T.C

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAMU HİZMETİ YÖNÜYLE AKILLI ŞEHİRLERDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

YÜKSEK LİSANS TEZİ

ORHAN KOCABIYIK

2100006172

Anabilim Dalı: Kamu Hukuku

Programı: İnsan Hakları

Tez Danışmanı: Dr. Öğr. Üyesi Elif ALTINOK ÇALIŞKAN

Temmuz 2023

T.C

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAMU HİZMETİ YÖNÜYLE AKILLI ŞEHİRLERDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

YÜKSEK LİSANS TEZİ

ORHAN KOCABIYIK

2100006172

Anabilim Dalı: Kamu Hukuku

Programı: İnsan Hakları

Tez Danışmanı: Dr. Öğr. Üyesi Elif ALTINOK ÇALIŞKAN
Jüri Üyeleri: Prof. Dr. Nilay ARAT
Doç. Dr. Mustafa Aytaç ÖZELÇİ

Temmuz 2023

İÇİNDEKİLER

İKİNCİ BÖLÜM

KAMU HİZMETİ YÖNÜYLE AKILLI ŞEHİRLERDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

KISALTMALAR

108 sayılı sözleşme	: 28/01/1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AoT	: Array of Things
AYM	: Anayasa Mahkemesi
B.No	: Başvuru Numarası
Bkz	: Bakınız
BİT	: Bilgi ve İletişim Teknolojileri
BM	: Birleşmiş Milletler
Bs.	: Baskı
C	: Cilt
CDEP	: Committee on Digital Economy Policy
CGK	: Ceza Genel Kurulu
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
DARPA	: The Defense Advanced Research Projects Agency
DGP	: Data Governance and Privacy
E.	: Esas Numarası
GDPR	: General Data Protection Regulation
GPS	: Global Positioning System
IoT	: Internet of Things

İBB	: İstanbul Büyükşehir Belediyesi
K.	: Karar Numarası
K.T.	: Karar Tarihi
Kurul	: Kişisel Verileri Koruma Kurulu
Kurum	: Kişisel Verileri Koruma Kurumu
KVKK	:6698 sayılı Kişisel Verilerin Koruması Kanunu
m.	: Madde
M.Ö.	: Milattan Önce
OECD	: Organisation for Economic Co-operation and Development
OEEC	: Organisation for European Economic Cooperation
S.	: Sayı
s.	: Sayfa
SCADA	: Supervisory Control and Data Acquisition
TBMM	: Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TCK	: 5237 sayılı Türk Ceza Kanunu
TMK	: 4721 sayılı Türk Medeni Kanunu
vd.	: Ve devamı

ÖZET

Artan şehirleşme oranı ile, trafik, gürültü, çevre kirliliği, su ve enerji kaynaklarının yetersizliği, konut yetersizliği gibi şehirlerin sorunları da artmaktadır. Bu sorunların karşısında akıllı şehirler, modern yaşamın gerektirdiği teknolojik ve sürdürülebilir çözümleri entegre ederek daha verimli, güvenli, sürdürülebilir ve yaşanabilir şehirler yaratmayı amaçlamaktadır. Akıllı şehirlerin itici gücü veridir. Şehrin her tarafını saran teknolojik altyapı ile şehir sakinlerinden kişisel verileri toplanmakta, bu veriler özellikle karar verme süreçlerinde, hizmet kalitesini artırmada, kaynakların etkin kullanılmasında, güvenlik ve afet yönetiminde kullanılmaktadır. Ancak bu durum insanlar için birtakım riskler de barındırmaktadır.

İnsanlar için tehdit oluşturabilecek ilk durum, akıllı şehirlerin bir gözetim toplumuna dönüşmesidir. Çünkü günün her saati izlenmek, her hareketinin kaydedilmesi, en mahrem bilgilerin bile idare veya özel şirketler tarafından öğrenilmiş olması, kişinin onurlu bir hayat yaşamasına engel olabilecektir. İkinci durum ise, toplanan kişisel verilerin siber saldırılarla ele geçirilmesi veya hukuka aykırı olarak bir başkasına verilme ihtimalidir. Bu ihtimalde, kişiye özel olan veriler yetkisiz 3. kişiler tarafından ele geçirilmiş olacaktır. Bu nedenle akıllı şehirlerde kişisel verilerin korunması bir zorunluluktur. Kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkı kapsamında gelişen ve günümüzde neredeyse bağımsız bir hak olarak anılan bir kişilik hakkıdır. Akıllı şehirlerde bu hakkın fonksiyonu, veri toplayarak elde edilmeye çalışılan kamu menfaati ile kişinin mahremiyetinin korunması arasında denge noktasını bulmaktır.

Çalışmada önce akıllı şehir kavramı ele alınmış, bu kavramın kamu hizmeti anlayışına etkisi açıklanmış ve daha sonra da akıllı şehirlerde verilerin korunması için uygulanacak hukuki düzenlemeler incelenmiştir.

Anahtar Kelimeler: Akıllı şehir, bilgi ve iletişim teknolojileri, kamu hizmeti, kişisel veri, kişisel verilerin korunması hakkı, gözetim toplumu, özel hayat.

ABSTRACT

With the increasing rate of urbanization, cities are facing challenges such as traffic congestion, noise pollution, environmental degradation, inadequate water and energy resources, and housing shortages. In response to these problems, smart cities aim to integrate technological and sustainable solutions that are essential for modern living, creating more efficient, safe, sustainable, and livable urban environments. The driving force behind smart cities is data. Through a pervasive technological infrastructure covering all aspects of the city, personal data is collected from city residents. This data is utilized in decision-making processes, improving service quality, optimizing resource utilization, and enhancing security and disaster management. However, this situation also poses certain risks for individuals.

The first threat that poses a risk to individuals is the transformation of smart cities into surveillance societies. Being constantly monitored, having every move recorded, and even the most private information being known by authorities or private companies hinder individuals from leading a dignified life. The second threat is the possibility of collected personal data being obtained through cyber attacks or being shared with others unlawfully. In such a scenario, data that is meant to be private to an individual can be compromised by unauthorized individuals. Therefore, the protection of personal data is imperative in smart cities. The right to the protection of personal data is an evolving aspect within the scope of the right to privacy, which is now recognized as an independent right. In smart cities, the function of this right is to find a balance between the public interest pursued through data collection and the preservation of an individual's privacy.

The study initially focuses on the concept of smart cities, explaining its impact on the understanding of public services. Subsequently, it examines the legal regulations that will be implemented to protect data in smart cities.

Keywords: Smart city, information and communication technologies, public service, personal data, right to the protection of personal data, surveillance society, privacy

GİRİŞ

Teknolojik gelişmeler hayatımızın her alanını etkilemektedir. Akıllı telefon, akıllı klima, akıllı buzdolabı, akıllı televizyon, akıllı saat, akıllı bina gibi gittikçe gelişen çağımız teknolojileri hayatımızın her alanına nüfuz etmektedir. Öyle ki bu gelişmelerin en önemlilerinden biri olarak "*akıllı şehir*" kavramı ortaya çıkmıştır.

Birleşmiş Milletler'in 2014 tarihli "*Dünya Kentleşme Beklentileri*" raporuna göre 2050 yılında kentlerde yaşayacak insan nüfusunun, dünya nüfusunun %70'i olması beklenmektedir. Şehirleşme sosyal ve ekonomik sınıf farklılıklarını, sağlık sorunlarını, altyapı ve kaynak sorunlarını beraberinde getirecek ve kentlerin kalitesi müdahale edilmezse düşecektir. Teknolojik alanda yaşanan gelişmeler, kentleşmenin sebep olduğu sorunların önüne geçmek için düşünülen çözüm önerilerine de yeni bir boyut kazandırmıştır. Şehirleşmenin yol açtığı olumsuz sonuçları en aza indirmek ve hayat kalitesini en yüksek seviyede tutmak için geliştirilen, 1990 sonrası ortaya çıkan ve tek açıdan konuyu alan bu yaklaşımların yanında konuyu daha kapsayıcı ele alan, bilgi teknolojileri temelli ve birçok yönden de sürdürülebilir hedefler belirleyen bir yaklaşım doğmuştur. Bu yaklaşım "*akıllı şehir*" kavramıdır.

Akıllı şehirler, atık yönetimi, evler, binalar, trafik sistemleri, ulaşım sistemleri, su şebekeleri, suç tespit sistemleri, hastaneler, okullar ve kütüphaneler gibi şehrin tamamını kapsayan kamu hizmetlerini izlemek ve yönetmek için, elektronik nesnelerin sensör denilen algılayıcıları yardımıyla verileri toplayan ve toplanan verilerden çıkarmış olduğu bilgileri kullanan şehirlerdir.

Prof. Boyd Cohen'in "*akıllı şehir çarkı*" metodolojisine göre akıllı şehrin altı boyutu vardır. Bunlar akıllı ekonomi, akıllı çevre, akıllı toplum, akıllı hareketlilik, akıllı yaşam ve akıllı yönetişimdir. Akıllı insan uygulamaları, odak noktasında sosyal sermayenin ana unsuru olan insanın bulunduğu unsurlardır. Akıllı yönetişim uygulamaları, şehir sakinlerinin karar alma sürecine katılmaları için görüş ve tavsiyelerini dile getirebildiği, bu görüş ve tavsiyelerin karar alıcılar tarafından da görülebildiği bir diğer ifadeyle şehir yönetiminin şeffaflık ilkesi gereğince yönetim verilerinin halka açıldığı platformlardır. Akıllı sağlık uygulamaları, bilgi ve iletişim

teknolojileri yardımıyla sağlık verilerinin analiz edilmesini sağlayan, sağlık hizmetlerinin etkili ve hızlı bir şekilde yerine getirilmesini amaçlayan uygulamalardır. Akıllı enerji uygulamaları, enerji kaynaklarının daha verimli kullanılması, enerjinin maliyet ve tüketim açısından tasarrufu, enerjinin kesintisiz ve kaliteli bir şekilde tedarik edilmesi ve çevresel etkilere karşı hassasiyet gösterilmesi gibi konuları amaçlayan yenilikçi teknolojileri ifade etmektedir. Akıllı güvenlik uygulamaları, veri analizi ile şehir güvenliğinin ölçümlenmesi ve etkinliğinin artırılması için tasarlanan, teknolojik altyapı ile kameralar, sensörler, akıllı cihazlar ve diğer teknolojik araçlarla donatılmış bir sistemdir. Akıllı çevre uygulamaları, bilgi ve iletişim teknolojileri (BİT) kullanımı ile çevrenin yönetilmesi ve sürdürülebilirliğinin sağlanmasını amaçlayan, bu kapsamda çevre ile ilgili verilerin toplanması, izlenmesi, analiz edilmesi ve bu verilere dayalı kararlar alınması hedefleyen uygulamalardır.

Akıllı şehirlerde kullanılan araçlar, büyük veri, açık veri, bulut bilişim, nesnelerin interneti ve yapay zekadır. Akıllı şehir araçlarının temelinde veri bulunmaktadır. Akıllı şehir yönetim süreci, verinin toplanması, depolanması, analiz edilmesi ve sonuç çıkarılması sürecidir. Bu süreçte kişisel verilerin hukuka aykırı olarak elde edilme, ifşa edilme, üçüncü kişilere aktarılma veya çalınma riskleri bulunmaktadır. Böylesi bir durumda ilgili kişilerin özel hayatının gizliliği ihlal edilmiş olacaktır.

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olan kişisel verinin korunması bilgisayar teknolojilerinin gelişmesiyle beraber 1960'lı yıllarda gündeme gelmiştir. İnsan Hakları Evrensel Beyannamesi'nde ve Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunması hakkı bağımsız bir hak olarak düzenlenmemiştir ancak özel hayatın gizliliği hakkı kapsamında koruma altına alınmıştır. Kişisel verileri korumayı amaçlayan ilk uluslararası belge OECD tarafından hazırlanmış olup, 23/09/1980 tarihinde kabul edilen Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri olmuştur. Uluslararası düzeyde ilk bağlayıcı olan belge ise Avrupa Konseyi tarafından hazırlanan 28/01/1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi olmuştur.

1982 Anayasası'nda 2010 yılında yapılan değişiklik ile kişisel verilerin korunması hakkı bağımsız olarak tanınmıştır. Avrupa Birliği ülkelerinde Avrupa Birliği Genel Veri Koruma Tüzüğü 2018 yılında yürürlüğe girmiştir. Ülkemizde ise 6698 sayılı Kişisel Verilerin Koruması Kanunu 2016 yılında yürürlüğe girmiştir.

Çalışmamızın ilk bölümünde akıllı şehir kavramının nasıl ortaya çıktığı, ne anlama geldiği, bileşenleri ve kullanılan teknolojik araçlar detaylı bir şekilde anlatılmıştır. Kamu hizmetinin tanımı yapılmış ve ilkeleri ortaya konulmuştur.

İkinci bölümde ise akıllı şehirlerde kişisel verilerin korunması hakkı kapsamında uygulanacak hukuk incelenmiştir. Bu çerçevede ulusal ve uluslararası düzenlemeler ele alınmıştır. Akıllı şehirlerde veri güvenliğini önemi, kişisel verilerin akıllı şehirlerde neden korunması gerektiği, akıllı şehirlerde veri işleme işlemlerini şartları, akıllı şehirlerde veri sorumlusunun kim olduğu ve sorumlulukları anlatılmıştır.

Bu çalışmanın amacı, geleceğin şehir konsepti olan akıllı şehirlerin bir gözetim toplumuna dönüşmemesi, akıllı şehir sakinlerinin insan haklarına uygun onurlu bir hayat yaşaması ve akıllı şehirlerde veri işleme açısından iktidarın sınırlarını çizerek kişilerin mahremiyetine saygı gösterilmesi gerektiğini vurgulamaktır.

BİRİNCİ BÖLÜM

KAMU HİZMETİ YÖNÜYLE AKILLI ŞEHİR KAVRAMI

I. AKILLI ŞEHİR KAVRAMININ ORTAYA ÇIKIŞI, TANIMI, BİLEŞENLERİ VE KULLANILAN TEKNOLOJİK ARAÇLAR

A. Akıllı Şehir Kavramının Ortaya Çıkışı

Şehir veya kent kavramının ne demek olduğu araştırıldığında görülmektedir ki, kavram üzerinde fikir birliği bulunmamaktadır. Sosyologlar, siyaset bilimciler, yönetim bilimciler, şehir planlamacıları, ekonomistler yani iktisatçılar, coğrafyacılar ve tarihçiler kenti tanımlarken kendi bilimsel kuramları açısından ele almışlar ve farklı farklı tanımlar ortaya çıkmıştır. Ayrıca kentin tanımı yapılırken yaşanılan zaman da büyük öneme sahiptir. Zaman içerisinde insanların şehir kavramına bakış açılar değişmiştir. Bir yerleşim yerinin şehir olarak nitelendirilmesi için sahip olması beklenen kriterler zamanla değişmiştir.

Kent kavramı ile ilgili ortaya çıkan ilk kuramlarda kent, köy kavramının karşıtı olarak görülmüştür. Köy olmayan yerleşim yerleri kent olarak tanımlanmıştır. Kenti ortaya koymak için ise köy ile kent toplumları arasındaki farklılıklara dikkat çekilmiştir. Ferdinand Tönnies'e göre; ırk, etnik köken ve kültür bakımından birbirlerine benzeyen insanlardan oluşan, ilişkilerin şahsi ve samimi olduğu küçük, homojen topluluklar "*cemaat*"; ırk, etnik köken, statü ve kültür bakımından farklılaşmış, heterojen topluluklar ise "*cemiyet*" olarak tanımlanmış olup, cemaat kavramı köyü, cemiyet kavramı kenti karşılamaktadır. Aynı şekilde Durkheim'in insan topluluklarını, mekanik dayanışmanın temel olduğu "*basit cemiyetler*" ve organik dayanışmanın temel olduğu "*karmaşık cemiyetler*" olmak üzere ikiye ayırması, köy ile kenti ayırmasına karşılık gelmektedir[1].

