-THD/393 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/adil-kullanim-noktasi-akn-uygulamasi.pdf . Erişim Tarihi: 22 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 27.12.2016 tarih ve 2016/DK-THD/518 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/adil-kullanim-noktasi-akn.pdf . Erişim Tarihi: 22 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.06.2021 tarih ve 2021/İK-ETD/169 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorunde-basvuru-sahibinin-kimliginin-dogrulanma-sureci-hakkinda-yonetmelik/169-2021-web.pdf . Erişim Tarihi: 22 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 06.01.2014 tarih ve 2014/DK-THD/25 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/engelli-tuketicilere-yonelik-duzenlemeler-konulu-kurul-karari.pdf . Erişim Tarihi: 22 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 17.10.2018 tarih ve 2018/İK-SDD/309 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/inceleme-vodafone-muhtelif-tuketici-sikayetleri/309-web.pdf . Erişim Tarihi: 23 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 14.09.2021 tarih ve 2021/İK-YED/282 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-acentelik-ve-bilgi-verme-ile-ilgili-mevzuat-ihlali-high-speed/282-2021-web.pdf . Erişim Tarihi: 4 Ekim 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 23.07.2018 tarih ve 2018/DK-ETD/222 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/engelli-gazi-ve-sehit-yakinlarina-yonelik-indirimli-internet-tarifelerinin-uygulama-esaslarinin-guncellenmesi/222-02-engelli-gazi-ve-sehit-yakinlarina-yonelik-indirimli-internet-tarifelerinin-uyg-23-07-2018.pdf . Erişim Tarihi: 23 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 19.11.2015 tarih ve 2015/DK-SDD/516 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/inceleme-turk-telekom-ayrim-gozetmeme.pdf . Erişim Tarihi: 24 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 27.01.2010 tarih ve 2010/DK-10/49 sayılı BTK Kurul Kararı, https://www.btk.gov.tr/uploads/boarddecisions/mobil-elektronik-haberlesme-sektorunde-seffafligin-saglanmasi.pdf . Erişim Tarihi: 25 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 17.02.2010 tarih ve 2010/DK-10/103 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/turk-telekomunikasyon-a-s-nin-sabit-sebekede-cagri-tasima-piyasasinda-etkin-piyasa-gucune-sahip-isletmeci-olarak-belirlenmesi.pdf . Erişim Tarihi: 1 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.07.2020 tarih ve 2020/İK-THD/210 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-tuketici-sikayetleri-vodafone-net/210-2020-web.pdf . Erişim Tarihi: 25 Mart 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Pazar Analizi Raporları https://www.btk.gov.tr/pazar-verileri . Erişim Tarihi: 1 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, İşletmeci Veri Formunun Doldurulmasına Yönelik Kılavuz. https://www.btk.gov.tr/uploads/pages/isletmeci-veri-formlari/isletmeci-veri-formu-doldurma-kilavuzu-final1.pdf . Erişim Tarihi: 1 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 08.06.2021 tarih ve 2021/DK-ETD/151 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/mobil-cagri-sonlandirma-ucretleri/151-2021-web.pdf . Erişim Tarihi: 3 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 17.06.2014 tarih ve 2014/DK-ETD/324 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/referans-tesis-paylasimi-ve-aydinlatilmamis-fiber-teklifi.pdf . Erişim Tarihi: 3 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.02.2022 tarih ve 2022/DK-ETD/53 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/referans-teklif-degisiklikleri-kimlik-dogrulama-yonetmeligi/53-2022-web.pdf . Erişim Tarihi: 3 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 14.12.2016 tarih ve 2016/UK-ETD/490 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/uzlastirma-turknet-ile-turk-telekom.pdf . Erişim Tarihi: 3 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 05.09.2012 tarih ve 2012/DK-07/415 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/netgsm-ile-vodafone-net-ve-netgsm-ile-vodafone-alternatif-arasinda-isletilen-uzlastirma-prosedurleri.pdf . Erişim Tarihi: 3 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 28.12.2021 tarih ve 2021/İK-THD/408 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/idari-yaptirim-2020-yili-birinci-ceyrek-donem-cagri-merkezi-hizmetine-iliskin-hizmet-kalitesi-yukumlulukleri-ttnet-turkcell-vodafone-millenicom-andromeda/408-2021-web.pdf . Erişim Tarihi: 12 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 27.12.2016 tarih ve 2016/DK-YED/516 sayılı BTK Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/ehsiyy-gecici-8-maddenin-ucuncu-fikrasinin-yurutulmesi.pdf . Erişim Tarihi: 13 Nisan 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 24.03.2020 tarih ve 2020/DK-THD/084 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/tuketici-sikayetleri-anlik-bildirimler-pop-up-push-notification-vb-ile-alinan-onay-riza/84-2020-web.pdf . Erişim Tarihi: 29 Mayıs 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.12.2021 tarih ve 2021/DK-BTD/403 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/elektronik-haberlesme-sektorunde-basvuru-sahibinin-kimliginin-dogrulanma-sureci-hakkinda-yonetmelikte-degisiklik-yapilmasina-dair-yonetmelik/403-2021-web.pdf . Erişim Tarihi: 4 Eylül 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 19.01.2016 tarih ve 2016/DK-SDD/30 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/aloses-numara-tasima-sistemi-baglantisi-ve-abonelik-sozlesmesi-sikayeti-plandisi-inceleme.pdf . Erişim Tarihi: 4 Eylül 2022.

Bilgi Teknolojileri ve İletişim Kurumu. 22.09.2014 tarih ve 2014/DK-THD/466 sayılı Kurul Kararı. https://www.btk.gov.tr/uploads/boarddecisions/borc-ve-alacak-bilgilerinin-sorgulanmasina-iliskin-usul-ve-esaslar.pdf . Erişim Tarihi: 14 Eylül 2022.

Bilgi Teknolojileri ve İletişim Kurumu. Türkiye Elektronik Haberleşme Sektörü 2022 yılı 2. Çeyrek Üç Aylık Pazar Verileri Raporu, https://www.btk.gov.tr/uploads/pages/pazar-verileri/2022-2-kurumdisi.pdf . Erişim Tarihi: 11 Ekim 2022.

Case C-673/17. 1 Ekim 2019. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=197495 . Erişim Tarihi: 20 Temmuz 2022.

Cisco. "Digital Subscriber Line (DSL)." cisco.com, https://www.cisco.com/c/en_uk/solutions/routing-switching/dsl.html . Erişim Tarihi: 16 Ekim 2022.

Claessens, Joris, Claudia Diaz, Caroline Goemans, Bart Preneel, Joos Vandewalle, Jos Dumortier, "Revocable Anonymous Access to the Internet." Computer Security and Industrial Cryptography (COSIC), Interdisciplinary Centre for Law and Information Technology (ICRI), 2002. https://www.esat.kuleuven.be/cosic/publications/article-92.pdf . Erişim Tarihi: 30 Ekim 2022.

Commercial Electronic Mail Message. https://www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=15-USC-941144812-289124299&term_occur=2&term_src=title:15:chapter:103:section:7702 . Erişim Tarihi: 1 Haziran 2022.

Convention 108 + Convention for the Protection of Individuals with regard to the Processing of Personal Data.

https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf . Erişim Tarihi: 17 Mayıs 2022.