Sorokin ve Zimmerman, meslek, çevre, genişlik, yoğunluk, türdeş olup olmama, toplumsal farklılaşma ve tabakalaşma, hareketlilik ve toplumsal ilişki

[1] A. Kadir Topal, "*Kavramsal Olarak Kent Nedir ve Türkiye'de Kent Neresidir*?", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 6/1 (2004), s. 278.

sistemi olarak sekiz ölçütle kent ile köy arasındaki farkı ortaya koymaya çalışmışlardır. Kenti nüfus büyüklüğü, yoğunluk ve heterojenlik özellikleriyle ele alan L. Wirth'e göre kent, göreli olarak büyük, yoğun ve toplumsal olarak heterojen kişilerin devamlı olarak yerleşmesidir. Weber'e göre kent, insanların tarımdan daha çok ticaret ile uğraştığı, bir pazaryeri ve bir kalesi bulunan, belli bir dereceye kadar hukuk düzeni bulunan ve belli bir dereceye kadar bağımsız olan yerleşim yeridir[2]. Teknolojinin gelişme düzeyine göre kent tiplerini belirlemeye çalışan Sjoberg'e göre ekolojik temel, teknoloji ve karmaşık sosyal organizasyonlar kentsel hayatı oluşturur[3].

Jean Louis Hout ise kenti, ekonomik ve sosyal faaliyetlerin çeşitlendiği, bireysel ve ailesel düzeyde çözülemeyecek sorunların çözülmesine imkân tanıyan bir karmaşık yapıya sahip, fikirlerin yayıldığı ilişkiler ve kararlar merkezi olarak görmektedir[4].

Görmez'e göre kent, tarım dışı üretime dayalı ekonomiye sahip, örgütlenme, uzmanlaşma ve iş bölümünün en yüksek seviyede olduğu, karmaşık ve dinamik bir mekanizmanın her zaman işlediği insan yerleşimleridir[5]. Bal'a göre kent, ticaret, sanayi ve hizmet gibi ekonomik etkinliği olan, ürünlerin dağıtıldığı, sınırlı bir alanda sosyal bakımdan tabakalaşmış yoğun bir nüfusa sahip, mesleki rollerin artarak değişiklik gösterdiği, sosyal gruplar, sivil toplum örgütleri, merkezi ve yerel idareyi temsil eden yönetim kurumları barındıran, yerel, bölgesel veya uluslararası ilişkiler ağına sahip heterojen toplumdur[6].

Netice olarak söylenebilir ki kent, tarımsal faaliyetin az, ticari, sanayi ve hizmet faaliyetlerinin daha yaygın olarak gösterildiği, imkanları kırsal alanlara göre

---

[2] Hüseyin Bal, "*Kent Sosyolojisi*", 9. bs., Sentez Yayıncılık, Bursa, 2020, s. 198 vd.
[3] Louis Wirth, "*Bir Yaşam Biçimi Olarak Kentlileşme*", Ayten Alkan, Bülent Duru (Der. ve Çev.), 20. Yüzyıl Kenti, İmge Yayınevi, Ankara, 2002, s. 105.; Topal, "*Kavramsal Olarak Kent Nedir ve Türkiye'de Kent Neresidir?*", s. 279 vd.
[4] Jean Louis Huot, Jean Paul Thalmann, Dominique Valbelle, "*Kentlerin Doğuşu"*, Ali Bektaş Girgin (Çev.), 1. bs., İmge Kitabevi, Ankara, 2000, s. 14.; Topal, "*Kavramsal Olarak Kent Nedir ve Türkiye'de Kent Neresidir?*", s. 281 vd.
[5] Kemal Görmez, "*Şehir ve İnsan*", Milli Eğitim Basımevi, İstanbul, 1991, s. 1.
[6] Hüseyin Bal, "*Kent Sosyolojisi*", s. 32.; Topal, "*Kavramsal Olarak Kent Nedir ve Türkiye'de Kent Neresidir*?", s. 285 vd.

daha fazla, içinde bulunan yoğun nüfusun örgütlenerek yaşamını devam ettirdiği, sosyal, ekonomik ve kültürel alanlardır[7].

Sanayi devrimi öncesi geçimini topraktan sağlayan toplumlardan dolayı, dünyadaki şehirleşme oranı yüzde 5'i geçmemiştir. Sanayi devrimi sonrası ticaret ve sanayinin gelişmesiyle toprağa bağlılık azalmış ve sosyal bir değişim süreci yaşanmıştır. Bu süreçte dünya nüfusunun da artmasıyla şehirlerde bir nüfus birikmesi yaşanmış; sanayileşmenin bir sonucu olarak şehirleşme kavramı gündeme gelmiştir[8].

Şehirler insanlık tarihi boyunca değişimin merkezi olmuştur, toplumdaki büyük çapta değişikliklerin fitili kentlerde ateşlenmiştir ve bu toplumsal değişimlerle beraber şehirlerin iç yapıları da değişmiştir. Ancak en büyük değişimler ise 20. yüzyılının son çeyreğinde olmuştur. Bu değişimde önemli bir etkisi olan kavram ise küreselleşmedir[9].

Dünyada hala kente göç devam etmekte olup kent nüfusu artış göstermektedir. Yirminci yüzyıl başlarında dünya nüfusunun yaklaşık %10'u şehirlerde yaşamaktaydı. 1980'lerde ise bu oran %30'lara ulaşmıştı[10]. İlk defa 2007 yılında insan nüfusunun çoğu şehirlerde yaşamaya başlamıştır[11]. Birleşmiş Milletler'in 2014 tarihli "*Dünya Kentleşme Beklentileri*" isimli rapora göre 2050 yılında kentlerde yaşayacak insan nüfusunun, dünya nüfusunun %70'i olması beklenmektedir[12].

Kentsel yayılmanın önemli bir kavram olduğu 20. yüzyılda büyüyen kentsel araziler, merkezden bağımsız olarak gelişen kentsel fonksiyonlar ve hızla gelişen toplu konutlar gibi faktörler birçok kentin kalitesini düşürmüştür. Çevresel deformasyon ve insan yapısına aykırı yaşam alanlarının artması 21. yüzyılda devam

---

[7] Burak Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", (Yüksek Lisans Tezi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara 2021), s. 7.

[8] Mücella Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", (Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2018), s. 2.

[9] Özgür Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", (Bitirme Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2017), s. 5.

[10] Huot, Thalmann, Valbelle, *"Kentlerin Doğuşu"*, s. 11.

[11] Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", s. 8 vd.

[12] Birleşmiş Milletler Dünya Kentleşme Beklentileri 2014 Basın Bülteni, Link: https://population.un.org/wup/Publications/Files/WUP2014-PressRelease.pdf (Çevrimiçi Tarihi: 21.07.2023)

etmekte olup sosyal ve ekonomik sınıf farklılıkları, sağlık sorunları, altyapı ve kaynak sorunları giderek artacaktır[13].

Ortaya çıkabilecek sorunların önüne geçebilmek için, yerleşim yerlerinin planlanması ve tasarlanması süreçlerinde akıllı gelişme stratejileri de entegre edilmiştir. Bu kaygılara çözüm olarak Sürdürülebilir Kentler (Sustainable Cities), Ekolojik Kentler (Ecological Cities, Green Cities), Akıllı Büyüme (Smart Growth), Yavaş Kentler (Slow Cities), Düşük Karbon Kentler (Low Carbon Cities), Yaşanabilir Kentler (Liveable Cities), Dijital Kentler (Digital Cities) ve Akıllı Kent Girişimleri (Smart Cities Initiatives) gibi kavramlar gelişmiştir[14].

Öğrenen Kentler; kentte öğrenmeyi yaygınlaştırmak amacıyla bilgi akışını kolaylaştıracak bir altyapıya sahip, yönetişim mekanizmalarının güçlü olduğu, paylaşma, katılımcılık ve hayat boyu öğrenmenin ön planda olduğu kentleri ifade eder[15].

Sürdürülebilir kentler; ekolojiyi ve çevreyi korumayı amaçlayan, geri dönüşüm esaslı tüketim modelinin benimsendiği, arazinin verimi kullanıldığı, yaşam kalitesinin yüksek olduğu sağlıklı ve sürekli şehir modelini ifade eder[16].

Yürünebilir kentler; ulaşım kaynaklı çevre sorunlarını en aza indirmek amacıyla yürümenin teşvik edildiği ve insanların yaşam alanlarına yürüyerek rahatça erişebildiği kentleri ifade eder[17].

Yavaş kentler; insanları yüksek tempolu bir şekilde yaşamaya sevk eden hızlı üretim-hızlı tüketim akımına karşı tepki olarak ortaya çıkan fikirlerin savunduğu şehir modelini ifade eder[18].

---

[13] Serkan Sınmaz, "*Yeni Gelişen Planlama Yaklaşımları Çerçevesinde Akıllı Yerleşme Kavramı ve Temel İlkeleri*", Megaron, 8/2 (2013): s. 77.

[14] Sınmaz, "*Yeni Gelişen Planlama Yaklaşımları Çerçevesinde Akıllı Yerleşme Kavramı ve Temel İlkeleri*", s. 77.; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 4 vd.

[15] Rongxia Zhuang, Haiguang Fang, Yan Zhang, Aofan Lu and Ronghuai Huang, "*Smart Learning Environments For A Smart City: From The Perspective Of Lifelong And Lifewide Learning*", Open Access, 2017, 4/6, (DOI 10.1186/s40561-017-0044-8), s. 3, Link: https://slejournal.springeropen.com/articles/10.1186/s40561-017-0044-8 (Çevrimiçi Tarihi: 09.07.2023); Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 25.

[16] Melih Ersoy, "*Kentsel Planlama – Ansiklopedik Sözlük*", 2. bs., Ninova Yayıncılık, İstanbul, 2016, s. 420.; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 25.

[17] Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 25.

[18] Erkan Polat, "*Ağır Ağır Çıkacaksın Bu Merdivenlerden: Yavaş Kent Hareketi (Cittaslow)*" Mimarlık Dergisi, S: 359, Mayıs-Haziran 2011; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 26.

Sağlıklı kentler; planlamanın insan ve sağlık eksenli yapıldığı, Dünya Sağlık Örgütü tarafından ortaya atılan kavramdır[19].

Düşük karbonlu kentler; karbon salınımının azaltılması ve çevreye olan olumsuz etkisini minimuma indirmeyi amaçlayan, bu amaç doğrultusunda şehir yoğunluğunun dengeli bir biçimde planlandığı kent modelini ifade eder[20].

Yaşanabilir kentler; insan-çevre-kent ilişkisinin insan doğasına en uygun olacak şekilde dengeli bir planlamaya sahip kentleri ifade eder[21].

Dijital kentler; kentin teknolojik altyapıyla donatıldığı, yönetim, fiziki çevre, toplum ilişkileri ve altyapının teknolojik uygulamalarla yeniden yapılandırıldığı kentleri ifade eder[22].

Teknolojik alanda yaşanan gelişmeler, kentleşmenin sebep olduğu sorunların önüne geçmek içi düşünülen çözüm önerilerine de yeni bir boyut kazandırmıştır. Şehirleşmenin yol açtığı olumsuz sonuçları en aza indirmek ve hayat kalitesini en yüksek seviyede tutmak için geliştirilen, 1990 sonrası ortaya çıkan ve tek açıdan konuyu alan bu yaklaşımların yanında konuyu daha kapsayıcı ele alan, bilgi teknolojileri temelli ve birçok yönden de sürdürülebilir hedefler belirleyen bir yaklaşım doğmuştur. Bu yaklaşımın ismi "*akıllı şehir*" kavramıdır.

Bu kavramın benimsenmesinde asıl rolü, küresel enerji krizi oynamıştır. Akıllı şehir kavramı ve modelini ilk defa 2008 yılında IBM Şirketi kullanmıştır[23]. IBM Daha Akıllı Gezegen projesi ile kentsel sorunların çözümü amacıyla ağlar, sensörler ve diğer yöntemler kullanılmaya başlanmıştır. Akıllı şehir temalı ilk kongre

[19] İsmail Başaran, "*Sağlıklı Kentler Kavramının Gelişiminde Sağlıklı Kentler Projesi*", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 9/3 (2007), s. 208.; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 26.

[20] Arif Şentek, "*Sorumlu Bir Mimarlık İçin Manifesto*", Mimarlık Dergisi, S:387, Ocak- Şubat 2016, Link: http://www.mimarlikdergisi.com/index.cfm?sayfa=mimarlik&DergiSayi=401&RecID=3824 (Çevrimiçi Tarihi: 14.07.2023); Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 26.

[21] Özge Yalçıner Ercoşkun, "*Sürdürülebilir Kent İçin Ekolojik-Teknolojik (Eko-tek) Tasarım: Ankara-Güdül Örneği*", (Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü), Ankara 2007, s. 37.; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 27.

[22] Akif Çukurçayır, "*Dijital Kentler ve Kent Yönetimi*", Link: https://www.academia.edu/14408770/Dijital_Kentler_ve_Kent_Y%C3%B6neti (Çevrimiçi Tarihi: 14.07.2023).; Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 27.

[23] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", s. 9.

2011 yılında Barcelona'da düzenlenmiştir. Çin, 2013 yılında 90, 2014 yılında 103, 2015 yılında 84 şehir için akıllı şehir projelerini açıklamıştır[24].

Akıllı şehir kavramının ortaya çıkması ve gelişmesinde etkili olan kavram ise teknolojidir. Kablolu veya kablosuz ağlar kurmak suretiyle şehirde teknolojik altyapının kurulması, bu altyapı sayesinde bilginin ulaşılabilir ve kullanabilir olması, kullanılan bu bilgelerle de gerek kamu kurumlarının gerekse özel kuruluşların şehirde yaşayan insanlara dijital hizmet sunması, bir şehrin akıllı olmasının özünü oluşturur[25].

B. Tanımı

T.C. Çevre ve Şehircilik Bakanlığı tarafından 2019 yılında hazırlanan *"2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı"*na göre akıllı şehirlerle amaçlanan;

- *"Şehrin mevcut ve gelecek beklenti ve problemlerini şehrin tüm mekânlarında ve sistemlerinde tetikleyici güç hâline getirmek,*
- *Fiziksel, sosyal ve dijital planlamayı birlikte ele alabilmek,*
- *Ortaya çıkan zorlukları sistematik, çevik ve sürdürülebilir bir şekilde öngörmek, tanımlamak ve karşılamak,*
- *Şehir içindeki organizasyonel yapılar arası etkileşimi sağlayarak bütünleşik hizmet sunumu ve yenilik üretme potansiyelini ortaya çıkarmaktır"*[26].

Akıllı şehir, insan odaklı, halkın katılımını sağlayacak şekilde iyi bir yönetişim modeli ile yönetilen, yaşam kalitesi yüksek, yeniliğe açık, rekabetçi, çevre dostu ve bu hedeflere ulaşmak için insanları, kenti ve bilgiyi yeni teknolojiler ile entegre eden, yüksek teknolojili şehirlerdir[27].

Uluslararası Standartlar Teşkilatı'nın tanımına göre (ISO) akıllı şehirler, planlama, inşa, yönetim ve hizmetleri kolaylaştırmak için büyük veri, bulut bilişim,

---

[24] Burcu Barutçu, "*Akıllı Şehirler Üzerine Sistemik Bir Literatür Taraması ve Akıllı Şehirlerde Endüstri Mühendisliği Uygulama Alanları*", (Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü), Ankara 2021, s. 9.

[25] Nefise Ayşe Şenay Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", (Yüksek Lisans Tezi, Çanakkale OMÜ Lisansüstü Eğitim Enstitüsü, Çanakkale 2022), s. 42.

[26] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", Link: https://akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf (Çevrimiçi Tarihi:05.04.2023)

[27] Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", s. 6.

nesnelerin interneti ve bütünleşmiş coğrafi bilgi sistemleri gibi yeni nesil bilgi iletişim sistemlerinin kullanıldığı yeni bir şehir modelidir. Avrupa Parlamentosu'na göre akıllı şehir, kamu sorunlarını bilgi iletişim teknolojileri tabanla çözümlerle ele alan şehirdir[28]. Birleşmiş Milletler'e göre akıllı şehir, tüm altyapıyı teknolojiyi kullanarak kuran, çevresel sürdürülebilirliği sağlayarak daha temiz bir çevreyi hedefleyen, vatandaş odaklı şehirdir[29].

Akıllı şehirler gibi çeşitli konularda da standartlar geliştirmekte ve danışmanlık hizmetleri sunmakta olan, İngiltere merkezli bir sertifikasyon ve standartlar oluşturma kuruluşu BSI Group'un tanımına göre akıllı şehir, "*ekosistem varlıklarına sürdürülebilir, müreffeh ve kapsayıcı bir gelecek sunmak için fiziksel, dijital ve insani sistemlerin yapılandırılmış bir çevre ile etkin entegrasyonudur*"[30]. Bu tanıma göre akıllı şehir; ulaşım, enerji, su, atık yönetimi gibi şehrin fiziksel alt yapısı, şehrin veri ve bilgi akışının olduğu teknolojik altyapısı ve insanların toplumsal, kültürel ve ekonomik ihtiyaçlarını entegre eden şehir olarak anlaşılmaktadır. Ayrıca akıllı şehirler, ekosistem varlıklarının gelecek nesillerin ihtiyaçlarını da karşılayacak şekilde kullanılmasını, yüksek yaşam standartlarına sahip, zengin ve kapsayıcı bir geleceği düşlemektedir. Bir başka ifadeyle bu yaklaşım şehirlerin çevresel, ekonomik ve sosyal sürdürülebilirliğini arttırmayı hedeflemektedir.

İngiliz Hükümeti, İş İnovasyonu ve Becerileri Departmanı (Department for Business Innovation and Skills) 2013 tarihli "*Smart Cities Background Paper*" isimli raporda akıllı şehirlerin sadece fiziksel altyapıyı değil, aynı zamanda sosyal sermayeyi ve vatandaşlık katılımını da kapsayan bir süreç olduğu vurgulanmaktadır. Ayrıca, dijital teknolojilerin de akıllı şehirlerin gelişmesine katkı sağladığına değinilmektedir[31].

Avrupa Parlamentosu "*Mapping Smart Cities in the EU*" isimli raporunda, akıllı şehirlerin, birden fazla paydaşın iş birliği içinde çalıştığı, BİT (Bilgi ve İletişim

[28] Aınıwaer Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", (Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2018), s. 4.
[29] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 38.
[30] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 19.
[31] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 19.

Teknolojileri) tabanlı teknolojik çözümlerle kamu sorunlarını çözmeyi hedefleyen bir yaklaşım olduğu ifade edilmektedir[32].

Manchester Dijital Geliştirme Ajansı (Manchester Digital Development Agency), akıllı şehirlerin, vatandaşların yaşam tarzları, iş ve seyahat seçenekleri hakkında bilinçli seçimler yapmaları için gerekli tüm bilgiyi sağlayarak, vatandaşları "*akıllı vatandaşlar*" olarak tanımlamayı hedeflediği ifade etmektedir[33].

T.C. Çevre ve Şehircilik Bakanlığı akıllı şehirleri "*Paydaşlar arası iş birliği ile hayata geçirilen, yeni teknolojileri ve yenilikçi yaklaşımları kullanan, veri ve uzmanlığa dayalı olarak gerekçelendirilen ve gelecekteki problem ve ihtiyaçları öngörerek hayata değer katan çözümler üreten daha yaşanabilir ve sürdürülebilir şehirler"* olarak tanımlamıştır[34].

Çevre ve Şehircilik Bakanlığı'nın yapmış olduğu bu tanım, akıllı şehirlerin özelliklerini ve hedeflerini belirleyen birçok önemli unsur içermektedir.

- Paydaşlar arası iş birliği: Akıllı şehirlerde, belediyeler, özel sektör, sivil toplum örgütleri ve diğer paydaşlar arasında güçlü bir iş birliği ve ortaklık gerektirir. Bu iş birliği, birlikte çalışarak ortak hedeflere ulaşmak için farklı becerileri, kaynakları ve uzmanlıkları bir araya getirmeyi içermektedir.

- Yeni teknolojiler ve yenilikçi yaklaşımlar: Akıllı şehirler, en son teknolojileri ve yenilikçi yaklaşımları kullanarak, şehirlerin daha verimli, sürdürülebilir ve yaşanabilir olmasını sağlayacak çözümler geliştirmeyi hedefler. Akıllı ulaşım sistemleri, akıllı bina teknolojisi, akıllı enerji yönetimi ve akıllı tarım uygulamaları ile örneklendirilebilir.

- Veri ve uzmanlığa dayalı olarak gerekçelendirilen: Akıllı şehirler, verileri toplamak, analiz etmek ve bunları karar verme süreçlerine dahil etmek için teknolojileri kullanır. Önce fiziki çevreden ve insanlardan veriler toplanır,

---

[32] Avrupa Parlamentosu, Mapping Smart Cities in EU, Link: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(2014)507480_EN.pdf (Çevrimiçi Tarihi: 14.07.2023).; T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 19.

[33] Link: https://www.centreforcities.org/reader/smart-cities/what-is-a-smart-city/ (Çevrimiçi Tarihi: 14.07.2023).; T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 19.

[34] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 20.

daha sonra şehir yöneticileri, vatandaş ve diğer paydaşlar toplanan bu bilgiye dayalı olarak kararlar alması sağlanır.

- Gelecekteki problemleri öngörmek: Akıllı şehirler, gelecekteki demografik, çevresel ve sosyal trendleri ve bunların şehirler üzerindeki etkilerini öngörerek, gelecekte ortaya çıkacak sorunları ele almak için hazırlıklı olmayı amaçlamaktadır.
- Hayata değer katan çözümler: Akıllı şehirler hem şehir yöneticileri hem de vatandaşlar için hayata değer katan çözümler üretir. Bu, şehirlerin daha verimli, daha sürdürülebilir ve daha iyi bir yaşam kalitesi sunan yerler olmasını sağlar.
- Yaşanabilir ve sürdürülebilir şehir: Akıllı şehirler, hayat kalitesinin yüksek olduğu, ekonomik, sosyal ve çevresel açılardan dengeli bir şekilde kalkınmış, gelecek nesillerin ihtiyaçlarını da karşılayacak şekilde mevcut kaynakları kullan şehirlerdir.

Görüldüğü gibi akıllı şehir kavramının net bir tanımını yapmaya çalışan birçok görüş bulunmaktadır.

Akıllı şehir kavramı tanımlanan kullanılan dört unsur göze çarpmaktadır. Birincisi, kentle ile ilgili fikirlerin bütünleşmesi için topluluklara ve şehirlere uygulanan, bilgi tabanına dayalı elektronik ve dijital uygulamalar; İkincisi, bilgi teknolojilerinin hayatı önemli bir boyutta değiştirecek şekilde kullanılması; üçüncüsü, bilgi teknolojilerinin kentin alt yapısı haline gelmiş olması ve bunun kullanılması; dördüncü olarak, bilgi işlem teknolojileri ve insanları, bilgiyi artırmak, problemleri çözmek, yenilik kazanmak için bir araya getiren mekanların varlığıdır[35].

Akıllı şehir kavramının iyileştirmeyi ve geliştirmeyi hedeflediği alan sadece şehirlerin fiziki alanları değildir ayrıca sosyal açıdan da farklı dinamiklerin geliştirilmesi hedeflenmektedir. Bir başka ifadeyle akıllanma mekânsal boyutla sınırlı kalmayıp her alanda kendini göstermesi beklenmektedir. Enerji kaynaklarının azalmasıyla ters orantılı olarak artan hizmet taleplerinin karşılanması için daha

[35] Ateş, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*", s. 29.; Barutçu, "*Akıllı Şehirler Üzerine Sistemik Bir Literatür Taraması ve Akıllı Şehirlerde Endüstri Mühendisliği Uygulama Alanları*", s. 4.; N. Komninos, "*Intelligent Cities: Innovation, Knowledge Systems And Digital Spaces, London And New York*", 2002, s. 2-10.

bütüncül, katılımcı ve dinamik bir karar alma ve yönetme mekanizmalarının kurulması akıllı şehirler için olmazsa olmazlar arasındadır. Bu nedenle akıllı şehirler, aktif katılımı hedefleyen, hizmet taleplerine pratik, sürdürülebilir ve çevresel çözümler üreten, yenilikçi, kaynakları tasarruf odaklı kullanan, teknolojinin tüm imkanlarını kullanarak bilgi teknolojilerine yatırım yapmış, dinamik ve birbiriyle sistematik olarak bağlantılı sistemlerle kurulmuş şehirlerdir[36].

C. Bileşenleri

Akıllı şehrin boyutları konusunda, tıpkı akıllı şehrin tanımında olduğu gibi literatürde farklı görüşler bulunmaktadır. Ancak bu görüşler arasında en fazla kullanılan ve Avrupa Birliği tarafından da kabul edilen, Giffenger ve arkadaşlarının çalışmaları ve Prof. Boyd Cohen'in "*akıllı şehir çarkı*" metodolojisidir. Giffenger ve arkadaşları, "*endüstri*", "*eğitim*", "*katılım*" ve "*teknik altyapı*" olmak üzere 4 boyut tanımlamışlar ve daha sonra Viyana Teknoloji Üniversitesi Bölgesel Bilim Merkezi tarafından yürütülen bir çalışmayla boyutlar; akıllı bir ekonomi, akıllı hareketlilik, akıllı çevre, akıllı insan, akıllı yaşam ve akıllı yönetişim olarak sıralanmıştır[37].

1. Akıllı Ekonomi

Akıllı ekonomi, akıllı şehirlerde üretkenliği yani işletmelerin verimliliğini artırarak, ticari marka oluşturarak, işgücüne dinamik ekonomik koşullarda piyasa ihtiyaçlarına göre hızlı uyum sağlayacak esnekliği kazandırarak, küresel piyasalara entegrasyonu hedefleyen bir yaklaşımdır. Akıllı şehirlerde, bu hedeflerin gerçekleştirilmesi için yenilikçi anlayışa, dönüşüm kabiliyetine ve rekabet gücünün artırılmasına ihtiyaç vardır[38].

Girişimcilik, akıllı şehirlerin yerel ekonomilerinin canlanması ve istihdamın artması için yenilikçi fikirlerle işletmeler kurarak veya olan işletmeleri büyüterek ekonomik faaliyetleri artırmayı hedefler. Ticari marka oluşturma, işletmelerin tanınmışlığını ve müşteri sadakatini artırarak, işletmelerin pazarlama faaliyetleriyle daha fazla müşteriye ulaşmasını ve daha fazla gelir elde etmesini sağlar.

---

[36] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", s. 10 vd.
[37] Abdurrahman Avcıoğlu, "*Akıllı Şehirlerden Akıllı Ülkelere: Akıllı Ülke Sıralama Modeli ve Türkiye Analizi*", (Doktara Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara 2020), s. 16 vd.
[38] Merve Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", (Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul 2020), s. 7.

Teknolojinin gelişmesiyle geleneksel üretim yöntemleri yerine e-iş konseptleri gelişmiştir. E-ticaret sayesinde tüketici, üreticiyle sanal ortamda buluşarak hızlı, güvenilir, seçenekleri çok ve ekonomik alışveriş yapma imkanına kavuşmuştur. Ulusal ve uluslararası ticaret daha izlenebilir duruma gelmiştir. Bu imkanlar akıllı şehirleri küresel çapta rekabetçi bir konuma getirmiştir[39].

2. Akıllı Çevre

Akıllı çevre, bilgi teknolojileri kullanarak doğal kaynakların israf edilmesini önleyen, çevre ve doğanın sürdürülebilirliğini sağlayan sistemdir[40]. Akıllı çevre hem doğal kaynakların korunmasını hem de ekonomik tasarruf sağlanması amaçlayan, ekolojik dengeleri gözeterek tasarlanan sistemlerdir. Bu sistemler, çevresel etkileri en aza indirmek için yeşil alanların korunmasına, su kaynaklarının yönetimine, atıkların toplanmasına ve geri dönüştürülmesine hizmet eder. Ayrıca hava kirliliği, gürültü kirliliği ve su kirliliği gibi çevresel problemlerin çözümüne de katkı sağlayarak, insanların yaşam kalitesini de arttırmayı hedefler.

Akıllı şehirler, doğal kaynaklarını etkin ve verimli bir şekilde kullanan, biyolojik çeşitliliği koruyan, yenilenebilir enerjiye odaklanmış ve etkili bir atık su yönetimine sahip şehirlerdir[41]. Akıllı çevre bileşeni, hava, su, toprak kirliliğini minimuma indirecek sistemler, tasarruf yapan akıllı aydınlatma sistemleri, yenilenebilir enerji sistemleri, akıllı şebekeler, yeşil binaları kapsamaktadır[42].

3. Akıllı Toplum

Akıllı şehir uygulamalarının odağında insan bulunmaktadır. Her konuda değişime açık ve her alanda kendini geliştiren, yeniliklere açık ve yaşadığı şehirle bütünleşmiş insanlar akıllı toplumu inşa eder[43]. Akıllı şehirleri inşa eden insanların, gelişime ve değişime ayak uydurabilmesi için eğitim seviyesi yüksek ve yaşam boyu öğrenmeye açık, yaratıcı ve yönetimde etkili olacak şekilde katılımcı olmaları

---

[39] Tuğçe Altınkilit, "*Akıllı Şehir Tasarım İlkeleri ile Uyumlu Bir E-planlama Sistemi Geliştirilmesi-Bayraklı Örneği*", (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Fen Bilimleri Enstitüsü, İzmir 2022), s. 9 vd.
[40] Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", s. 18.
[41] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 46 vd.
[42] Büşra Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir 2022), s. 39.
[43] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 44.

önemlidir[44]. Akıllı insan, teknolojileri sadece kullanan değil aynı zamanda teknoloji üreten, bilgi iletişim teknolojilerini kullanarak toplumsal hayata aktif katılımda bulunan, yaratıcılık ve yenilikçilikle donanmış bireydir[45].

Akıllı toplum, esnek, yaratıcı, açık fikirli, e-öğrenme yöntemleriyle yaşam boyu öğrenmeyi alışkanlık haline getirmiş, toplumsal kalkınmada aktif rolü olan, kültürel, sosyal ve siyasi bakımdan farklı kökenlere sahip insanların bir arada yaşadığı ve karşılıklı etkileşim içinde olduğu, evrensel perspektife sahip toplum demektir[46].

4. Akıllı Yönetişim

Akıllı yönetim, şeffaflık, işbirlikçilik ve katılımcılık prensiplerini benimsemiş, vatandaşlara çevrim içi hizmetler sağlamak için dijital altyapıları geliştiren yönetişimi ifade eder. Şeffaflık, çevrimiçi uygulamalar vasıtasıyla yönetime ilişkin verileri vatandaşla paylaşmayı, vatandaşların diledikleri her an yönetim verilerine ulaşıp kullanabilmelerini ifade eder. Şehir yönetiminde kamu kurumları, özel kuruluşlar, araştırma kuruluşları, üniversiteler gibi katılımcıların yanı sıra halkın da söz sahibi olması önemlidir. Akıllı şehirlerde sunulan uygulamalar ile şehir sakinleri, görüşünü belirtip, yönetime ilham verme, karar alma sürecine ortak olma imkanlara sahiptir[47].

Yönetişim, bir kuruluşun veya topluluğun etkin bir şekilde yönetilmesi için farklı paydaşların katılımı sağlanarak, şeffaf ve hesap verebilir olarak kullanılan yöntem ve süreçlerin tamamıdır. Akıllı şehirlerde kamu yönetimi, devlet, özel sektör ve sivil toplumun iş birliğine dayanmakta ve alınan kararlardan etkilenecek vatandaşlar da karar sürecinde söz sahibi olmaktadır. Vatandaşlar kamu yönetim sürecine, bilgi iletişim teknolojileri kullanılarak oluşturulan kanallar aracılığı ile katılım sağlamaktadır. Bu sürece "*e-yönetişim*" denilmektedir[48].

---

[44] Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", s. 12 vd.
[45] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 7.
[46] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 45.
[47] Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", s. 15 vd.
[48] Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", s. 40.