Countly. Push Notifications: A Review of Best Practices for Mobile Product Managers. Count.ly. https://count.ly/resources/white-papers/countly_push-notifications-a-review-of-best-practices-for-mobile-product-managers.pdf . Erişim Tarihi: 29 Mayıs 2022.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı. Temmuz 2020. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf . Erişim Tarihi: 28 Ekim 2022.

Çağlayan, Ramazan. İdare Hukuku Dersleri. Ankara: Adalet Yayınevi, 2021.

Çekin, Mesut Serdar. "Telekomünikasyon Sektöründe Şeffaflık İlkesi ve Sağlayıcının Bilgilendirme Yükümlülüğü." İç. Telekomünikasyon Hukuku, editör Halil Akkanat. İstanbul: Filiz Kitabevi, 2017: 80-95.

Çekin, Mesut Serdar. *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık, 2019.

Çelikel, Serdar. "Kişisel Verilerin İşlenmesinde, Açık Rıza Hukuka Uygunluk Nedeninin, 95/46 Sayılı Direktif ve Gdpr'la Karşılaştırmalı Olarak İncelenmesi." *Uyuşmazlık Mahkemesi Dergisi* 9, no.17 (2021): 161-190.

Davis, Vivian Witkind, David Landsbergen, Raymond W. Lawton, Larry Blank, Nancy Zearfoss, John Hoag. Telecommunications Service Quality, (Ohio: The National Regulatory Research Institute, 1996. https://ipu.msu.edu/wp-content/uploads/2016/12/Davis-Telecom-Service-Quality-96-11-Mar-96.pdf . Erişim Tarihi: 12 Nisan 2022.

Değirmenci, Olgun. "Yargısal İçtihatların Ortaya Çıkardığı Bir Hak: Unutulma Hakkı (Çerçevesi ve Hak Üzerine Düşünceler)." *Terazi Hukuk Dergisi* 13. no.144 (2018): 153-163.

Determann, Lothar. *Kişisel Verilerin Korunması Uygulama Kılavuzu Şirketlerin Uluslararası Mevzuata Uyumu*. İstanbul: On İki Levha Yayıncılık, 2020.

Direct-Dial-In (DDI). https://dialogictelecom.com/2021/01/what-is-a-ddi-telephone-number/ . Erişim Tarihi: 26 Eylül 2022.

Directive 1997/66/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN . Erişim Tarihi: 17 Temmuz 2022.

Directive 2002/19/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0019&from=EN . Erişim Tarihi: 28 Şubat 2022.

Directive 2002/20/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0020&from=EN . Erişim Tarihi: 28 Şubat 2022.

Directive 2002/21/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en . Erişim Tarihi: 28 Şubat 2022.

Directive 2002/58/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN . Erişim Tarihi: 28 Şubat 2022.

Directive 2002/77/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0077&from=EN . Erişim Tarihi: 1 Nisan 2022.

Directive 2006/24/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0024&from=en . Erişim Tarihi: 16 Ekim 2022.

Directive 2009/136/EC of the European Parliament and of the Council, EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN . Erişim Tarihi: 6 Mart 2022.

Doğan, Başak, Tuğçe Bozkurt. "Kişisel Verilerin Korunması Çerçevesinde Çerezler; Türleri, Kullanımları ve Uygulama Örnekleriyle." blog.lexpera.com.tr, Son Güncelleme: 10 Eylül 2020, https://blog.lexpera.com.tr/kisisel-verilerin-korunmasi-cercevesinde-cerezler-turleri-kullanimlari-ve-uygulama-ornekleriyle/ . Erişim Tarihi: 5 Temmuz 2022.

Doğan, Korcan, Sacit Arslantekin. "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum," Ankara Üniversitesi Dil Tarih Coğrafya Fakültesi Dergisi 56, no.1 (2016): 15-36.

Dural, Mustafa, Tufan Öğüz. *Türk Özel Hukuku Cilt II Kişiler Hukuku*. İstanbul: Filiz Kitabevi, 2012.

Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi Yayıncılık, 2020.

Dülger, Murat Volkan. "Yurt Dışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı." ssrn.com. 1-11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388 . Erişim Tarihi: 1 Ağustos 2022.

Dwyer, Tim. "Privacy From Your Mobile Devices? Algorithmic Accountability, Surveillance Capitalism, and the Accumulation of Personal Data,". ed. Rich Ling, Leopoldina Fortunati, Gerard Goggin, Sun Sun Lim, Yuling Li. iç. *The Oxford Mobile Handbook of Mobile Communication and Society*. (Oxford: Oxford University Press, 2020).

E-Devlet, e-Kayıt Başvurusu Onay İşlemleri, https://www.turkiye.gov.tr/btk-e-kayit-basvurusu-onay-islemleri-gercek-kisi . Erişim Tarihi: 10 Eylül 2022.

E-Devlet, Ticari Elektronik İleti Şikayet Sistemi, https://www.turkiye.gov.tr/gtb-ticari-elektronik-ileti-sikayet-sistemi . Erişim Tarihi: 9 Ekim 2022.

Egan, Erin. Charting a Way Forward Data Portability and Privacy, Facebook, 2019. https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf , 3. Erişim Tarihi: 28 Ekim 2022.

Ekici, Şerafettin. *Bilişim ve Teknoloji Hukuku*. Ankara: Seçkin Yayıncılık, 2022.

Ekici, Şerafettin. *Özel Sektöre Açıldıktan Sonra Türk Telekomünikasyon Hukuku (Elektronik İletişim)*. İstanbul: Vedat Kitapçılık, 2006.

Elagib, Sara B., Aisha-Hassan A. Hashim, R. F. Olanrewaju. "CDR Analysis using Big Data Technology." International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering. 2015: 467-471. https://ieeexplore.ieee.org/document/7381414 . Erişim Tarihi: 9 Ekim 2022.

Elektronik Haberleşme Kanunu Tasarısı ile Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu Raporu (1/1120). https://www5.tbmm.gov.tr/sirasayi/donem22/yil01/ss1057m.htm . Erişim Tarihi: 1 Mart 2022.

Ercoşkun Şenol, Kübra. "Sözleşmenin İçeriğini Belirleme Özgürlüğü ve Bunun Genel Sınırı: TBK m.27." *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 74, no.2 (2016): 709-737.

Eren, Abdurrahman. *Anayasa Hukuku Dersleri*. Ankara: Seçkin Yayıncılık, 2021.

Erol, Mesut. "Kamu Hizmetlerinin Görülüş Usullerinden Ruhsat (Lisans, İdari İzin, Yetkilendirme) Yöntemi ve Düzenleyici ve Denetleyici Kurumların Lisans Konusundaki Yetkilerinin Danıştay Kararları Çerçevesinde Değerlendirilmesi." *Türkiye Barolar Birliği Dergisi*. no.90 (2010): 344-378.

Ersöz, Oğuz. "Genel İşlem Koşullarının Kişi Bakımından Uygulama Alanı ve Tacirler Hakkında Uygulanması." *İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi* 3. no.1 (2017): 69-104.

EUR-Lex. 10 Şubat 2021 tarihli Elektronik Haberleşme Direktifi Taslağı. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN . Erişim Tarihi: 1 Ağustos 2022.