5. Akıllı Hareketlilik

Akıllı ulaşım, metro, tren, tramvay, otobüs, araba, bisiklet ve yaya gibi birden fazla ulaşım şeklinin birbirine bağlanarak bütünleştiği, bilgi teknolojileri ile desteklenmiş, güvenli ulaşım sistemlerini ifade eder. Akıllı ulaşımda en önemli ilke temiz enerji taşımacılığıdır. Hava kirliliğini azaltmak amacıyla bisiklet, elektrikli taşıma gibi çevre dostu yöntemler ile kişi başı araç sayısının düşürülmesi için toplu taşıma teşvik edilmektedir[49]. Bunun için bisiklet park yerleri, elektrikli araç şarj merkezleri, güvenli yürüme yolları, toplu taşımada demiryolu-karayolu-denizyolu sistemlerinin entegre olması, aktarmaların rahatça yapılabilmesi gibi gerekli altyapı sağlanır.

Ayrıca maliyet ve zaman kaybının önlenmesi için insanlara en doğru istikametinin oluşturulması da hedeflenmektedir[50]. Şehir sakinleri mobil uygulamalar ile şehrin trafik durumunu kontrol edebilmektedir. Şehrin cadde ve sokaklarında insanları yönlendirici akıllı uyarı sistemleri bulunur. Şehre yerleştirilmiş ağlar ve sensörler ile inşa edilmiş trafik yönetim sistemi sayesinde güvenli bir şekilde trafik düzeni sağlanır.

6. Akıllı Yaşam

Toplumun sosyalleşebilmesi için yeterli sosyal tesislerin varlığı, sağlık hizmetlerinin yürütülmesi için yeterli fiziki imkanların ve personelin bulunması, suç işleme oranının düşürülmesi için alınmış güvenlik tedbirleri, barınma ihtiyacını karşılayacak yeterli konut sayısı ve eğitim hizmetlerinin sunulması için gereken eğitim tesisleri yaşam kalitesini etkileyecek unsurlardır. Yaşam kalitesini artırmak için bu unsurlara ulaşmayı hedefleyen uygulamaların tamamına akıllı yaşam denilmektedir[51]. Akıllı yaşam, teknolojinin yardımıyla insanların hayatını daha kolay ve konforlu hale getirmeyi amaçlayan bir kavramdır.

Akıllı şehirler, kaliteli kamusal imkanlara sahip, tarihe, kültüre ve doğaya önem veren, özellikle çocuk, kadın ve yaşlılar için güvenli bir yaşam alanı sunan,

[49] Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", s. 17 vd.
[50] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 9.
[51] Aihemaiti, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", s. 12.

hayatın estetiğini geliştirmek için sanatçıların bir araya geldiği, her zaman canlı bir merkezi olan şehirdir[52].

D. Akıllı Şehirlerde Kullanılan Teknolojik Araçlar

Veri, tek başına anlam ifade etmeyen veya kullanılamayan, bununla birlikte enformasyona ve bilgiye temel oluşturan, ilişkilendirilmeye, gruplandırılmaya, yorumlanmaya, anlamlandırılmaya ve analiz edilmeye gereksinim duyulan ham bilgidir[53].

Akıllı şehirlerin temelini güncel bilgi iletişim teknolojilerinin kullanılması bulunmaktadır. BİT'lerin yapıtaşı ise, belirli bir konuda farklı türdeki bilgilerin kaydedilmiş hali olan verilerdir. Bu veriler, metin, sayısal değerler, ses ve görüntü dosyaları şeklinde farklı türde olabilir. Bilgi iletişim teknolojileri bu verilerin depolanması, saklanması, taşınması, istediği zaman tekrar ortaya çıkarılması, analiz edilmesi gibi süreçlerde kullanılan araçlardır. Dolayısıyla akıllı şehirlerin araçları da büyük veri, açık veri, bulut bilişim, nesnelerin interneti ve yapay zekâ olacaktır.

1. Büyük Veri

İlk defa 1990'lı yıllarda tanımı yapılan "*büyük veri*", geleneksel veri tabanları veya işleme yöntemleri ile yönetilemeyecek kadar çok büyük hacimlerde ve yüksek hızda olan, farklı kaynaklardan gelen yapısal veya yapısal olmayan veri setleridir. Bir veri kümesinin büyük veri olarak adlandırılması için 5V olarak isimlendirilen unsurlara sahip olması gerekir. Bu unsurlar; hacim (volume), çeşitlilik (variety), hız (velocity), kalite (value) ve doğrulama (verification) olarak kabul edilmektedir[54].

Büyük verinin büyüklüğü terabaytlar ve petabytelar düzeyindedir. Bu kadar büyük verinin işlenmesi için de veri hızının normalden daha yüksek olması gerekir. Yapılandırılmış (yapısal), yapılandırılmamış (yapısal olmayan) ve yarı yapılandırılmış (yarı yapısal) olmak üzere 3 çeşit veri vardır. Bu ayrım verinin kaydedilirken tasnif edilme şekline göre yapılmaktadır. Yapılandırılmış veri, veri

---

[52] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 50.

[53] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", 21. Malik Yılmaz. "*Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi*." Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi 49/1 (2009), s. 95-118.

[54] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 11.

tabanları veya elektronik tablolar ile belirli bir düzen içinde organize edilmiş, kolayca erişilebilen, filtrelenebilen ve sorgulanabilen verilerdir. Müşteri bilgileri, personel listesi veya stok bilgisi veri tabanlarına kaydedilen veriler yapısal veriye örnek gösterilebilir. Yapılandırılmamış veri, serbest bir şekilde kaydedilmiş, manuel olarak sınıflandırılmış, metin dosyaları, görüntüler veya videolar gibi biçimsel olmayan verilerdir. Sosyal medya paylaşımları, müşteri yorumları, blog yazıları gibi veriler örnek olarak verilebilir. Yarı yapılandırılmış veri, belirli bir düzen veya yapı içinde olmayan, ancak belirli bir düzenleme ile veri madenciliği teknikleriyle analiz edilebilir hale getirilebilen hem yapısal hem de yapısal olmayan veri özellikleri taşıyan veri türüdür. Örnek olarak, anket veya form verileri, dokümanlarda belirli anahtar kelimelerin yer alması gibi veriler verilebilir. Büyük verinin analizi ve kullanımının doğru bir şekilde yapılabilmesi için veri toplama, işleme, depolama süreçlerinin de özenle yapılmış olması ve verinin doğru, işe yarar ve tutarlı olması gerekir. Bu nedenle denilmektedir ki büyük veri, kaliteli ve doğrulanmış veridir.

Kaynakları açısından büyük veri; yönlendirilmiş, otomatik ve gönüllü olmak üzere 3 kategoriye ayrılmaktadır. Yönlendirilmiş veri, bilinçli bir şekilde ve belirli bir amaca yönelik olarak bir operatör tarafından toplanan verilerdir. Anketler, yönlendirilmiş veri toplama yöntemleri kullanılarak toplanan veriye örnek verilebilir. Otomatik veri ise, bir planlama veya zamanlama sınırı olmaksızın, bir sistem tarafından doğal olarak üretilen, sensörler tarafından toplanan verilerdir. Örneğin, üniversite girişinde turnikeye öğrenci kartının okunması neticesinde, kartı okuyan cihaz, kart sahibi kişinin turnikeden geçiş yaptığı zamanı otomatik olarak sisteme kaydeder. Sitemde depolanan, kart sahibi kişinin üniversiteye giriş-çıkış verileri otomatik veridir. Gönüllü veriler ise, herhangi bir kimse tarafından istenmeksizin yani zorunlu olmamasına rağmen kullanıcılar tarafından çeşitli kanallar aracılığıyla paylaşılan verilerdir. Örneğin, bir kişinin sosyal medya hesabında kendisi hakkında bilgiler paylaşması durumunda ortaya çıkan veri gönüllü veridir[55].

Sosyal, kültürel, ekonomik ve teknolojik gelişmeler dünya genelinde veri hacminin artmasına neden olmuştur. Özellikle şehirler, yüksek nüfus yoğunluğu ve gelişmiş teknolojik altyapıları sayesinde farklılaşmış ve büyük ölçekli verilerin üretiminde önemli bir rol oynamaktadır. Bu veriler, kentsel alanlarda bulunan

[55] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 12.

sistemler ve sensörler aracılığıyla toplanmaktadır. Ancak geleneksel bilgi ve iletişim teknolojileri, bu verilerin toplanması, saklanması ve analiz edilmesi için yetersiz kalmaktadır. Bu nedenle, büyük veri analizi için özel teknolojiler ve araçlar geliştirilmiştir[56].

Akıllı şehirlerin oluşturulması sürecinde önemli bir rol oynayan bilgi ve iletişim teknolojileri, şehir içindeki kamu hizmetlerinin verimli ve etkili bir şekilde yürütülmesi, şehrin sürdürülebilirliği ve sosyoekonomik gelişiminin sağlanması için kullanılmaktadır. Akıllı şehirlerde hizmetlerin entegre edilmesi ve şehrin bütününü kapsayan bir bilgi bütünlüğü sağlanması da BİT'nin görevleri arasındadır. Bu sayede, şehirdeki farklı hizmetlerin birbirleriyle entegre edilerek daha etkili ve verimli bir şekilde çalışması, hizmetlerin daha kolay yönetilmesi ve şehirdeki yaşam kalitesinin artırılması hedeflenmektedir. Bu ise ancak uygun yazılım araçları ve teknolojiler kullanılarak, büyük miktarda veri toplayan, depolayan ve analiz eden tematik ortamla mümkün olacaktır. Şehirden alınan verilerle oluşan şehir büyük verisinin, karar alıcılar tarafından etkili bir şekilde kullanılmasıyla yönetim kolaylaşacaktır. Akıllı şehirlerde büyük veri, anlık sistem takibi sağlar ve böylece maliyetten ve zamandan tasarruf imkânı verir[57]. Örneğin, akıllı şehirlerde belediyeler, ulaşım kartı verilerinden yola çıkarak günün hangi saatinde ve şehrin hangi güzergahından toplu taşıma kullanan insanların yoğun olduğunu tespit edip, bu verilere göre otobüs seferi planlaması yapabilecektir. Akıllı şehir sakinleri ise, trafik yoğunluk haritasına bakarak, açık olan yolların hangilerini olduğunu, yoğunluk olan bölgelerin nereler olduğunu, yol bakımı yapılan veya trafik kazasının meydana geldiği yerlerin nereler olduğunu tespit ederek, gitmek istedikleri yere en kısa sürede nasıl gideceklerine karar verebileceklerdir.

2. Açık Veri

Açık veri, herkes tarafından herhangi bir amaç için kontrol mekanizması olmaksızın paylaşılabilen ve kullanılabilen verilerdir. Açık veri, yayınlanmadan önce tam ve doğru olacak şekilde ayıklanmış, elde edilme ve analiz edilme süreci kayıt altına alınmış, toplumun tüm kesimlerine eşit mesafeli, tescil sahibi veya maliki bulunmayan, uzun süre erişilebilen ve yeniden kullanılabilen veridir. Açık verinin en

[56] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", s. 21.
[57] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 12 vd.

önemli özelliği ise, farklı sistemlerin koordinasyonlu bir şekilde çalışması ve kıyaslanabilmesidir[58].

Verilere "*açık*" olarak nitelendirilmesi için şu şartların yerine getirilmiş olması gerekmektedir:

- Kullanılabilirlik ve erişim: Verilerin uygun bir biçimde sunulması, kullanıcıların veriyi kolayca bulmasını ve kullanmasını sağlar. Veriler, mümkün olduğunca internet üzerinden kolayca indirilebilir olmalıdır ve değiştirilebilir bir biçimde sunulmalıdır.
- Yeniden kullanım ve yeniden dağıtım: Veriler, analizleri yapmak, yeni bilgiler elde etmek veya başka amaçlar için kullanmak için diğer verilerle karıştırılabilir, yeniden kullanılabilir ve yeniden dağıtılabilir olmalıdır.
- Evrensel katılım: Açık veri, herkes tarafından kullanılabilir ve yeniden dağıtılabilir olmalıdır[59].

Akıllı şehirlerde açık veri, kamusal sorunların çözümünde veri odaklı yaklaşımın gelişmesine, yönetimin şeffaflaşmasına, vatandaşların daha hesap soran ve hizmetlerin gelişmesinde katkı sunan aktörler olmasına hizmet etmektedir. Akıllı şehirlerde açık veri portallar oluşturulmuştur[60]. Bu portallarda insanlarda şehirde yaşanan güncel olaylar, faaliyetler, şehir içinde kullanılabilecek uygulamalar hakkında bilgi sahibi olabilmektedir. Portallar uzman olmayan kişilerin dahi rahatlıkla kullanıp, veri analizi yapabileceği şekilde hazırlanmaktadır[61].

Örneğin, https://data.ibb.gov.tr/ adresinden ulaşılabilen İstanbul Büyükşehir Belediyesi Açık Veri Portalı İBB ve çevre kuruluşlarından yayımlanan verileri vatandaşların kullanımına sunmaktadır. Hatta portalda olmayan veriler dahi talep edilebilmektedir. Bu portalda İBB açık veriyi "*daha bilinçli bir kamuoyu oluşturma, müşteri hizmetlerini geliştirme, verimlilikleri artırma, vatandaşlardan katma değerli faydalar elde etme ve şeffaf yönetim çabasının bir parçası olarak*" sunduğunu belirtmektedir. Portalda veriler kümelenmiş halde veri seti olarak sunulmaktadır. Kullanıcıların aradıkları verileri rahatça bulabilmeleri için veriler ekonomi, enerji,

[58] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 14.
[59] Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", s. 30.
[60] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 16 vd.
[61] Melek Emikönel, "*Göç ve Akıllı Şehir Türkiye Uygulaması*", (Yüksek Lisans Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2021), s. 18.

yaşam, yönetişim, insan, çevre, BİT, güvenlik ve mobilite olarak kategorilere ayrılmıştır.

3. Bulut Bilişim

Günümüzde BİT cihazlarının ve bu cihazların ürettiği verilerin artması, bu verilerin saklanması ve depolanması sorununu da beraberinde getirmiştir. Depolanması gereken büyük verilerin hacimce çok büyük boyutta olması, bu verilerin fiziki ortamda muhafaza edilmesini imkansızlaştırmaktadır. Bu soruna çözüm olarak bulut teknolojisi ortaya çıkarılmıştır. Bulut bilişim, sunucu, ağ, depolama, veri tabanı, yazılım gibi hizmetlerin ucuz, hızlı ve esnek olarak sunulan yazılımsal depolama hizmetidir. Bulut bilişim hizmeti veren sunucular, altyapı, platform ve yazılım hizmeti sunarak, hizmet alıcılara depoladıkları verilere internet üzerinden ulaşma ve verileri düzenleme imkânı tanımaktadır. Hizmet alıcılar da verilerini fiziki depolama cihazı kullanmaksızın korumakta ve ihtiyaç olduğunda da bu verilere ulaşmaktadırlar[62].

Akıllı şehirlerde de elde edilen verilerin hacimce büyük olması nedeniyle fiziki ortamlarda saklanması neredeyse imkansızdır. Bu nedenle verilerin depolanması, saklanması ve işlenmesi için bulut bilişim teknolojilerinden faydalanmak büyük kolaylık sağlayacaktır.

4. Nesnelerin İnterneti

Bilgisayar ve diğer teknolojik cihazlar internet sayesinde radyo frekansı sinyalleri aracılığıyla veri iletişimi yapmaktadır. İnternet sadece insanlar arasında kullanılan bir ağ değil aynı zamanda nesneler arasında da kullanılan bir ağdır. İnternet ve diğer teknolojilerin de yardımıyla nesneler arasında oluşan bu ağ yeni bir ekosistem ortaya çıkarmaktadır. Bu ekosistemdeki akıllı nesneler sensörler aracılığıyla algılama yapmakta, elde edilen veriler analiz edilmekte ve bu analizler neticesinde bir sonuç çıkarılmaktadır. Bu ağ yapısı "*nesnelerin interneti*" (Internet of Things) olarak tanımlanmaktadır[63]. Nesnelerin interneti kavramı, internete bağlı olan nesnelerin bilgiyi algılayabildiği, internet aracılığıyla başka nesnelerle iletişim

[62] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", s. 22.
[63] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 21 vd.

kurabildiği ve veri paylaşabildiği, nesnelerin birbirleriyle paylaşım yaparak oluşturduğu cihazlar sistemidir[64].

Nesnelerin interneti teknolojisi canlı bir yapıdır. Bu yapıda sensörler tıpkı bir sinir hücresi gibi görev alırlar. Sensörler fiziksel aktiviteleri ve sıcaklık, ışık, basınç ve ses gibi özellikleri elektriksel sinyallere dönüştürerek veri oluştururlar. Bu veriler, ana cihazlar olan kontrolörlere ulaşır. Kontrolörler ise kendilerine ulaşan bu verileri analiz eder ve başka bir cihaz olan aktivatöre gönderirler. Aktivatör, kendisine ulaşan verileri analiz ederek nesneyi harekete geçirme kabiliyetine sahiptir[65]. Bu ekosistemde yer alan cihazlar genellikle sensörler, giyilebilir cihazlar, akıllı ev cihazları, arabalar, endüstriyel cihazlar gibi farklı türdeki nesnelerdir. IoT (Internet of Things) teknolojisi, sensörlerin ve diğer cihazların internete bağlı olması sayesinde farklı amaçlar için kullanılabilir. Örneğin, akıllı ev cihazları sayesinde ev sahibi evde olmadığı zamanlarda bile klima ortamın sıcaklığını daima oda koşullarında tutabilir, evdeki diğer cihazlar evde bulunmadan da uzaktan kontrol edebilir.

IoT teknolojisi, fiziksel altyapıdan sosyal altyapıya, ekonomik alt yapıdan teknolojik altyapıya kadar geniş bir çapta yaygın olarak kullanıldığı durumda, bu teknolojisi sayesinde bir şehir daha akıllı hale gelebilir. Akıllı şehirlerin amaçları arasında bulunan, çevresel sorunların takibi, enerjinin etkin kullanılması, şehir sakinlerini katılımının artırılması, hayat kalitesinin yükseltilmesi gibi hedeflere ulaşmak için kullanılabilecek ideal bir teknolojidir. Akıllı şehirlerin oluşması için gereken, akıllı binalar, akıllı yaşam alanları, akıllı ulaşım sistemleri, akıllı çevre gibi unsurlar IoT teknolojisi sayesinde oluşacaktır[66].

Örneğin, Şikago "*Array of Things*" isimli kentsel ölçüm projesini hayata geçirmiş ve geliştirmeye devam etmektedir. Bu projede, çevre bilimi ve akıllı şehir araştırması için gelişmiş uç bilgi işlem yeteneklerine sahip yeni bir kablosuz güdümlü sensör platformu olan "*Waggle Platformu*" kullanılarak kentsel çevre, altyapı ve faaliyetler hakkında gerçek zamanlı ve konuma dayalı veriler toplanmaya çalışılmaktadır. Bu sistem, iklim, hava kalitesi ve gürültü gibi kentsel ortamda yaşanabilirliği etkileyen faktörleri ölçen, şehir için bir "*fitness takipçisi*"ne benzetilmektedir. Bu projenin, araştırmacıların, politikacıların ve şehir sakinlerinin

[64] Taşçı, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", s. 19.
[65] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 22.
[66] Emikönel, "*Göç ve Akıllı Şehir Türkiye Uygulaması*", s. 31.

birlikte çalışmasına ve şehirleri daha sağlıklı, daha verimli ve daha yaşanabilir hale getirecek belirli eylemler gerçekleştirmesine izin verme potansiyeline sahip olduğu düşünülmektedir. Veriler, şehirlerin daha verimli çalışmasına ve kentsel sel ve trafik güvenliği gibi ortaya çıkabilecek problemleri öngörerek, önleyici tedbirler alınmasını sağlayarak maliyet tasarrufu gerçekleştirmesine yardımcı olmaktadır. AoT verileri, hava kalitesini ve sesi izleyen sensörler sayesinde şehirdeki en sağlıklı ve en sağlıksız yürüme sürelerini ve rotalarını önerebilir veya hastalıklar ile kentsel çevre arasındaki ilişki hakkında fikir verebilmektedir. Gece geç saatlerde yürümek isteyen yayaların güvenliğini artırmak için güvenli ve verimli yollar önermek veya trafik sıkışıklığından kaynaklanan kirliliği azaltmak ve yoğun trafik saatlerinde trafik ışıklarını zamanlamak için gözlem yapılabilmektedir[67].

5. Yapay Zekâ

İnsanlık tarihi boyunca insanlar makineler icat ederek kendi hayatını bu makineler yardımıyla kolaylaştırma çabası içerisinde olmuştur. Bu süreçte basit makinelerden bilgi ve iletişim teknolojilerine doğru bir evrimsel gelişme yaşanmıştır. Bugün geldiğimiz nokta itibariyle, insanlar tarafından yüklenen bilgiyle işlem yapan motorlardan, algılama yetenekleri ile kendi kendine öğrenip elde ettiği bilgilerden çıkarım yaparak kendi karar verebilen teknolojilere geçiş dönemindeyiz. Bu zamana kadar insana özgü olan öğrenme ve öğrendiğinden sonuç çıkarma yeteneği yani zekâ günümüzde makinelerin yetenekleri arasına girmeye başlamıştır. Bu yeteneğe yapay zekâ denilmektedir.

Yapay zekâ, insanın zekasıyla gerçekleştirdiği akıllı yürütme, fikir belirtme, belirttiği fikri yargılama, karar verme gibi davranışların, insan müdahalesi olmaksızın bir makine tarafından gerçekleşmesini sağlayan teknolojinin adıdır[68].

1940'larda McCulloch ve Pitts nöronların beyinde nasıl çalıştıklarını matematiksel olarak açıklayan "*Beynin Boolean Devre Modeli*" teorisi ortaya koymuşlardır. Konrad Zuse yapay zekanın programlama dili olan dünyanın ilk evrensel programlama dili olan "*Plankalkül*"ü ortaya koymuştur. 1950'li yıllarda Alan Turing "*Computing Nachinery and Intelligence*" isimli makalesinde yapay

[67] https://arrayofthings.github.io/, https://wa8.gl/
[68] Merve Melek Sarıgül, "*Yapay Zeka Teknolojilerinin Akıllı Şehirlerdeki Uygulamalarına Yönelik Bir Araştırma: Konya İli Örneği*", (Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2022), s. 8 vd.

zekanın felsefi yönünü araştıran çalışmalar yapmıştır. Yapay zekâ kavramı resmi olarak ilk defa 1956 yılında "*Dartmouth College Artificial Intelligence*" konferansında McCarthy öncülüğünde ileri sürülmüştür. 1970'lerde Amerikan İleri Savunma Araştırma Projeleri Ajansı (DARPA) tarafından ilkel bir yapay zekâ işlemcisi kullanılarak navigasyon ve harita sistemlerinin temelleri atılmıştır. 2009'da Asimo isimli, yürüyebilen, koşabilen, dans edebilen ve araba sürebilen bir robot, yapay zekanın gelişmiş örneği olarak Kaliforniya'da düzenlenen bir konferansta tanıtılmıştır. Ancak bu robotun düşünme, karar verme ve tercih etme yeteneğinin olmaması nedeniyle günümüzde yapay zekâ olarak nitelendirilmesi zor görülmektedir[69].

Birçok alanda kullanılan yapay zekâ, akıllı şehirlerde de büyük verinin elde edilmesi, yorumlanması, analiz edilmesi, sonuç çıkartılması ve karar verilmesinde kullanılabilecek, zaman ve maliyetten tasarruf sağlayacak bir araçtır. Yapay zekâ sayesinde, akıllı şebekeler oluşturulup enerji tasarrufu sağlanabilir, sensör ve kameralar sayesinde sokaklarda yaşanan kaza, yangın gibi olaylar çok kısa sürede tespit edilip müdahale edilebilir, uyarıcı levhalar yardımıyla sürücü ve yayalara en uygun rota tavsiye edilebilir, herhangi bir sorunla ilgili toplanan verilerin analiz edilip çözüm için bir karar alınmasında daha hızlı ve efektif sonuca ulaşılabilir.

II. AKILLI ŞEHİRLERDE KAMU HİZMETİ KAVRAMI VE KİMİ UYGULAMA ÖRNEKLERİ

A. Genel Olarak Kamu Hizmeti Tanımı ve İlkeleri

1. Tanım

Kamu hizmeti kavramı, siyaset bilimi, kamu ekonomisi, idare hukuku gibi multidisipliner bir kavramdır. Bu nedenle kavramın tanımı açısından bir uzlaşı bulunmamaktadır[70].

[69] Sarıgül, "*Yapay Zekâ Teknolojilerinin Akıllı Şehirlerdeki Uygulamalarına Yönelik Bir Araştırma: Konya İli Örneği*" s. 11 vd.
[70] Raziye Betül Şener, "*Kamu Hizmeti Anlayışındaki Değişim ve Akıllı Kentler*", (Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2019), s. 12.

Onar'a göre, İdare hukuku konusunu açıklamaya çalışan düşüncelerin birleştikleri kavramlardan biri olan "*kamu hizmeti*"[71], devlet veya diğer kamusal kuruluşlar tarafından ya da bu kuruluşların denetimi ve gözetiminde, toplumun genel ihtiyaçlarını karşılamak ve kamu yararını sağlamak amacıyla sürekli ve düzenli olarak gerçekleştirilen faaliyetlerdir[72].

Kişilerin ve özel hukuk kuruluşlarının üstesinden gelemeyeceği genel ihtiyaçların giderilmesi, devletin görevi ve hatta devletin var olma sebebidir. Bir ihtiyaç özel hukuk kişileri tarafından karşılanıyorsa, faaliyetin konusu, kural olarak bir kamu hizmeti değildir. Çünkü kamu hizmetinin önemli özelliklerinden biri bunun bir devlet girişimi olmasıdır. Yani kamu hizmeti faaliyetinin personel, mal ve sermayesi devlet tarafından karşılanmış ve devlet tarafından yürütülmüş olması gerekmektedir. Bir kamu hizmetinin bazen özel hukuk kişilerine gördürülmesi mümkündür. İmtiyaz suretiyle gördürülen bu hizmetlerde devlet, denetim ve gözetim yetkisine sahiptir. Bu nedenle bu tür hizmetler de kamu hizmeti mahiyetindedir[73].

Kamu hizmeti kavramı organik, maddi ve şekli olmak üzere 3 farklı bakış açısı ile tanımlanmaktadır[74]:

- Organik bakış açısına göre, hizmeti sunan kişinin kim olduğuna bakılır ve devlet tarafından sunulan hizmetler kamu hizmetidir.
- Maddi açıdan bakıldığında, hizmetin niteliği ele alınmaktadır, kamu amacı yararı taşıyan ve toplumun genel ihtiyaçlarını karşılayan hizmetler kamu hizmetidir. Bu bakış açısına göre hizmet, özel sektör tarafından yerine getirilse bile kamu hizmetidir.
- Şekli bakış açısına göre, hizmetin usulüne bakılmaktadır, kamu yönetimi usulüne göre yerine getirilen hizmetler kamu hizmetidir.

Kamu hizmetlerinin zamanın şartlarına göre yerine getirilmesi için hizmeti yerine getiren kişi ve kurumların da değişkenlik göstermesine sebep olmuştur.

---

[71] Diğer kavram da "*hakimiyet ve idari rejim*" kavramıdır.
[72] Sıddık Sami Onar, "*İdare Hukukunun Umumi Esasları"*, Marifet Basımevi, İstanbul, 1952, s. 12 ve 13.
[73] Onar, "*İdare Hukukunun Umumi Esasları*", s. 14 ve 15.
[74] Ulvi Okur, "*Kamu Hizmeti Sunan Aktörlerin Anlatılarında Kentsel Politik Mekanlar: Gazi Mahallesi Örneği*", (Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2022), s. 25.

Özelleşme süreci, idare ile bağlantılı olan kamu hizmeti kavramında organik unsurun önemini yitirmesine sebep olmuştur[75].

Kamu hizmetleri toplum ihtiyaçlarına daha kolay, daha hızlı ve sürekli olarak cevap vermesi adına genelde özel bir usul ile yerine getirilir. Kamu hizmetlerinin sahip olduğu özel bir takım ilke ve prensipler, kamu yararının özel yarardan üstün olması, çağın gerekliliğe göre değişkenlik gösteren bir teşkilatlanma ile yürütülmesi ve hizmetin sözleşmeye değil kanun ve yönetmeliğe dayanmış olması kamu hizmetini özel kılmaktadır[76].

2. Kamu Hizmeti İlkeleri

a. Süreklilik/Devamlılık İlkesi

Devamlılık ilkesi, kamu hizmetlerinin niteliğine göre, sağlık, güvenlik gibi bir kısım hizmetlerin kesintisiz bir şekilde, temizlik, ulaşım gibi bir kısım hizmetlerin de düzenli yapılmasını ifade eder. Her kamu hizmeti eşit yoğunlukta ve sürekli yerine getirilmek zorunda değildir.[77] Örneğin, toplu taşıma araçları yolcu yoğunluğuna göre günün farklı saatlerinde hizmet vermekte hatta geceleri hiç hizmet vermemektedir. Bunun yanında bir itfaiye idaresinin yılbaşında görev yapmaması düşünülemez, yılın her günü, günün her saati hizmet vermek zorundadır. Sonuç olarak devamlılık ilkesi her zaman kesintisiz olmak demek değildir önemli olan istikrarlı bir şekilde yapılmasıdır. Gülan'a göre süreklilik zaman bakımından değil "*ihtiyacın tatmini*" bakımından gereklidir. Hatta bir hizmet zaman açısından sürekli yerine getiriliyor ancak ihtiyacı tatmin etmiyorsa, süreklilik ilkesine aykırılık doğacaktır[78].

Onar, kamu hizmetlerinin devamlı ve düzenli bir şekilde yerine getirilmesinin önemini anlatırken kamu hizmetlerini, insanın yaşaması için gerekli olan kan dolaşımı, soluma ve sindirim gibi faaliyetlere benzetmektedir. Kamu hizmetlerinde

[75] Aydın Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", (Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 1987), s. 3.
[76] Onar, "*İdare Hukukunun Umumi Esasları*", s. 23 ve 24.
[77] Onur Karahanoğulları, "*Kamu Hizmeti*", 3. bs., Turhan Kitabevi, 2015, s. 191; Okur, "*Kamu Hizmeti Sunan Aktörlerin Anlatılarında Kentsel Politik Mekanlar: Gazi Mahallesi Örneği*", s. 31 vd.
[78] Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", s. 34.

yaşanan bir aksaklık toplumun buhran geçirmesine neden olması anlamına gelmektedir[79].

b. Değişebilirlilik/Uyarlama İlkesi

Uyarlama İlkesi, kamu hizmetlerinin sunumunda, içinde bulunduğumuz dönemin sosyal, teknik, teknolojik ve bilimsel imkanlarının mümkün olduğunca dikkate alınması ve hizmetin güncel gelişmelere uygun bir şekilde sunulmasını ifade eden bir kamu hizmeti ilkesidir[80].

Kamu hizmeti değişkendir, bu nedenle gelişen toplumsal ihtiyaçlara ve teknolojinin getirdiği yeniliklere kendisini uyarlamak zorundadır. Bu nedenle kamu hizmetlerinin sadece devamlı olarak yerine getirilmesi yeterli değildir[81]. Bunun yanında hizmetin toplumun ihtiyaçlarına cevap verebilmesi için gelişim sürecine uygun bir şekilde yerine getirilmesi gerekmektedir. Bu nedenle kamu hizmetlerinin işleme tarzı ve hizmeti yerine getiren kurumların yapılanmaları değişiklik gösterebilir[82]. Bu değişiklik, kamu hizmetlerinin nitelik açısından ihtiyaçları tatmin edecekte yeterlilikte olması gereğinden doğmaktadır[83].

Danıştay'ın bir kararında, *"İdarelerin; düzenleme yetkisine sahip olduğu alanlarda, uygulamaları çağın gereklerine ve toplumun ihtiyaçlarına uygun olarak değiştirip, yeniden düzenlemesi, kamu hizmetine egemen olan ilkelerden biri olan uyarlama (değişkenlik) ilkesi uyarınca hem bir görev hem de bir yetki ise de…"*[84] diyerek uyarlama ilkesini hem tanımlamış hem de bu ilkeyi kamu hizmetine egemen olan ilkelerden biri olarak belirtmiştir.