EUR-Lex. 2015/2120 sayılı Açık İnternet Erişimi ile ilgili Önlemleri Belirleyen ve Evrensel Hizmet ve Elektronik İletişim Ağları ve Hizmetlerine İlişkin Kullanıcı Haklarına İlişkin 2002/22/EC Sayılı Direktif'i ve AB İçerisinde Genel Mobil İletişim Ağlarında Dolaşıma İlişkin 531/2012 Sayılı Direktif'te Değişiklik Yapan Direktif, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN . Erişim Tarihi: 20 Ağustos 2022.

EUR-Lex. Elektronik Haberleşme Direktifi'nde yapılan değişiklikleri gösteren taslakların yayımlanma süreci, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010 . Erişim Tarihi: 1 Ağustos 2022.

EUR-Lex. European Electronic Communications Code. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN . Erişim Tarihi: 3 Ağustos 2022.

European Data Protection Board (EDPB). Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021 https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-032021-eprivacy-regulation_en . Erişim Tarihi: 24 Temmuz 2022.

European Data Protection Board (EDPB). Guidelines 05/2020 on Consent under Regulation 2016/679, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf , Erişim Tarihi: 22 Mayıs 2022.

European Telecommunications Standards Institute (ETSI). “Satellite for UMTS/IMT-2000,” etsi.org, https://www.etsi.org/technologies/satellite/satellite-umts-imt-2000 . Erişim Tarihi: 4 Ekim 2022.

European Treaty Series - No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, https://rm.coe.int/1680078b37 . Erişim Tarihi: 17 Mayıs 2022.

Federal Trade Commission. “In the Matter of DoubleClick,” “Online Profiling and Privacy,” Hearing Before the Committee on Commerce, Science, and Transportation United States Senate 106. Congress, (2000).

Firdous, Sadaf, Rahela Farooqi. Service Quality To E-Service Quality: A Paradigm Shift, (Bangkok: Industrial Engineering and Operations Management Society International-IEOM, 2019:1656-1666. http://www.ieomsociety.org/ieom2019/papers/404.pdf . Erişim Tarihi: 10 Nisan 2022.

General Data Protection Regulation (GDPR). https://gdpr-info.eu . Erişim Tarihi: 17 Mayıs 2022.

General Data Protection Regulation (GDPR). Article 94. https://gdpr-info.eu/art-94-gdpr/ . Erişim Tarihi: 17 Mayıs 2022.

Goemans, Caroline, Jos Dumortier. “Enforcement Issues - Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity.” (2003):1-20. https://www.law.kuleuven.be/citip/en/archive/copy_of_publications/440retention-of-traffic-data-dumortier-goemans2f90.pdf . Erişim Tarihi: 1 Ekim 2022.

González, Elena Gil, Paul De Hert, Vagelis Papakonstantinou. “The Proposed Eprivacy Regulation: The Commission’s and the Parliament’s Drafts At A Crossroads?.” *Brussels Privacy Hub Working Paper* 6, no.20 (2020): 1-29. https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOL6-N20.pdf . Erişim Tarihi: 15 Mayıs 2022.

Google Workspace Yöneticisi Yardım. "CAPTCHA nedir?." https://support.google.com/a/answer/1217728?hl=tr . Erişim Tarihi: 28 Ekim 2022.

Göçmen Uyarer, Sinem. *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Ankara: Seçkin Yayıncılık, 2020.

Gören, Zafer. "Genel Eşitlik İlkesi." *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 22*, no.3 (2016): 3279-3301.

Grabowska-Moroz, Barbara. "Data Retention in the European Union." iç. *European Constitutional Courts towards Data Retention Laws*. ed. Marek Zubik, Jan Podkowik, Robert Rybski. Switzerland: Springer Nature, 2021.

Gregory, Peter. IT Disaster Recovery Planning For Dummies, Hoboken: Wiley Publishing, 2011. https://books.google.com.tr/books?id=YC49DXW-_60C&printsec=frontcover&dq=IT+Disaster+Recovery+Planning+For+Dummies&hl=tr&sa=X&redir_esc=y#v=onepage&q=IT%20Disaster%20Recovery%20Planning%20For%20Dummies&f=false . Erişim Tarihi: 21 Eylül 2022.

Harris, Leslie. "Balancing Privacy and Security: The Privacy Implications of Goverment Data Mining Programs," Hearing Before the Committee on the Judiciary United States Senate 110. Congress (2007): 104-115.

Hondagneu-Messner, Sasha. "Data Portability: A Guide and a Roadmap." *Rutgers Computer Technology Law Journal* 47, no.2 (2021): 240-273.

Hoofnagle, Chris Jay, Ashkan Soltani, Nathan Good, Dietrich James Wambach, Mika D Ayenson. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law & Policy Review,* no.6 (2012): 273-296. https://ssrn.com/abstract=2137601 . Erişim Tarihi: 14 Temmuz 2022.

Horne, Ross, Sjouke Mauw. "Discovering Epassport Vulnerabilities Using Bisimilarity," *Logical Methods in Computer Science* 17, no.2 (2021): 24-52. https://lmcs.episciences.org/7537/pdf . Erişim Tarihi: 19 Eylül 2022.

Hou, Liyang. *Competition Law and Regulation of the EU Electronic Communications Sector A Comparative Legal Approach*. Alphen aan den Rijn: Wolters Kluwer Law and Business, Chapter 1, 2012. https://books.google.com.tr/books?id=uIqWDwAAQBAJ&pg=PT374&dq=Hou,+Liyang.+Competition+Law+and+Regulation+of+the+EU+Electronic+Communications+Sector+A+Comparative+Legal+Approach.&hl=tr&sa=X&ved=2ahUKEwiSx8GcwN37AhXDyaQKHTHYCPUQ6AF6BAgIEAI#v=onepage&q=Hou%2C%20Liyang.%20Competition%20Law%20and%20Regulation%20of%20the%20EU%20Electronic%20Communications%20Sector%20A%20Comparative%20Legal%20Approach.&f=false . Erişim Tarihi: 28 Şubat 2022.

IBM. "What is end-to-end encryption?." ibm.com. https://www.ibm.com/topics/end-to-end-encryption . Erişim Tarihi: 28 Ekim 2022.

InfoDev. *Telecommunications Regulation Handbook Module 3 Interconnection,* ed. Hank Intven. Washington: The World Bank, 2000.

Information Commissioner's Office (ICO). Guidance on the Use of Cookies and Similar Technologies, (2019): 40-41. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf . Erişim Tarihi: 24 Temmuz 2022.

Information Commissioner's Office (ICO). What do you mean by an 'information society service'? https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/ . Erişim Tarihi: 12 Temmuz 2022.

Information Commissioner's Office (ICO). Right to erasure, ico.org.uk. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ . Erişim Tarihi: 29 Ekim 2022.

Information Commissioner's Office (ICO). How should we obtain, record and manage consent?. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-

the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/ . Erişim Tarihi: 24 Mayıs 2022.

Information Commisioner's Office (ICO). Location Data. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/ . Erişim Tarihi: 2 Ekim 2022.

Information Commissioner's Office (ICO). Traffic Data. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/traffic-data/ . Erişim Tarihi: 26 Eylül 2022.

International Telecommunication Union (ITU). Calling Line Identification Restriction (CLIR). https://www.itu.int/rec/T-REC-I.251.4-199208-I/en . Erişim tarihi: 1 Eylül 2022.