İdare, kamu görevlilerinin statüleri, hizmetten yararlanma koşulları ve hizmetin görülüş şekli açısından değişiklik yapma yetkisine sahiptir. Bu yetkinin karşısında bireyler korumasız değildir. İşlemlerin geçmişe yürümemesi ilkesi,

[79] Onar, "*İdare Hukukunun Umumi Esasları*", s. 18 ve 19.
[80]Ahmet Bağrıaçık, "*Kamu Hizmetinin Uyarlama İlkesi Üzerine Bir Değerlendirme*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 26, S. 3, 2018, s. 156.
[81] Oğuz Sancakdar, Lale Burcu Önüt, Eser Us Doğan, Mine Kasapoğlu Turhan, Serkan Seyhan, "*İdare Hukuku Teorik Çalışma Kitabı*", 11 bs., Ankara, Seçkin Yayıncılık, 2022, s. 564.
[82] Onar, "*İdare Hukukunun Umumi Esasları*", s. 19.
[83] Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", s. 35.
[84] Danıştay. 8. Dairesi. E:2009/6617, 25/12/2009.

hizmetin düzgün işlemesini talep hakkı ve idarenin hukuki denetimi, bireylere güvence sağlamaktadır[85].

Akıllı şehirler konsepti tam olarak da uyarlama ilkesi ile ilgilidir. İdare sunmuş olduğu kamu hizmetlerini daha hızlı ve verimli sunabilmek için akıllı teknolojiler ile sunduğu hizmetlere bu değişimi yansıtmak istemektedir. Akıllı şehirlerde kullanılan yapay zekâ teknolojileri bu çerçevede en önemli örneklerden biridir. Ancak burada idarenin sadece bu teknolojiyi hizmete uyarlaması yeterli değildir aynı zamanda hizmetten yararlananları da bu teknolojileri kullanabilir düzeyde eğitmesi gerekir. Bu gereklilik nedeniyle bugünkü teknolojiler kapmasında kamu hizmetini klasik tanımından ayırarak idare edilenlerin de katıldığı "*ortak hizmet sunumu*" olarak nitelendirilebileceği öğretide önerilmiştir[86].

c. Eşitlik İlkesi

Kamu hizmetlerinin yapılanması ve yürütülmesi ile hizmetlerden yararlanma açısından eşitliği ifade eder. Hizmet herkese sunulur ve herkes eşit şartlarda yararlanır[87]. Kanun önünde eşitlik ilkesinin bir neticesi olan[88] eşitlik ilkesi, sadece kamu hizmetlerinden yararlanma noktasında değil kamu hizmetlerinin her aşamasında etkisini göstermektedir.

Eşitlik mutlak değildir. Herhangi bir açıdan farklı olma durumu bir diğer ifadeyle statü farkı söz konusu olduğunda farklı rejimin uygulanması eşitlik ilkesine aykırılık teşkil etmez. Eşitlik ilkesi tarafsızlık ve meccanilik ilkelerini de doğurmaktadır[89].

Eşitlik İlkesini Anayasa Mahkemesi'nin eşitlik ilkesine yönelik verdiği kararlarda ifade ettiği gibi "*aynı durumda olanlara aynı, farklı durumlarda olanlara farklı uygulamaların yapılabileceği*" biçiminde tanımlamak gerekir[90].

---

[85] Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", s. 39.
[86] Elif Altınok Çalışkan, "*Dijital Dönüşümün Getirdiği Yeniliklerin Kamu Hizmetine Uyarlanmasında Yeni Bir Kavram Olarak 'Ortak Hizmet Sunumu' Üzerine Değerlendirmeler*", UYSAD 6th International Management and Social Research Conference, Proceeding Book, C. I, 2021, s. 485 vd.
[87] Züleyha Keskin, "*Kamu Hizmetlerinde Eşitlik İlkesi*", (Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2014), s. 80 vd.
[88] Şener, "*Kamu Hizmeti Anlayışındaki Değişim ve Akıllı Kentler*", s. 13.
[89] Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", s. 39.
[90] AYM, E. 2009/47, K. 2011/51, 17.03.2011.

d. Tarafsızlık İlkesi

Eşitlik ilkesini tamamlar nitelikte olan tarafsızlık ilkesine göre kamu politikaları bir azınlığın menfaatleri doğrultusunda değil toplumun genel çıkarı doğrultusunda belirlenmelidir[91]. Kamu hizmeti yürütülürken belirli bir kesimin yanında olmama anlamına gelmektedir[92].

e. Meccanilik İlkesi

Meccanilik ilkesi, kamu hizmetlerinin parasız olmasını ifade etmektedir. Onar'a göre kamu hizmetlerinin kamuya sunulmuş olmasının neticelerinden biri meccani olmasıdır. Kamu hizmetlerinden para alındığı takdirde hizmetlerin gelir düzeyi yüksek olan kişilere sunulduğu ve gelir düzeyi düşük kişilerin hizmetlerden istifade edemeyeceği düşüncesini akıllara getirebilir. Bu nedenle kamu hizmeti bedelsizdir. Ancak bazı kamu hizmetlerinin bir karşılığı olarak para alınması durumunda, bu para kişilerin hizmete katkısı olarak görülmektedir. Bu ücret hizmet gören kişilerin vermiş olduğu doğrudan bir vergidir. Bu ücretler meccanilik ilkesine aykırılık teşkil etmemektedir[93]. Ayrıca tüm kamu hizmetlerinin bedelsiz oluşu, hizmetten yararlanan kişiler ile yararlanmayan kişiler arasında eşitsizlik doğurmaktadır. Bu nedenle de cüzi bir miktar ücret alınması gerekebilir[94]. Kaldı ki meccanilik ilkesi, "*parasız*" olma olarak değil "*kâr amacı gütmeme*" olarak ele alınmalıdır[95].

B. Akıllı Şehir Uygulamalarının Kamu Hizmeti Tanımına Etkisi

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler hayatımızın her alanını etkilemiştir. İnsanlar çarşı pazarda alışveriş yapmak yerine mobil uygulamalar üzerinden alışveriş yapmayı tercih etmiş, doktorlar telekonferans yöntemiyle tedavi uygulamaya başlamış, çevrimiçi derslerle eğitim veren üniversiteler çoğalmış ve daha birçok alanda yaşam tarzı değişmiştir. Bu değişimden kamu hizmetlerinin etkilenmemesi düşünülemez. Kamu hizmetinin değişebilirlik ilkesi gereği, hizmetlerin sunulma şekillerinde değişimler görülmüştür.

---

[91] Okur, "*Kamu Hizmeti Sunan Aktörlerin Anlatılarında Kentsel Politik Mekanlar: Gazi Mahallesi Örneği*", s. 30.
[92] Keskin, "*Kamu Hizmetlerinde Eşitlik İlkesi*", s. 92.
[93] Onar, "*İdare Hukukunun Umumi Esasları*", s. 16 ve 17.
[94] Şener, "*Kamu Hizmeti Anlayışındaki Değişim ve Akıllı Kentler*", s. 14.
[95] Gülan, "*Kamu Hizmeti ve Görülüş Usulleri*", s. 40.

Kamu hizmetlerinde yaşanan dijitalleşme ile bürokrasi azaltılmış, şeffaflık artmış ve hizmet sunumu hızlanarak zaman kazanılmıştır. Örneğin, devlet dairesine gitmeden e-Devlet üzerinden resmi evrak alınabilmekte, interaktif vergi dairesi üzerinden borç ödenebilmekte, evden ihaleye katılabilmektedir. Bu değişim halen devam etmekte olup şehir yönetimlerinde akıllı cihazların kullanılması ve böylece hızlı bir şekilde en verimli kararı alabilmek ve hizmet sunabilmek için akıllı şehir projeleri hayatımıza girmeye başlamıştır.

Akıllı şehirlerde yaşam kalitesi artırmak için uygulamaların odak noktasında, sosyal sermayenin ana unsuru olan insan bulunmalıdır. Bu insanın, çevresindeki insanları, nesneleri, olayları ve duyguları anlamaya ve değerlendirmeye çalışan, fikirlerini beyan edebilen ve hayal gücünü kullanarak yeni ve özgün fikirler üretebilen, hayat boyu öğrenen, bilişim teknolojilerini hayatına dâhil etmiş bireyler olması gerekmektedir. Bu kapsamda, eğitim, sağlık, kültür, turizm, sanat, spor ve sosyal yardımlar gibi alanlarda verimliliği artırmak, erişilebilirliği iyileştirmek ve insanların ihtiyaçlarını karşılamak için teknolojiden yararlanılır. Şehirlerde bir arada yaşayan farklı kesimlerin kültürel etkileşimi teşvik edilir ve kültürel mirasın korunmasını amaçlanır. Akıllı şehirlerde her türlü bağımlılık, yalnızlık ve diğer problemlerin önlenmesi, mücadele edilmesi ve tedavi edilmesi için çözümler üretilir[96].

Denver'de çocuklar "*My Denver Card'* isimli kartıyla sosyal, kültürel ve sportif merkezlerden ücretsiz hizmet alabilmektedir ve restoranlardan ücretsiz bir şekilde sağlıklı olması için belli gıda standartlarında hazırlanmış öğünlerden alabilmektedirler[97]. Barcelona'da "*Vincles BCN*" projesi ile yaşlıların kendilerini daha mutlu hissetmeleri için arkadaşları ile bağlantı kurma olanağı verilmiştir[98]. Antalya'da "*Sesli Adımlar*" projesi ile görme engelli kişilere sesli navigasyon hizmeti sunularak, engelli vatandaşların hayat kalitesi artırılmak istenmiştir[99].

[96] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 23.
[97] Elif Ilgaz, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgar Enerjisinin Yönetimi ve Organizasyonu*", (Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018), s. 37.
[98] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 53.
[99] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 75.

Akıllı yönetişim uygulamaları, şehir sakinlerinin karar alma sürecine katılmaları için görüş ve tavsiyelerini dile getirebildiği, bu görüş ve tavsiyelerin karar alıcıların da görebildiği, şehir yönetiminin de şeffaflaşması için yönetim verilerinin halka açıldığı platformlardır.

Şeffaflık, hesap verebilirlik ve katılımcılık ilkelerini hayata geçirmek adına Londra'da geliştirilen "*Talk London*" isimli uygulama ile vatandaşlar güvenlik, sağlık, çevre, sanat gibi toplumu ilgilendiren konularda görüş ve önerilerini iletebilmektedir. Vatandaşların bu görüşleri yönetim tarafından dikkate alınmakta ve böylece halk karar alma mekanizmasında rol üstlenmiş olmaktadır. Halk sadece kamu hizmetlerinden faydalanan değil aynı zamanda tasarlayan da olmaktadır[100]. Aynı şekilde İstanbul için, https://inovasyon.iett.gov.tr/# adresinden insanlar toplu ulaşım araçları ile ilgili fikirlerini dile getirebilmekte ve toplu ulaşımın kalitesini artırmak için düşündükleri projelerini sergileyebilmektedir.

Barcelona'da "*açık bütçe*" isimli platform ile dileyen herkes kamu kaynaklarının ne kadar ve nereye harcandığını görebilmektedir. "*Dijital Pazar*" uygulaması ile de kamu ihaleleri herkese açık olacak şekilde yürütülmektedir. Vatandaşlar ihaleye katılan şirketlerin bilgilerine ulaşabilmektedir[101].

C. Akıllı Şehirlerdeki Kimi Kamu Hizmetlerinde Uygulama Örnekleri

1. Akıllı Sağlık Uygulamaları

Akıllı sağlık uygulamaları, bilgi ve iletişim teknolojileri yardımıyla sağlık verilerinin analiz edilmesini sağlayan, sağlık hizmetlerinin etkili ve hızlı bir şekilde yerine getirilmesini amaçlayan uygulamalardır. Toplumda bakıma muhtaç olan yaşlı ve hasta insanların bakım merkezlerine toplanıp gözlemlenmesi hizmetleri günümüzde evde bakım hizmetlerine yerini bırakmıştır. Düzenli olarak sağlık durumunun izlenmesi gereken kişilerin evine sağlık ekiplerinin gidip kişiyi muayene etmeleri hem zamanın kısıtlı olması hem yeterli personelin olmaması hem de maliyet açısından sağlık hizmeti sunan kamu görevlilerini zora sokmaktadır. Bu konuda bilgi iletişim teknolojilerinin kullanılmasıyla hem sağlık personellerinin daha az efor sarf edeceği hem de takip edilen hastanın sürekli izlenebileceği yöntemler bulmak

[100] Aygün, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", s. 54 vd.
[101] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 57.

mümkündür. Örneğin giyilebilir sensörlü ölçüm cihazları hastanın tıbbi değerleri ölçülüp, cihaz tarafından doktora mesaj gönderilmesi mümkündür. Bu yöntemle doktor da hastaları görmeden anlık olarak hastaların verilerini takip edebilmektedir. Bu şekilde hem doktor hastaları gezmek zorunda kalmamakta hem hastalar sık sık doktor tarafından rahatsız edilmemektedir. Ayrıca doktor fiziki olarak hastanın yanına günde bir kere kontrol edebilirken, akıllı sağlık uygulamaları ve cihazları sayesinde her zaman kontrol etme imkanına sahip olacaktır[102].

Singapur'da "*Yaşlıları İzleme Sistemi*" ile yaşlıların hareketlerini izlemekte, uzun süre hareket etmeyen yaşlı olduğunda tanıdıklarına veya bakıcıya uyarı gitmektedir[103]. Hindistan'da "*TelePresence*" isimli uygulamaya hastaların tıbbi bilgileri eklenmiş olup, hastaların tanı ve tedavi süreçlerinde hız kazanılması hedeflenmektedir[104]. Bursa'da "*Sevgi Çipi*" projesi ile zihinsel engelli ve Alzheimer hastası olan kişilerin üzerinde bulunan cihazlar sayesinde, hasta yakınları istedikleri her an hastalardan haberdar olabilmektedir[105].

2. Akıllı Ulaşım Uygulamaları

Akıllı şehirlerde, günlük hayatta insanların gittikleri iş merkezleri, kamu binaları, alış-veriş merkezleri, sosyal ve kültürel merkezlerin yaşam standartlarını yükseltecek şekilde birbirine bağlanması ve ulaşımda etkin ulaşım araçlarının şehir sakinlerinin hizmetine sunulması akıllı ulaşım uygulamalarının amaçlarından biridir. Bu amaca ulaşmak için otobüs, tramvay, metro ve vapur gibi toplu taşıma araçlarının birbirleriyle entegre olması önem arz etmektedir. Bu hususta şehir sakinlerinin bir yerden bir yere giderken araç tercihlerini belirlemesine yardımcı olmak için, toplu ulaşım araçlarının güzergâh, saat, aktarma noktaları, seyahat süresi gibi bilgilerine erişebilecekleri mobil uygulamalar geliştirilir. Örneğin İstanbul Büyükşehir Belediyesi tarafından geliştirilen "*Otobüsüm Nerede*" isimli uygulama ile kişiler

---

[102] Barutçu, "*Akıllı Şehirler Üzerine Sistemik Bir Literatür Taraması ve Akıllı Şehirlerde Endüstri Mühendisliği Uygulama Alanları*", s. 14.
[103] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 58.
[104] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği"*, s. 60.
[105] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 74.

gitmek istedikleri yere nasıl gidebileceklerini, yakınındaki durakları, sefer saatlerini ve otobüslerin nerede olduklarını öğrenebilmektedir[106].

Akıllı ulaşım uygulamalarından en yaygın olanı, trafik sinyalizasyon sistemlerinin trafik yoğunluğuna göre çalışmasıdır. Trafik ışıkları yoğunluğun olduğu bölgede trafik akışını hızlandıracak şekilde uzun süre yeşile dönerken, trafiğin yavaşlatılması gereken bölgelerde ise uzun süre kırmızı olmaktadır. Bir başka ifadeyle, trafik ışıklarının kaç saniye kırmızı veya yeşil yanacağı sabit olarak belirlenmemiştir, trafiğin durumuna göre değişkenlik göstermektedir. Bu teknoloji aynı zamanda polis, itfaiye, ambulans gibi geçiş üstünlüğü olan araçların veya servis, otobüs gibi öncelik verilmek istenen araçların yolunu açmak için de kullanılmaktadır. Örneğin, toplu ulaşımı teşvik etmek amacıyla Fransa'nın Toulouse şehrinde trafik ışıklarının otobüslere öncelik verecek şekilde ayarlanması neticesinde toplu taşıma araçlarının trafik ışıklarında bekleme süresi neredeyse yarı yarıya düşürülmüştür[107].