International Telecommunication Union (ITU). *Collection of The Basic Texts Adopted By The Plenipotentiary Conference*. ITU Publication, 2019. https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-PLEN-2019-PDF-E.pdf . Erişim Tarihi: 27 Şubat 2022.

International Telecommunication Union (ITU). ITU E.800 Definitions of Terms Related to Quality Of Service. https://www.itu.int/rec/T-REC-E.800-200809-I/en . Erişim Tarihi: 10 Nisan 2022.

IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide*. (Cambridge, IT Governance Publishing, 2020). https://books.google.com.tr/books?id=LicDEAAAQBAJ&pg=PA384&dq=General+Data+Protection+Regulation+(GDPR)&hl=tr&sa=X&ved=2ahUKEwjrlsm6l5L7AhUzRPEDHTZRCW4Q6AF6BAgPEAI#v=onepage&q=General%20Data%20Protection%20Regulation%20(GDPR)&f=false . Erişim Tarihi: 20 Mayıs 2022.

It's Your Data-Take Control. https://ec.europa.eu/info/sites/default/files/data-protection-overview-citizens_en_0.pdf . Erişim Tarihi: 28 Ekim 2022.

Jain, Garima, Sanjeet Dahiya. "NFC: Advantages, Limits and Future Scope." *International Journal on Cybernetics& Informatics (IJCI)* 4, no.4 (2015):1-12. https://airccse.org/journal/ijci/papers/4415ijci01.pdf . Erişim Tarihi: 28 Ağustos 2022.

Jones, Meg Leta, Jenny Lee. "Comparing Consent to Cookies: A Case for Protecting Non-Use." *Cornell International Law Journal* 53, no.1 (2020): 97-132. https://community.lawschool.cornell.edu/wp-content/uploads/2021/03/Jones-Lee-final.pdf . Erişim Tarihi: 21 Ağustos 2022.

Kama Işık, Sezen. *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*. İstanbul: On İki Levha Yayıncılık, 2020.

Kamarinou, Dimitra, Christopher Millard, Jatinder Singh. "Machine Learning with Personal Data," ssrn.com. Queen Mary School of Law Legal Studies Research Paper No. 247/2016, 2016. https://ssrn.com/abstract=2865811 . Erişim Tarihi: 4 Kasım 2022.

Kaya, Mehmet Bedii. *Elektronik Ticaret Hukuku Ticari Elektronik İletiler*. İstanbul: On İki Levha Yayıncılık, 2020.

Kaya, Mehmet Bedii. *İnternet Hukuku*. İstanbul: On İki Levha Yayıncılık, 2021.

Kart Erişim Cihazı (KEC). https://bilgem.tubitak.gov.tr/tr/icerik/ekds-elektronik-kimlik-dogrulama-sistemi . Erişim Tarihi: 22 Eylül 2022.

Kayar, İsmail. *6102 sayılı Türk Ticaret Kanunu'na Göre Ticaret Hukuku*. (Ankara: Seçkin Yayıncılık, 2018.

Kayıhan, Şaban. *Ticari İşletme Hukuku*. Ankara: Seçkin Yayıncılık, 2018.

Kent, Bülent. *Türkiye'de İnternet Sitelerine Erişimin Engellenmesi.* Ankara: Adalet Yayınevi, 2019.

Kent, Bülent. "Telekomünikasyon Sektöründe Evrensel Hizmet Kavramı." *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 16, no.2 (2012): 169-198.

Kişisel Verileri Koruma Kurulu. 27.02.2020 tarih ve 2020/173 sayılı Amazon Turkey Perakende Hizmetleri Limited Şirketi Kararı. https://www.kvkk.gov.tr/Icerik/6739/2020-173 . Erişim Tarihi: 24 Mayıs 2022.

Kişisel Verileri Koruma Kurulu. 31.01.2018 tarih ve 2018/10 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/4110/2018-10 . Erişim Tarihi: 25 Eylül 2022.

Kişisel Verileri Koruma Kurulu. 27.08.2020 tarih ve 2020/649 sayılı Kararı. https://www.kvkk.gov.tr/Icerik/6815/2020-649 . Erişim Tarihi: 25 Eylül 2022.

Kişisel Verileri Koruma Kurulu. 01.10.2019 tarihli ve 2019/296 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/6557/2019-296 . Erişim Tarihi: 14 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 16.02.2021 tarih ve 2021/1262 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/7287/2021-1262 . Erişim Tarihi: 14 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 26/08/2021 tarihli ve 2021/859 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/7135/2021-859 . Erişim Tarihi: 25 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 21.04.2022 tarih ve 2022/388 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/7252/2022-388 . Erişim Tarihi: 28 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 23.06.2020 tarih ve 2020/481 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/6776/2020-481 . Erişim Tarihi: 30 Ekim 2022.

Kişisel Verileri Koruma Kurulu. Kişilerin Ad ve Soyadı ile Arama Motorları Üzerinden Yapılan Aramalarda Çıkan Sonuçların İndeksten Çıkarılmasına İlişkin Değerlendirmede Dikkate Alınacak Kriterler. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/68f1fb19-5803-4ef8-8696-f938fb49a9d5.pdf . Erişim Tarihi: 30 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 29.09.2020 tarih ve 2020/746 sayılı Kararı.https://www.kvkk.gov.tr/Icerik/6954/2020-746 . Erişim Tarihi: 11 Ekim 2022.

Kişisel Verileri Koruma Kurulu. 08.12.2020 tarih ve 2020/927 sayılı Karar.https://www.kvkk.gov.tr/Icerik/6871/2020-927 . Erişim Tarihi: 30 Ekim 2022.

Kişisel Verileri Koruma Kurumu. Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi. Nisan 2019. https://www.kvkk.gov.tr/Icerik/5394/Aydinlatma-Yukumlulugunun-Yerine-Getirilmesi-Rehberi . Erişim Tarihi: 18 Haziran 2022.

Kişisel Verileri Koruma Kurumu. Çerez Uygulamaları Hakkında Rehber. Haziran 2022. https://www.kvkk.gov.tr/Icerik/7353/Cerez-Uygulamalari-Hakkinda-Rehber Erişim Tarihi: 3 Temmuz 2022.

Kişisel Verileri Koruma Kurumu. Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler . Erişim Tarihi: 18 Haziran 2022.

Kişisel Verileri Koruma Kurumu. Sorularla VERBİS. https://verbis.kvkk.gov.tr/UploadedFiles/SORULARLA_VERB%C4%B0S.pdf . Erişim Tarihi: 20 Haziran 2022.

Kişisel Verileri Koruma Kurumu. "Açık Rıza Alırken Dikkat Edilecek Hususlar." https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar . Erişim Tarihi: 24 Mayıs 2022.

Kişisel Verileri Koruma Kurumu. Açık Rıza Rehberi. https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf . Erişim Tarihi: 22 Mayıs 2022.

Kişisel Verileri Koruma Kurumu. Kişisel Veri Güvenliği Rehberi, 2018. https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf . Erişim Tarihi: 28 Ekim 2022.

Kişisel Verileri Koruma Kurumu Tasarısı (1/541). https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf . Erişim Tarihi: 23 Mayıs 2022.