Akıllı ulaşım sistemlerinden, trafik sistemi içerisinde yaşanan aksaklıkları en kısa sürede çözüm üretecek mercilere iletmesi, konumunu değiştirmek isteyen kişilere yoğun bilgi ve alternatif yollar sunması, araçların trafik sistemi ve sürücüler ile bağlantılı olarak etkileşime girmesi beklenmektedir[108]. Örneğin, Denver'de (Amerika Birleşik Devletleri – Colorado) araçlar yakınlarında bulunan araçlarla radyo frekansları sayesinde bilgi paylaşımı yapabilmektedir. Böylece sürücüler bu bilgiler ışığında hareket etme imkanına sahip olmaktadırlar[109].

Akıllı ulaşım uygulamalarından biri de karbon emisyonlarının azaltılması için bisiklet ve hibrit araçların kullanılmasının teşvik edilmesidir. Bu kapsamda yaya ve bisikletler için güvenli yolların oluşturulması, elektrikle çalışan araçlar için şarj ünitelerinin yerleştirilmesi önem arz etmektedir. Ayrıca bisiklet kullanımını teşvik edici, insanları bisiklet kullanmaya motive edici uygulamalar ile başarılı sonuçlar elde etmek mümkündür. Örneğin, halkın yarısından fazlasının işe bisiklet ile gittiği Kopenhag'da, şehre yerleştirilen 380'in üzerinde akıllı trafik sinyali sayesinde

[106] https://www.iett.istanbul/#mobiett
[107] Savaş Muharrem Gülmez, "*Yerel Yönetimlerde Akıllı Şehir Uygulamalarının Yansımaları ve Süreç Yönetimi: İstanbul Büyükşehir Belediyesi Örneği*", (Yüksek Lisans Tezi, İbni Haldun Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul 2022), s. 31 vd.
[108] Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", s. 14.
[109] Ilgaz, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgar Enerjisinin Yönetimi ve Organizasyonu*", s. 37.

bisikletle seyahat edenlerin seyahat süresi %10 azaltılmıştır[110]. Sağlanan bu zaman tasarrufu şehir halkını bisiklet kullanma konusunda motive etmektedir.

3. Akıllı Enerji Uygulamaları

Akıllı enerji uygulamaları, enerji kaynaklarının daha verimli kullanılması, enerjinin maliyet ve tüketim açısından tasarrufu, enerjinin kesintisiz ve kaliteli bir şekilde tedarik edilmesi ve çevresel etkilere karşı hassasiyet gösterilmesi gibi amaçlayan yenilikçi teknolojileri ifade etmektedir[111]. Akıllı şehirlerin önemli hedeflerinden biri enerji kaynaklarının verimli kullanılması ile hem maliyet tasarrufu yapmak hem de kaynakları gelecek nesillere aktarmaktır. Bunun için akıllı şehirlerin yenilebilir enerji alt yapısına sahip olması gerekmektedir. Ayrıca enerjinin dağıtılması konusunda planlama yapmak için kullanım verilerini toplamak, bu verileri analiz edip politika üretmek akıllı şehir uygulamalarının amaçları arasında yer alır.

Akıllı sayaçların özelliği, kullanılan miktarın belirlenmesinde yani faturalandırma sürecinde ve abone başlangıç ve iptal işlemlerinde, sayacın bulunduğu yere hiç kimsenin gitmesine gerek kalmaksızın işlemlerin uzaktan yapılabilmesine imkân sağlamasıdır[112]. Ayrıca akıllı şebeke uygulamaları ve akıllı sayaçların sağladığı önemli faydalardan biri enerjinin verimli bir şekilde kullanılmasını sağlamaktır. Akıllı sayaçlar kullanıcıları enerji tasarrufu sağlama noktasında yönlendirici olacak şekilde uyarılar vererek insanlara tavsiye niteliğinde ipuçları sunabilmektedir. Enerji üretimi konusunda da akıllı şebeke uygulamaları, güneş ve rüzgâr enerjilerinden üretilen enerjiyi şebekeye entegre etme ve üretim taleplerini yönetme hususlarında yardımcı olabilmektedir[113].

Akıllı enerji uygulamaları kapsamında Dünyada, akıllı sokak lambalarını ilk defa uygulayan Oslo kentinde %70'e varan oranlarda enerji tasarrufunun sağlandığı görülmüştür[114]. Zhenjiang şehrinde (Çin), halk otobüslerini izleyen uygulama sayesinde, yakıt maliyetleri 2,7 milyon dolar, karbon emisyonlarını 6.700 ton

---

[110] Gülmez, "*Yerel Yönetimlerde Akıllı Şehir Uygulamalarının Yansımaları ve Süreç Yönetimi: İstanbul Büyükşehir Belediyesi Örneği*", s. 31.
[111] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 24.
[112] Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", s. 16.
[113] Ilgaz, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgâr Enerjisinin Yönetimi ve Organizasyonu*", s. 40 vd.
[114] Özsüer, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", s. 15.

azaltılmıştır[115]. İzmir'de elektrikli otobüsler kullanılmaya başlanmış olup bu otobüslerin kullandığı elektrik güneş santralinde üretilmektedir[116]. Londra'da Oxford Caddesi'ne yerleştirilen fayanslara yürüyen insanlar bastıkça, kullanılan akıllı teknoloji sayesinde insanların kinetik enerjisi elektrik enerjisine dönüştürülmekte ve caddenin lambaları bu elektriği kullanmaktadır[117].

4. Akıllı Güvenlik Uygulamaları

Akıllı güvenlik uygulamaları, veri analizi ile şehir güvenliğinin ölçümlenmesi ve etkinliğinin artırılması için tasarlanan, teknolojik altyapı ile kameralar, sensörler, akıllı cihazlar ve diğer teknolojik araçlarla donatılmış bir sistemdir. Bu sistem, şehirlerdeki şehir güvenliğine yönelik oluşabilecek tehditleri önceden tespit etmek, olası tehditlere karşı ihtiyaç duyulan önlemleri almak ve böylece etkili bir kriz yönetimini sağlamak için kullanılır[118]. Bu uygulamalar, güvenlikle ilgili verileri sürekli olarak toplayarak, analiz ederek ve raporlayarak şehir yöneticilerine ve güvenlik güçlerine anlık bilgi sağlar. Bu sayede, şehirdeki suç oranlarının izlenmesi, trafik kazalarının önlenmesi, doğal afetler veya terör saldırıları gibi olaylara hızlı ve etkili müdahale edilmesi gibi hedefler gerçekleştirilebilir.

New York, şehir güvenliğinin sağlanması amacıyla akıllı güvenlik uygulamaları kapsamında "*akustik silah sesi izleme sistemi*" kullanmaktadır. Bu sistemde sensörler bir silah sesi algıladığında olay yerine en yakın olan polis memurunun telefonunda bulunan uygulamaya bir mesaj iletilmektedir. "*IdeaScale*" isimli uygulama sayesinde halk emniyet hizmetleriyle ilgili taleplerini iletebilmekte, yorum ve değerlendirme yapabilmektedir[119]. Hindistan'da servis otobüslerine GPS yerleştirilmiş olup rotasından uzaklaşan servislere hızlı bir şekilde müdahale edilmesi için kolluk güçlerine bildirim gitmektedir[120]. Ankara-Sincan'da "*Harikalar Diyarı Akıllı Şehir Projesi*" kapsamında parklara yerleştirilen akıllı sistemler sayesince, güvenliği tehdit eden bir konu olduğunda güvenlik güçleri hemen devreye

---

[115] Ilgaz, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgâr Enerjisinin Yönetimi ve Organizasyonu*", s. 40.
[116] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 73.
[117] Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", s. 53.
[118] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 23.
[119] Ilgaz, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgâr Enerjisinin Yönetimi ve Organizasyonu*", s. 36 vd.
[120] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 60.

girebilmektedir[121]. Antalya'da oluşturulan "*Güven Çemberi*" projesi ile çocuk, yaşlı ve evcil hayvanlara bileklik takılarak, mobil uygulama üzerinden bu kişilerin ve hayvanların nerede oldukları gösterilmekte ve belirlenen alanlardan dışarı çıktıklarında ise sistem bildirim göndermektedir[122].

5. Akıllı Çevre Uygulamaları

Akıllı çevre uygulamaları, bilgi ve iletişim teknolojileri (BİT) kullanımı ile çevrenin yönetilmesi ve sürdürülebilirliğinin sağlanmasını amaçlayan, bu kapsamda çevre ile ilgili verilerin toplanması, izlenmesi, analiz edilmesi ve bu verilere dayalı kararlar alınmasını hedefleyen uygulamalardır. Bu uygulamalar sayesinde hava, su, toprak gibi doğal kaynakların yönetimi ve kontrolü daha etkin ve verimli hale getirilir[123].

Örneğin, Denver'de "*The Sustainable Neighborhoods*" isimli proje ile, mahalle sakinleri ile mahalli yöneticiler, daha yaşanabilir ve daha sürdürülebilir bir çevre oluşması için eğitim ve aktiviteler düzenlenmekte, düzenlenen bu etkinliklere katılım arttıkça mahallelere "*Katılımcı Sürdürülebilir Bir Mahalle*" veya "*Olağanüstü Sürdürülebilir Bir Mahalle*" gibi özel tabelalar asılmaktadır[124].

Amsterdam'da "*Yağmur Geçirmez*" projesi ile yağmur suyu, kullanılabilir suya çevrilmektedir[125]. Barcelona'da "*Gözlem Kontrol ve Veri Edinim Sistemi (SCADA)*" ile park ve bahçelerde, bitkilerin nem oranına göre sulama yapılmaktadır[126]. Berlin'de "*IPgarden*" uygulaması ile kişiler online olarak yani tarım arazisine gitmeden organik tohum veya bitki ekebilmekte ve sulayabilmektedir. "*Gieß den Kiez*" uygulaması ile neredeyse tüm ağaçların türü, yaşı, bakımı gibi bilgiler gösterilmekte, insanlar bu ağaçlara abone olmakta ve bu ağaçlara yerleştirilen cihazlar sayesinde yapılması gereken bakımı yapabilmektedirler[127].

---

[121] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 72.
[122] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 75.
[123] T.C. Çevre ve Şehircilik Bakanlığı, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", s. 23.
[124] Ilgaz, *"Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgâr Enerjisinin Yönetimi ve Organizasyonu*", s. 38.
[125] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 53.
[126] Özkan, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*", s. 56.
[127] Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", s. 60.

6. Akıllı Atık Yönetimi Uygulamaları

Atık yönetimi, çevre kirliliğinin önüne geçmek amacıyla atıkların tespit edilmesi, bu atıkların toplanması ve toplanan atıkların yine çevreye zarar vermeyecek şekilde ortadan kaldırılması sürecidir. Özellikle atık imha sürecinde atıkların çevreye zarar vermeyecek şekilde ortadan kaldırılması önem arz etmektedir. Atığı yakma veya toprağa gömme yöntemlerinin hava ve toprak kirliliğine sebep olduğu aşikardır. Bu nedenle atığın tekrar değerlendirmek üzere geri dönüşümü için teknolojiler geliştirilmiş ve böylece kaynak israfının da önüne geçilmiştir. Bu sürece akıllı uygulama sıfatını kazandırmak için öncelikle gerekli teknolojik cihazların sürece entegre edilmesi gerekir. Akıllı atık yönetiminden söz edebilmemiz için, atık kutularının doluluk oranlarını tespit eden ve atık kutusunun boşaltılması gerektiğinde uyarı veren sensörlerin kullanılması, atık toplamanın ve ayrıştırmanın otomatik araçlarla yapılması, toplama merkezlerinin çevreyi koruyacak şekilde modern olması, atıklardan enerji elde edilmesi mümkünse bundan faydalanılması ve bu sürecin çevre dostu olarak yönetilmesi gerekmektedir[128].

Londra'da "*Love Clean London*" uygulaması ile vatandaşlar atık süreci ile ilgili şikayetlerini, görsel dosyaları da ekleyerek yöneticilere iletme imkanına sahiptir. Bu durumda atık toplama ve çevre temizliği planlamasında bu şikayetler de göz önünde bulundurulmaktadır[129].

[128] Gülmez, "*Yerel Yönetimlerde Akıllı Şehir Uygulamalarının Yansımaları ve Süreç Yönetimi: İstanbul Büyükşehir Belediyesi Örneği*", s. 36.
[129] Doruk, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", s. 54.

İKİNCİ BÖLÜM

KAMU HİZMETİ YÖNÜYLE AKILLI ŞEHİRLERDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

I. GENEL OLARAK KİŞİSEL VERİ KAVRAMI, TANIMI, UNSURLARI, TARİHSEL GELİŞİMİ VE HUKUKSAL NİTELİĞİ

A. Kavram

Latince "*persona*" kelimesinden türetilmiş olup uluslararası literatürde "*person, persona, personne*" gibi ifadelerle karşılık bulan, "*şahıs*" olarak de tanımlanan "*kişi*" kavramı, haklara ve borçlara sahip olabilen varlığı ifade etmektedir[130]. Kişisel kavramı ise, kişiye özgü anlamına gelmektedir.

"*Veri*", tek başına herhangi bir anlam ifade etmeyen, olay ve olgularla ilgili işlenmemiş gerçeklerdir. Verinin toplama, sayma, gruplama, özetleme, eleme ve ayıklama gibi işlemlerinin elle veya bilgisayar ile işlenmesi sonucu organize edilip, anlam kazanmış haline "*enformasyon*" denir. Enformasyonun kişiselleştirilmiş yani kişiye özel haline "*bilgi*" denir. Beyine ulaşan enformasyon diğer bilgilerle işlenerek yeni bir bilgiye dönüşür[131].

Bu bilgiler ışığında kişisel veri kavramı, *"kişiye özgü olan, özgülenen kişi hakkında diğer kişilerin bilgi sahibi olmasına sebep olan şey"* olarak tanımlanabilir.

B. Tanım

6698 sayılı Kişisel Verilerin Koruması Kanunu'nda (KVKK) kişisel verinin tanımı *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*

---

[130] Ömer Ergün, "*Kişi Kavramı ve Çeşitleri*", Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi, 1/1, 2017, s. 2 vd.

[131] T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, "*Akıllı Şehirlerde Veri*", Aralık 2020. Link: https://www.akillisehirler.gov.tr/wp-content/uploads/KapasiteGelistirme/Egitim_Pdf/Akilli_Sehirlerde_Veri.pdf (Çevrimiçi Tarihi: 10.06.2023)

şeklinde yapılmıştır. Kanunda, ilerleyen bölümlerde daha detaylı bir şekilde ele alınacak olan tüm uluslararası belgelere uygun bir tanım yapılmıştır.

Anayasa Mahkemesi (AYM) içtihadında, kişisel verilerin hangi verileri kapsadığına dair *"Anayasa Mahkemesi kararlarında da belirtildiği üzere kişisel veri -belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgileri ifade etmekte olup ad, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, sağlık bilgileri, genetik bilgiler, IP adresi, e-posta adresi, alışveriş alışkanlıkları, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin kişisel veri kapsamında olduğu belirtilmektedir*." denilmektedir[132].

Yargıtay ise kişisel verileri doktrin görüşlerinden hareket ederek kişisel verileri şu şekilde sınıflandırmıştır:

- Hayat tarzına ilişkin kişisel veriler: Kişilerin ayırımcılığa maruz kalmaması ve haysiyetinin korunmasıyla ilgili olarak, dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler.
- Ekonomik ve finansal kişisel veriler: Herhangi bir suçun mağduru olmaması için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alışverişler, kredi kartlarına ilişkin veriler.
- Bilişim alanına ilişkin kişisel veriler: İnternette gezinirken bırakılan izler, dijital ortamda paylaşılan ve kayıt altına alınan bilgiler, e-posta adresi veya şifre gibi veriler.
- Sağlıkla ilgili kişisel veriler: Toplumsal statü, iş güvenliği ve sigorta kapsamını belirlemesi açısından önemli olan, sosyal yaşantı ve psikolojik durumlar hakkında bilgi veren sağlık verileri ve biyometrik veriler.
- Siyasi kişisel veriler: Kişinin ayrımcılığa maruz kalmasına sebep olacak bilgiler[133].