Klasson, Sebastian, Nina Lindström. "Longitudinal Analysis of the Certificate Validation Chains of Big Tech Company Domains." *Linköping University Department of Computer and Information Science Bachelor's Thesis*, 15 ECTS, (2021): i-vii ve 1-30. http://www.diva-portal.org/smash/get/diva2:1586424/FULLTEXT01.pdf . Erişim Tarihi: 22 Eylül 2022.

Koca, Güneş. "Mukayeseli Açıdan Telekomünikasyon Hukukunda Tüketicinin Korunması." Telekomünikasyon Kurumu Uzmanlık Tezi, Şubat 2005. https://www.btk.gov.tr/uploads/thesis/mukayeseli-acidan-telekomunikasyon-hukukunda-tuketicinin-korunmasi-duzenleyici-otoritelerin-rolu-alinmasi-gereken-tedbirler-olmasi-gereken-hukuk-acisindan-oneriler.PDF . Erişim Tarihi: 22 Mart 2022.

Koenig, Christian, Ernst Roder. "Regulation of Telecommunications in the EU a Challenge for the Countries Acceding to the European Community." *European Business Law Review* 10, no.7/8 (1999): 333-339.

Kosta, Eleni. *Consent in European Data Protection Law.* Leiden-Boston: Martinus Nijhoff Publishers, 2013.

Kulular İbrahim, Merve Ayşegül. *Modern Teknolojinin Hukuki Temelleri: Telgraf Örneği*. Ankara: Adalet Yayınevi, 2021.

Kuner, Christopher. *European Data Privacy Law and Online Business*. New York: Oxford University Press, 2003.

Kutluay, Ezgi. "Türk Borçlar Kanunu'nda Genel İşlem Koşulları." Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 19. no.3 (2017): 1369-1422.

Küçük, Adnan. "1982 Anayasası'ndaki Temel Hak ve Hürriyetlerin Sınırlanması Rejimi Bağlamında Kişisel Verilerin Korunması Hakkının Sınırlanmasının Anayasaya

Uygunluğu." İç. *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku*, editör Bayram Doğan. Ankara: Adalet Yayınevi, 2022: 11-74.

Küçük, Adnan. "Hukukun Hakim Kılınmasının Bir Gereği Olarak İdari Şeffaflık ve Bilgi Edinme Hürriyeti." *Liberal Düşünce Dergisi 22,* no.86 (2017): 69-95.

Küçük, Adnan. *Türkiye'de Başkanlık (Cumhurbaşkanlığı) Sistemi*. Ankara: Adalet Yayınevi, 2021.

Küzeci, Elif. *Kişisel Verilerin Korunması*. İstanbul: On İki Levha Yayıncılık, 2021.

Lambert, Paul. The Data Protection Officer Profession, Rules, and Role. Boca Raton: CRC Press - Taylor & Francis, 2017.

Lambert, Paul. *Understanding the New European Data Protection Rules*. Chapter 4, Need For Updating Data Protection. Boca Raton: CRC Press - Taylor & Francis, 2017. https://books.google.com.tr/books?id=QL42DwAAQBAJ&pg=PT3&dq=Lambert,+Paul.+Understanding+the+New+European+Data+Protection+Rules&hl=tr&sa=X&ved=2ahUKEwjiz8nuqa37AhX8_rsIHe0GAN4Q6AF6BAgHEAI#v=onepage&q=Lambert%2C%20Paul.%20Understanding%20the%20New%20European%20Data%20Protection%20Rules&f=false . Erişim Tarihi: 20 Mayıs 2022.

Liu, Yichuan, Hailey James, Otkrist Gupta, Dan Raviv. "MRZ Code Extraction from Visa and Passport Documents Using Convolutional Neural Networks." *International Journal on Document Analysis and Recognition (IJDAR)*, (2020):1-14. https://arxiv.org/pdf/2009.05489.pdf . Erişim Tarihi: 20 Eylül 2022.

Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.

Mackow, Witold, Jerzy Pejas. "Unauthorized Servers for Online Certificates Status Verification." Edited by Khalid Saeed, Jerzy Pejas, *Information Processing and Security Systems*. Newyork: Springer, 2005: 167-174.

Magee, John. "The Law Regulating Unsolicited Commercial E-Mail: An International Perspective," *Santa Clara High Technology Law Journal* 19, no.2 (2003): 333-382.

https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1322&context=chtlj . Erişim Tarihi: 30 Mayıs 2022.

Maietta, Angelo. "The Right to be Forgotten." Revista de Estudos Constitucionais Hermenêutica e Teoria do Direito (RECHTD), 12(2): 207-226, https://revistas.unisinos.br/index.php/RECHTD/article/view/rechtd.2020.122.03 Erişim Tarihi: 29 Ekim 2022.

Mayer-Schönberger, Viktor, Yann Padova. "Regime Change? Enabling Big Data Through Europe's New Data Protectıon Regulation," *The Columbia Science & Technology Law Review* 17, no.2 (2016): 315-335. https://journals.library.columbia.edu/index.php/stlr/article/view/4007/1769 . Erişim Tarihi: 17 Mayıs 2022.

Mena, Jesus. Data Mining Your Website. Boston: Digital Press Butterworth-Heinemann, 1999.

Messerschmitt, David G. "Telecommunications in the 21st Century." University of California (1996): 1. http://people.eecs.berkeley.edu/~messer/PAPERS/93/Japan1/Japan1.pdf . Erişim Tarihi: 27 Şubat 2022.

Misek, Jakub. "Consent to Personal Data Processing the Panacea or the Dead End?." *Masaryk University Journal of Law and Technology* 8, no.1 (2014): 69-83.

Mobildev. "SMS aktivasyon için gerekli evraklar nelerdir? Turkcell - Vodafone Ek evraklar." https://www.mobildev.com/support-knowledge-detail.asp?sid=66&id=1&sssid=41 . Erişim Tarihi: 3 Eylül 2022.

Nalbantoğlu, Seray. "Bir Temel Hak Olarak Unutulma Hakkı." *Türkiye Adalet Akademisi Dergisi* 9, no.15 (2018): 583-605.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Aydınlatma Metni - Kişisel Verilerinizin Aktarıldığı Taraflar ve Aktarım Amaçları. https://www.netgsm.com.tr/gizlilik-ve-guvenlik/ . Erişim Tarihi: 25 Haziran 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Başvuru Formu. https://www.netgsm.com.tr/belgeler/formlar/netgsm-ilgili-kisi-basvuru-formu.pdf Erişim Tarihi: 11 Ekim 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Bireysel Sabit Telefon Hizmetleri Abonelik Sözleşmesi. https://www.netgsm.com.tr/abonelik/sozlesme/bireyselabonelik.php . Erişim Tarihi: 25 Ağustos 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Kurumsal Sabit Telefon Hizmeti Abonelik Sözleşmesi. https://www.netgsm.com.tr/abonelik/sozlesme/kurumsalabonelik.php . Erişim Tarihi: 7 Mart 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Netgsm Aboneliği İçin Gerekli Belgeler Nelerdir?. https://bilgibankasi.netgsm.com.tr/bilgi-bankasi/netgsm-aboneligi-icin-gerekli-belgeler-nelerdir/ . Erişim Tarihi: 5 Eylül 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Ön Kayıt. https://www.netgsm.com.tr/on-kayit . Erişim Tarihi 23 Ağustos 2022.

Netgsm İletişim ve Bilgi Teknolojileri A.Ş. Yetkili Değişikliği Formu. https://www.netgsm.com.tr/belgeler/formlar/netgsm-yetkili-degisikligi-formu.pdf . Erişim Tarihi: 8 Ekim 2022.

Loideain, Nora Ni. "The EC Data Retention Directive: Legal Implications for Privacy and Data Protection," iç. *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, Christina Akrivopoulou, Athanasios- Efstratios Psygkas. New York: Information Science Reference, 2011.

OneTrust LLC. "The Ultimate Cookie Handbook For Privacy Professionals." onetrust.com. Kasım 2020. https://www.dataguidance.com/sites/default/files/20201228-onetrust-cookieconsent-handbook-digital.pdf . Erişim Tarihi: 10 Temmuz 2022.

Organisation for Economic Co-Operation and Development (OECD) Rehber İlkeler, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . Erişim Tarihi: 15 Mayıs 2022.

Oriyano, Sean-Philip. *Penetration Testing*. Indianapolis: Sybex, 2017.

Orji, Uchenna Jerome. *International Telecommunications Law and Policy*. Newcastle upon Tyne: Cambridge Scholars Publishing, 2018).

Orta, Mesut. *Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)*. Ankara: Yetkin Yayınları, 2015.

Öktem Çevik, Seda. *Mobil Telefon Abonelik Sözleşmesi*. İstanbul: Beta Basım Yayım, 2008.

Özkaya, Ayşe. *Elektronik Haberleşme Sektöründe Tüketicinin Korunması Açısından Abonelik Sözleşmelerinin İncelenmesi*. 2011. BTK Bilişim Uzmanlığı Tezi. https://www.btk.gov.tr/uploads/thesis/elektronik-haberlesme-sektorunde-tuketicinin-korunmasi-acisindan-abonelik-sozlesmelerinin-incelenmesi.PDF . 6 Mart 2022.

Öztekin, Alp. *Teori ve Uygulamada Türk İnternet Hukuku*. Ankara: Seçkin Yayıncılık, 2021.

Öztürk, Bahri, Elif Altınok Çalışkan. "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu." *Fasikül Hukuk Dergisi* 10, no.100 (2018): 277-336.

Öztürk, Burak. "Elektronik Haberleşme Hizmetlerinde Yetkilendirmenin Hukuki Niteliği." *Ankara Barosu Dergisi*, no.1 (2009): 26-42.

Pantelic, Ognjen, Kristina Jovic, Stefan Krstovic. "Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations." *Sustainability* 14, no. 9 (2022): 1-14. https://doi.org/10.3390/su14095015 . Erişim Tarihi: 5 Temmuz 2022.

Papakonstantinou, Vagelis, Paul De Hert. "Big Data Analytics in Electronic Communications: A Reality in Need of Granular Regulation (Even if This Includes An Interim Period of No Regulation at All)." *Cyber and Data Security Lab Working Paper*, no.1 (2019): 1-28. http://dx.doi.org/10.2139/ssrn.3535701. Erişim Tarihi: 15 Mayıs 2022.

Papakonstantinou, Vagelis, Paul De Hert. "The Amended EU Law on ePrivacy and Electronic Communications After Its 2011 Implementation: New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights." *Journal of Computer Information Law* 29, no.1 (2011): 29-74. https://repository.law.uic.edu/jitpl/vol29/iss1/2/ . Erişim Tarihi: 17 Temmuz 2022.

Pennington, Brian. "New Technology Briefing: Cookies-Are They a Tool for Web Marketers or a Breach of Privacy?." *Interactive Marketing* 2, no.3 (2001): 251-255.

Pierson, Jo, Rob Heyman. "Social Media and Cookies: Challenges for Online Privacy." *Info* 13, no.6 (2011): 30-42. https://www.emerald.com/insight/content/doi/10.1108/14636691111174243/full/html . Erişim Tarihi: 7 Temmuz 2022.

Podkowik, Jan, Robert Rybski, Marek Zubik. "Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?" *International Journal of Constitutional Law* 19, no.5 (2021): 1597–1631, https://academic.oup.com/icon/article/19/5/1597/6498025 , Erişim Tarihi: 18 Ekim 2022.

Polater, Salih. "Kişisel Verilerin Reklam Amaçlı İşlenmesinde Hukuka Uygunluk Sebepleri." *Kişisel Verilerin Korunması Dergisi* 1, no.1 (2019): 1-20.

Pope, Nick. "Protecting Long Term Validity of PDF Documents with PAdES-LTV," (Eds)Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider, ISSE 2009 Securing Electronic Business Processes, Mörlenbach:Vieweg+Teubner, (2010): 320-327.

Rekabetçi Telekomünikasyon İşletmecileri Derneği (TELEKOMDER). "Ortak Abone Kayıt Deseni'ne Geçiş Nasıl Olmalı?." https://www.telekomder.org/ortak-abone-kayit-desenine-gecis-nasil-olmali/ . Erişim Tarihi: 25 Eylül 2022.

Roussos, George. *Networked RFID: Systems, Software and Services*. London: Springer, 2008.

Rubinstein, Ira S., Ronald D. Lee, Paul M. Schwartz. "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches." The University of Chicago Law Review 75, (2008): 261-285. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5656&context=uclrev . Erişim Tarihi: 6 Kasım 2022.

Saka, Rıza, Ramazan Çağlayan, Mahmut Koca. *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası.* Ankara: Seçkin Yayıncılık, 2020.

Sanal Ortamda İşlenen Suçlar Sözleşmesi. https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf . Erişim Tarihi: 28 Ekim 2022.

Sancakdar, Oğuz, Lale Burcu Önüt, Eser Us Doğan, Mine Kasapoğlu Turhan, Serkan Seyhan. *İdare Hukuku Teorik Çalışma Kitabı*. Ankara: Seçkin Yayıncılık, 2021.

Selek, Ozan. "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 21, no.2 (2019): 911-951.

Serbest Telekomünikasyon İşletmecileri Derneği (TELKODER). "Abone Deseni Yükümlülüğüne İlişkin Tespit ve Öneriler." https://telkoder.org.tr/wp-content/uploads/2020/06/20-028.pdf . Erişim Tarihi: 25 Eylül 2022.

Serbest Telekomünikasyon İşletmecileri Derneği (TELKODER). Danıştay 13. Dairesi 2019/2412 E. Sayılı davada, yürütmenin durdurulması isteminin reddedildiğine ilişkin yayınlanan karar. https://telkoder.org.tr/wp-content/uploads/2022/04/Dan%C4%B1%C5%9Ftay-13.-D.-2017-968-

Y%C3%BCr%C3%BCtmenin-Durdurulmas%C4%B1-Red-Karar%C4%B1.pdf . Erişim Tarihi: 25 Eylül 2022.

Searchinform. "Information Security Levels." searchinform.com. https://searchinform.com/challenges/information-security/information-security-basics/key-aspects-of-information-security/the-basic-principles-of-information-security/information-security-levels/ . Erişim Tarihi: 14 Eylül 2022.

Sezginer, Murat. "İdarenin Müdahale Ettiği Özel Hukuk Sözleşmeleri (Bileşik İradeli "Birleşme" Sözleşmeler)." *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 17, no.1-2 (2013): 1589-1621.

Sharma Vibhor, Preeti Gusain, Prashant Kumar. "Near Field Communication." *Proceedings of the Conference on Advances in Communication and Control Systems (CAC2S 2013)*, (Atlantis Press, 2013): 342-345. https://www.atlantis-press.com/proceedings/cac2s-13/6331 . Erişim Tarihi: 19 Eylül 2022.

Sidak, J. Gregory. "Does The Telephone Consumer Protection Act Violate Due Process As Applied?." *Florida Law Review* 68, (2016): 1403-1412.

Simbase Telecommunication. MSISDN- (Mobile Station Integrated Services Digital Network), https://www.simbase.com/iot-glossary-dictionary/msisdn . Erişim Tarihi: 26 Ağustos 2022.

Solove, Daniel J. "Introduction: Privacy Self-Management and The Consent Dilemma." *Harvard Law Review* 126, (2013): 1880-1903.

Soltani, Ashkan, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle. "Flash Cookies and Privacy." ssrn.com, (2009): 1-8. http://dx.doi.org/10.2139/ssrn.1446862 . Erişim Tarihi: 12 Temmuz 2022.

Söyler, Yasin. *Yeni Başkanlık Sisteminde Cumhurbaşkanlığı Kararnamesi*. Ankara: Seçkin Yayıncılık, 2018.

Söyler, Yasin. *Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi*. Ankara: Savaş Yayınevi, 2014.

Spagnuelo, Dayana, Ana Ferreira, Gabriele Lenzini. "Transparency Enhancing Tools and the GDPR: Do They Match?." İç. *Information Systems Security and Privacy ICISSP 2019*, editörler Paolo Mori, Steven Furnell, Olivier Camp, Communications in Computer and Information Science 1221, Prague: Springer Cham, 2020: 162-185. https://doi.org/10.1007/978-3-030-49443-8_8 . Erişim Tarihi: 15 Haziran 2022.

Surveillance Self-Defense. "Cep Telefonları: Konum Takibi." Son Güncelleme: 4 Mayıs 2021. https://ssd.eff.org/tr, https://ssd.eff.org/tr/module/cep-telefonlar%C4%B1-konum-takibi . Erişim Tarihi: 23 Ağustos 2022.

Tan, Turgut. "Kamu Hizmeti İmtiyazından Yap-İşlet-Devret Modeline." *Ankara Üniversitesi SBF Dergisi* 47, no.3 (1992): 307-325.

Telefonica. 2021 yılına ait Şeffaflık Raporu. https://www.telefonica.com/en/wp-content/uploads/sites/5/2021/08/Report-on-Transparency-in-Communications-2021.pdf . Erişim Tarihi: 24 Mart 2022.

Telestream. What Does OTT Really Mean? https://www.telestream.net/video/solutions/what-is-ott.htm . Erişim Tarihi: 1 Ağustos 2022.

TS 13678. Elektronik Kimlik Doğrulama Sistemi Standartı. https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?081118051115108051104119110104055047105102120088111043113104073086073081073066071066080088098075. Erişim Tarihi: 21 Eylül 2022.

Tsai, Janice Y., Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh. "Location-Sharing Technologies: Privacy Risks and Controls." TPRC 2009, (2010): 1-26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1997782 . Erişim Tarihi: 24 Ağustos 2022.

TT Mobil İletişim Hizmetleri A.Ş. TT Mobil Mobil Telefon Hizmetleri Bireysel Tip Abonelik Sözleşmesi. https://www.turktelekom.com.tr/tt-yardim/Documents/TT-mobil-bireysel-abonelik-sozlesmesi.pdf . Erişim Tarihi: 1 Eylül 2022.

TT Mobil İletişim Hizmetleri A.Ş. Referans Arabağlantı Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/tt-mobil-rat-08-06-2021.pdf . Erişim Tarihi: 3 Nisan 2022.

TT Mobil İletişim Hizmetleri A.Ş. Yeni Mobil Hat Başvuru İşlemleri, https://www.turkiye.gov.tr/ttmobil-yeni-mobil-hat-basvuru-islemleri . Erişim Tarihi: 14 Eylül 2022.

TTNet A.Ş. İnternet Ek Hizmet Talep/Değişiklik Formu, https://bireysel.turktelekom.com.tr/evde-internet/web/destek/internet/SozlesmeVeTaahhutnameler/INTERNET_EKHiZMET.pdf . Erişim Tarihi: 8 Ekim 2022.

Turkcell İletişim Hizmetleri A.Ş. Abonelik Başvurusu Aydınlatma Metni, https://www.turkcell.com.tr/tr/turkcell-abonelik-basvurusu-aydinlatma-metni . 29 Ağustos 2022.

Turkcell İletişim Hizmetleri A.Ş. Abonelik İşlemleri, https://www.turkcell.com.tr/yardim/hattiniz/abonelik-islemleri/fatura-alternatifleri-nelerdir . Erişim Tarihi: 25 Ağustos 2022.

Turkcell İletişim Hizmetleri A.Ş. Hat Almak İçin Gerekli Fatura Alternatifleri Nelerdir?. https://www.turkcell.com.tr/yardim/kampanya/kampanyalar-faturali/fatura-alternatifleri-nelerdir . Erişim Tarihi: 3 Eylül 2022.

Turkcell İletişim Hizmetleri A.Ş. Nasıl Faturalı Hat Alabilirim?. https://m.turkcell.com.tr/yardim/turkcellli-olmak/turkcellli-olmak/nasil-faturali-hat-alabilirim . Erişim Tarihi: 3 Eylül 2022.

Turkcell İletişim Hizmetleri A.Ş. Aydınlatma Metni - Kişisel Verileriniz Nelerdir? https://www.turkcell.com.tr/tr/gizlilik-ve-guvenlik?page=kisisel-verilerin-korunmasi . Erişim Tarihi: 29 Ağustos 2022.

Turkcell İletişim Hizmetleri A.Ş. Aydınlatma Metni – Kişisel Verilerin Aktarılması. https://www.turkcell.com.tr/tr/gizlilik-ve-guvenlik?page=kisisel-verilerin-korunmasi . Erişim Tarihi: 25 Haziran 2022.

Turkcell İletişim Hizmetleri A.Ş. Referans Arabağlantı Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/turkcell-rat-08-06-2021.pdf . Erişim Tarihi: 3 Nisan 2022.

Turkcell İletişim Hizmetleri A.Ş. Ön Başvuru Formu, https://www.turkcell.com.tr/tr/form/gnc-numara-tasima-on-basvuru-formu . Erişim Tarihi: 23 Ağustos 2022.

Turkcell İletişim Hizmetleri A.Ş. Yaşım 18'den Küçük, Nasıl Hat Alabilirim? https://www.turkcell.com.tr/yardim/turkcellli-olmak/turkcellli-olmak/yasim-18den-kucuk-nasil-hat-alabilirim#:~:text=Turkcell%27li%20Olmak&text=Yeni%20hat%20al%C4%B1rken%20gereken%20t%C3%BCm,anne%20veya%20baban%C4%B1z%C4%B1n%20kimli%C4%9Fi%20gerekmektedir. Erişim Tarihi: 3 Eylül 2022.

Turkcell İletişim Hizmetleri A.Ş. "Hedefli Mesaj," https://www.turkcell.com.tr/kurumsal/dijital-is-servisleri/diger-kurumsal-cozumler/hedefli-mesaj , Erişim Tarihi: 8 Kasım 2022.

Turkcell İletişim Hizmetleri A.Ş. "Güvenli Dijital İmza Nedir ve Neden Güvenlidir?," https://www.turkcell.com.tr/yardim/hattiniz/abonelik-islemleri/guvenli-dijital-imza-nedir-ve-neden-guvenlidir . Erişim Tarihi: 25 Eylül 2022.

Turkcell İletişim Hizmetleri A.Ş. "Nasıl Kurumsal Hat Alabilirim?", https://m.turkcell.com.tr/kurumsal/yardim/turkcelli-olmak/abonelik-islemleri/nasil-kurumsal-hat-alabilirim . Erişim Tarihi: 3 Eylül 2022.

Turkcell İletişim Hizmetleri A.Ş. https://hizligiris.com.tr/hizligiris/generic/sms_otp . Erişim Tarihi: 14 Ekim 2022.

Turknet İletişim Hizmetleri A.Ş. Başvuru Formu. https://turk.net/taahhutsuz-ozgur-iletisim-abonelik . Erişim Tarihi 23 Ağustos 2022.

Türk Telekomünikasyon A.Ş. Aydınlatma Metni - Kişisel Verilerin Aktarılması. https://bireysel.turktelekom.com.tr/mobil/sayfalar/gizlilik-ve-guvenlik.aspx . Erişim Tarihi: 25 Haziran 2022.

Türk Telekomünikasyon A.Ş. Referans Arabağlantı Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/turk-telekom-rat-22-02-2022.pdf . Erişim Tarihi: 3 Nisan 2022.

Türk Telekomünikasyon A.Ş. Referans Ortak Yerleşim ve Tesis Paylaşımı Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/roytept-27-04-2014-tarihli-kk-geregi-05-05-2016.pdf . Erişim Tarihi: 3 Nisan 2022.

Türk Telekomünikasyon A.Ş. Referans Al-Sat Yöntemiyle ATM/FR/ME İnternet Toptan Satış Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/rafmet-22-02-2022-53.pdf . Erişim Tarihi: 3 Nisan 2022.

Türk Telekomünikasyon A.Ş. Sesli Abonelik Sözleşmesi, https://www.turktelekom.com.tr/yardim/bireysel-mobil/abonelik-sozlesmeleri , Erişim Tarihi: 3 Eylül 2022.

Türk Telekomünikasyon A.Ş. Engellilere Özel Hizmetler, https://www.turktelekom.com.tr/destek/engellilere-ozel-hizmetler . Erişim Tarihi: 22 Mart 2022.

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf . Erişim Tarihi: 11 Ekim 2022.

Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş. "E-devlet'te Abonelik Sözleşme Sürecini İşleten İlk Telekom Operatörü Türksat Kablo Oldu," https://www.turksat.com.tr/tr/haberler/e-devlette-abonelik-sozlesme-surecini-isleten-ilk-telekom-operatoru-turksat-kablo-oldu . Erişim Tarihi: 10 Eylül 2022.

Tyson, Jeff. "How Virtual Private Networks Work." communicat.com.au. https://www.communicat.com.au/wp-content/uploads/2013/04/how_vpn_work.pdf . Erişim Tarihi: 23 Ağustos 2022.

Ulusoy, Ali. *Yeni Türk İdare Hukuku*. Ankara: Yetkin Yayınları, 2019.

Ulusoy, Ali. "Telekomünikasyon Alanındaki Son Yasal Düzenlemeler ve Uygulamaların Değerlendirilmesi." Rekabet Kurumu Perşembe Konferansları. 57-92. https://www.rekabet.gov.tr/Dosya/persembe-konferanslari-yayinlari/perskonfyyn46.pdf . Erişim Tarihi: 1 Mart 2022.

Ulusoy, Ali. *Telekomünikasyon Hukuku*. Ankara: Turhan Kitabevi, 2002.

van Tilborg, Henk C.A., Sushil Jajodia. *Encyclopedia of Cryptography and Security*. New York: Springer, 2011.

Vedaschi, Arianna, Valerio Lubello. "Data Retention and Its Implications for the Fundamental Right to Privacy A European Perspective." *Tilburg Law Review* 20, (2015): 14-34. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2589524 . Erişim Tarihi: 26 Ekim 2022.

Vermaat, Misty E., Susan L. Sebok, Steven M. Freund, Jennifer T. Campbell, Mark Frydenberg, Discovering Computers 2018 Digital Technology, Data, and Devices-Module 2, Boston: Cengage Learning, 2018.

Vodafone Net İletişim Hizmetleri A.Ş. Hizmetlerden Yararlanmak İçin Gerekli Evraklar, https://www.vodafone.com.tr/yardim/hizmetlerden-yararlanmak-icin-gerekli-evraklar-nelerdir-330 . Erişim Tarihi: 25 Ağustos 2022.

Vodafone Telekomünikasyon A.Ş. Aydınlatma Metni – Kişisel Verilerin Aktarıldığı Alıcı Grupları. https://www.vodafone.com.tr/VodafoneHakkinda/gizlilik-ve-guvenlik-politikalari . Erişim Tarihi: 25 Haziran 2022.

Vodafone Telekomünikasyon A.Ş. Referans Arabağlantı Teklifi, https://www.btk.gov.tr/uploads/pages/referans-erisim-ve-arabaglanti-teklifleri/vodafone-rat-08-06-2021.pdf . Erişim Tarihi: 3 Nisan 2022.

Waller, Spencer Weber, Daniel B. Heidtke, Jessica Stewart. "The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology." *Loyola Consumer Law Review* 26, (2014): 343-425.

Whalen, David. “The Unofficial Cookie FAQ Versiyon 2.6.” cookiecentral.com, Son Güncelleme: 8 Haziran 2002, http://www.cookiecentral.com/faq/ . Erişim Tarihi: 4 Temmuz 2022.

Yergin, Rebecca I. “Consent in The Age of Facebook: Applying The Telephone Consumer Protection Act to Text Messages from Social Media Platforms.” *Columbia Law Review Online* 116, (2016): 81-92.

Yıldırım, Turan, Muhammed Göçgün, “İdarenin Düzenleyici İşlemlerinde Eşitlik İlkesi.” *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 3, no.2 (2016): 39-60.

Yıldız, Mustafa Göktürk. *Son Kullanıcıyla Akdedilen Elektronik Haberleşme Sözleşmesi*. On İki Levha Yayınları: İstanbul, 2012.

Yılmaz, Süleyman, Gökçe Filiz Çavuşoğlu. *Kişisel Verileri Koruma Hukuku.* Ankara: Yetkin Yayınları, 2020.

Yücer Aktürk, İpek. “Tüzel Kişi Tacirin Tüketici Sıfatı.” *Gazi Üniversitesi Hukuk Fakültesi Dergisi* 20, no.2 (2016): 103-128.

Yüksel, Aytaç. Elektronik Haberleşme Hukukundaki İdari Yaptırımlar ve Yargısal Denetimi. Ankara: Adalet Yayınevi, 2018.