[132] AYM, Ali Çığır, B. No: 2015/19298, 8/5/2019, § 63
[133] Yargıtay CGK., E. 2012/1510 K. 2014/331, 17/6/2014

Görüldüğü gibi kişisel veriler hayatın her alanında karşımıza çıkabilecek bilgilerdir. Teknolojinin gelişmesi ve kullanımının yaygınlaşması nedeniyle insanların günlük hayattaki çoğu faaliyeti teknolojik cihazlarla yapılmaktadır. Dijital ortamda gerçekleşen her hareket kayıt altına alınmaktadır. Dijital ortamda tutulan kayıtlar bir kişiyle ilişkilendirilebilir nitelikleri haiz olduğu için, insanların dijital faaliyetleri hakkındaki bilgileri de kişisel veri olarak nitelendirilecektir. Bu nedenle akıllı şehir uygulamalarında teknolojik altyapısında bulunan akıllı cihaz ve sensörlerle toplanan verilerin de çoğu kişisel veri olacaktır. Akıllı ulaşım uygulamalarında kullanılan konum verileri, akıllı sağlık uygulamalarında kullanılan nabız, nefes, tansiyon gibi diğer tıbbi veriler, akıllı enerji uygulamaları kapsamında ölçülen enerji ölçüm değerleri, akıllı güvenlik uygulamaları kapsamında elde edilen ses ve görüntüler kişileri belirlenebilir nitelikte veriler olup, bu veriler kişisel veri olarak tanımlanacaktır. Ancak bunun yanında havanın nemi, ortamın sıcaklığı veya aydınlık seviyesi gibi herhangi bir kişiyle ilişkilendirilmeyen veriler kişisel veri olarak nitelendirilemez. Bu ayrımın sınırlarını net bir şekilde belirleyebilmek için kişisel veri kavramının unsurları incelenecektir.

C. Unsurları

Kişisel veri tanımına bakıldığında; kavramın "*veri*", "*kimliği belirli veya belirlenebilir bir gerçek kişi*" ve "*verinin kişiye ilişkin olması*" şeklinde üç unsurun bulunduğu görülmektedir.

1. Veri

Bir görüşe göre veri, bilgi ve enformasyon kavramları birbirinden farklı olup, birbirlerinin yerine kullanılmamalıdır. Diğer bir görüşe göre ise, bu ayrım bilişim dünyası için kabul edilebilir olsa da veri koruma hukuku açısından bu şekilde bir ayrım yapmak gereksizdir ve zordur. Bu tartışmanın hukuka olan katkısı bulunmamaktadır[134]. Kanaatimce de hukuk açısından veri ve bilgi kavramlarını farklı değerlendirmek, kişisel verileri koruma hukukunun kapsamını oldukça daraltacaktır. Kaldı ki kişisel verilerin korunması hakkının korumak istediği değerler, bilişim alanında veri olarak nitelendirilen dijital değerlerden çok daha geniştir. Kişisel

[134] Firdevs Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", (Doktora Tezi, Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü, Trabzon 2021), s. 25.

verileri koruma hukukunda korunan veriler çok çeşitli formlarda karşımıza çıkabilmektedir. Bu nedenle hukuk açısından veri ile bilgi kavramı farkı gözetilmemektedir.

Bilginin aleni veya gizli olması, öznel veya nesnel nitelikte olması, dijital veya elle tutulur olması, doğru veya yanlış olması, o bilginin kişisel veri olarak değerlendirilip değerlendirilmeyeceği noktasında önemi olmayan hususlardır[135].

2. Gerçek Kişi

Kişisel verilerin korunması hakkı kapsamında, hak sahibinin gerçek kişi veya tüzel kişi olması konusunda ayrım yapıp sadece gerçek kişilerin hakkını koruyan düzenlemeler ağırlıklı olup, ayrım yapmaksızın hem gerçek kişilerin hem tüzel kişilerin verilerinin korunabileceğini belirten düzenlemeler de bulunmaktadır. Örneğin, 28/01/1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve OECD tarafından hazırlanan Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri, ülkelere bu konuda takdir yetkisi vermiş olup ülkeleri sadece gerçek kişilerin verilerini korumakla sınırlamamıştır. İsviçre Federal Veri Koruma Kanunu tüzel kişileri de kapsamaktadır.

1982 Anayasası'nda kişisel verinin tanımı yapılmamıştır. Anayasa Mahkemesi (AYM) içtihatlarında yapılan kişisel veri tanımı KVKK'da yapılan kişisel veri tanımından bir hususta ayrışmaktadır. Anayasa Mahkemesi içtihadında *"Anayasa hükmünün lafzı, konuya ilişkin uluslararası belgeler ve karşılaştırmalı hukuk dikkate alınarak Anayasa Mahkemesi tarafından kişisel veri kavramının - belirli veya kimliği belirlenebilir olmak şartıyla- bir gerçek veya tüzel kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmiştir."* denilmektedir[136]. Görüldüğü gibi KVKK gerçek kişilere ilişkin bilgileri kişisel veri olarak tanımlasa da AYM hem gerçek hem tüzel kişiye ilişkin verileri kişisel veri olarak tanımlamıştır. KVKK kapsamında tüzel kişilerin verileri koruma kapsamına girmemekle beraber, tüzel kişilerin verileri ile bir gerçek kişiye ulaşılabiliyorsa, bu veriler koruma kapsamında olacaktır[137].

---

[135] Berat Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*" (Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2020), s. 51.
[136] AYM. Ertan Erçıktı (3), B. No: 2018/14040, 30/6/2021, § 102.
[137] Bahri Öztürk, Elif Altınok Çalışkan, Serkan Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", 2. bs, Seçkin Yayıncılık, Ankara, 2022, s. 18.

KVKK'nın gerekçesinde, bir kişinin belirli veya belirlenebilir olması, mevcut veriler ile bir gerçek kişinin ilişkilendirilerek, o kişinin tanımlanabilir duruma getirilmesini ifade ettiği belirtilmiştir. Veri, doğrudan ya da dolaylı bir şekilde kişiyi belirlenebilir kılıyorsa, o veri kişisel veridir.

3. Verinin Gerçek Kişiyle İlgili Olması

Verinin kimliği belirli veya belirlenebilir gerçek kişiye ilişkin olması demek verinin bir kişiye isnat edilebilir olması yani veri ile kişi arasında bir nedensellik bağının bulunduğu anlamına gelmektedir. Veri ile kişi arasında bir bağ yoksa, o verinin kişisel veri olarak nitelendirilmesi mümkün değildir[138].

Kişi ile veri arasında bir bağın olduğunu iddia etmek için, verinin içerik, amaç veya sonuç unsurlarından en az birinin kişi ile bağlantılı olması gerekmektedir. İçerik unsuru, verinin kişi veya kişinin faaliyeti hakkında olması ile ilgilidir. Amaç unsuru verinin, kişinin durumunu hakkında fikir yürütmek, kişiye belirli bir şekilde davranmak veya kişiyi etkilemek amacıyla kullanılmasını ifade etmektedir. Örneğin bir dairede aylık tüketilen elektrik miktarı, şehirde tüketilen elektrik miktarını tespit etmek amacıyla kullanıldığında kişisel veri değilken, o dairede mukim kişiden tüketilen elektriğin bedeli istenirken kişisel veri niteliğinde olacaktır. Sonuç unsuru, verinin kullanılmasıyla belirli bir kişinin hak ve menfaati etkilenmesiyle ilgilidir[139]. Örneğin ulaşım hizmeti sunan toplu taşıma araçlarında bulunan ve aracın konumunu gösteren GPS cihazları, otobüsün duraklardan geçme vaktini tespit etmek için kullanıldığında bu veri otobüse yani bir nesneye ilişkin bir veridir. Ancak bu veri otobüsü kullanan bir kişinin konumunu tespit etmek amacıyla kullanıldığında yani sonuç olarak belirli bir kişinin konumunu gösterdiğinde kişisel veri niteliğinde olacaktır.

Sonuç olarak kişisel veri, kullanıldığında belirli bir kişiyi diğer kişilerden ayırma fonksiyonu olan, bizi belirli bir kişiye ulaştıran veridir.

D. Tarihsel Gelişim

Arkeolojik kazılarda çıkan sonuçlar bize şunu göstermektedir ki, insanlar her dönem her ne sebeple olursa olsun elde ettikleri bilgileri kayıt altına alma ihtiyacı

[138] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 55.
[139] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 54.

duymuşladır. Yazının keşfi öncesi duvarlara resim ve figürler çizerek, yazının keşfiyle de artık yazarak çeşitli konularda izler bırakılmıştır. Devletleşmeden sonra devletler hakimiyetinde olan insanların bilgilerini kayıt altına alarak hem bu kişileri bilmek hem de bu kişilere sunula hizmetleri yürütmek amacıyla kişisel verileri toplamaya başlamışladır. Örneğin, M.Ö 2000-1750 yıllarına dair Eski Asur Ticaret Kolonileri Devri'nden günümüze kalan Asurca kil tabletlerde, Asur'dan Anadolu'ya ticaret yapmak için gelen tüccarların ticari ve hukuki sorunlarıyla ilgili kişisel verilerine rastlanılmıştır[140].

Bunun yanında insanoğlu bazı bilgilerin de gizli kalması için çabalamıştır. Sır saklama yükümlülüğünün geçmişi 2500 yıl öncesine dayanmaktadır. Bazı meslek grupları için sır saklama yükümlülüğü zorunlu kılınmıştır[141]. Örneğin, M.Ö. 5. Yüzyıldan beri günümüze kadar kabul görmüş ve kullanılan Hipokrat Yemini'nde hastalara ilişkin bilgilerin sır niteliğinde gizli kalması hususunda hekimlere yükümlülük yüklenmektedir. Bir başka örnek, kilisede görevli din adamının günah çıkarma işlemi sırasındaki sır saklama yükümlülüğü verilebilir[142].

1890 yılında Harward Law Review'de, Samuel Warren ve Louis Brandeis isimli hukukçular, kişilerin kendileriyle ilgili bilgilerinin rızaları olmaksızın üçüncü kişilerle paylaşılmaması gerektiğini vurgulayarak "*yalnız bırakılma hakkı*" (to be let alone) üzerine "*The Right to Privacy*" başlıklı makale yayınlamıştır. Makalede özel hayatın korunması ile ilişki kurularak, mahremiyete hukuki koruma getirilmesi gerektiği belirtilmiştir[143].

1950'li yıllarda bilgisayarın kullanımıyla beraber yeni tehditler ortaya çıkmıştır. Devlet kurumları ve özel kurumlar ellerindeki verileri bir platformda toplamak istemişlerdir. Veri bankaları kurma fikirleri ilk olarak, Almanya'da başlayıp dünyaya yayılmıştır. 1960'lı yıllarda İsveç'te nüfus sicili ve vergi sicili oluşturulmaya başlanmıştır. Amerika Birleşik Devletleri'nde siyasi şüphelilerin bilgilerinin toplandığına dair haberlerin çıkmasıyla, vatandaşların verilerini toplama fikrine, kişilerin yalnız bırakılma hakları ile bağdaşmayacağı ileri sürülerek karşı çıkılmıştır. Bilgisayar kullanılarak otomatik yollarla kişisel verilerin işlenmesine

[140] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 6.
[141] Büşra Merve Kılınç Sucu, "*Temel Hak Boyutuyla Kişisel Verilerin Korunması*", (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir 2022), s. 28.
[142] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 117.
[143] Kılınç Sucu, "*Temel Hak Boyutuyla Kişisel Verilerin Korunması*", s. 29.

karşı olarak tepkiler doğmuştur. Bu tepkiler bireysel olarak, kişisel verilerine sahip çıkmak adına bir savunma ve bir yurttaş hakkı olarak görülmüştür. Ancak zamanla bu bireysel çabaların yetersiz olduğu görülmüş ve bir hukuki düzenleme yapma ihtiyacı doğmuştur. Düşünülen hukuki düzenlemeden beklenen, bilgisayar kullanımından doğan zararlara çözüm bulmak ve bir denge noktası bularak devlete karşı kişisel verileri korumaktır[144].

İlk defa 1970'li yıllarda Almanya'nın Hessen eyaletinde bir düzenleme yapılmış ancak bu düzenleme eyalet seviyesindedir. 1973 yılında veri koruma kanununu ulusal düzeyde yapan ilk ülke İsveç olmuştur. 1974 yılında ABD, 1977 yılında Kanada ve Almanya, 1978 yılında Fransa, 1979 yılında Luxemburg, 1984 yılında İngiltere ulusal düzenlemelerini yürürlüğe koymuştur. 1983 yılında da Alman Anayasa Mahkemesi tarafından ilk kez kişisel verilerin korunması hakkı bir anayasal hak olarak tanınmıştır[145].

İnsan Hakları Evrensel Beyannamesi'nde ve Avrupa İnsan Hakları Sözleşmesi'nde kişisel verilerin korunması hakkı bağımsız bir hak olarak düzenlenmemiştir ancak özel hayatın gizliliği hakkı kapsamında koruma altına alınmıştır. Kişisel verileri korumayı amaçlayan ilk uluslararası belge OECD tarafından hazırlanmış olup, 23/09/1980 tarihinde kabul edilen Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri olmuştur. Uluslararası düzeyde ilk bağlayıcı olan belge ise Avrupa Konseyi tarafından hazırlanan 28/01/1981 tarihli 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi olmuştur. Söz konusu belgeler ve bu belgeleri referans alan diğer uluslararası düzenlemeler ilerleyen bölümlerde anlatılacaktır.

E. Hukuksal Niteliği

Kişisel verilerin güvenliğini sağlamakla korunmak istenen menfaatinin tespit edilmesi gerekmektedir. Bunu için de kişisel verilerin hukuki niteliği belirlenmelidir. Kişisel verilerin hukuki niteliğini tanımlamak için ileri sürülen görüşler temelde ikiye ayrılmaktadır. Kişisel verilerin korunması, ekonomik değer merkezli

[144] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 119.
[145] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 10 vd.

Amerika'da ekonomik bir hak olarak, sosyal değer merkezli Avrupa'da ise insan hakları kapsamında olan bir hak olarak değerlendirilmektedir[146].

1. Ekonomik Hak Yaklaşımı

Ekonomik faaliyetlerin temelinde bilgi ve bilgi işlem teknolojilerinin bulunduğu ekonomik modele "*bilgi ekonomisi*" denilmektedir. Müşterilerin tercihlerini tespit etmekte kullanılan kişisel veriler, talebin belirlenmesinde ve dolayısıyla arzın şekillenmesinde ciddi bir rol oynamaktadır. Bu nedenle bilgi ekonomisi modelinde kişisel veriler düşük düzeyde korunmuş, veri işlemeye getirilen sınırlamalar minimum düzeyde tutulmuştur. Çünkü sektörel çözümler kişisel verilere nazaran daha önemli görülmüştür. Bilgi ekonomisi modelinin tartışıldığı Amerika'da kişisel verilerin bir hak olarak tanınıp tanınmaması veya bir hak ise bu hakkın hukuki niteliğinin ne olacağı konusunda fikir ayrılıkları vardır. Kişisel verileri bir hak olarak görenler de mülkiyet hakkı veya fikri mülkiyet hakkı olarak iki farklı görüşe ayrılmaktadır[147].

a. Mülkiyet Hakkı Görüşü

Mülkiyet hakkı görüşünü savunanlara göre, günümüz teknolojisinin geldiği son konumda bir veri pazarı oluşmuş, bu pazarda kişisel veriler de bir ticari değer kazanmıştır. Tüketici profillerinin ve tüketim alışkanlıklarının tespitinde, üretim politikasının belirlenmesinde hatta reklam faaliyetlerinin çeşitlenmesinde kullanılan kişisel veriler, çağın petrolü olarak nitelendirilmektedir. Bu nedenle kişisel verilerin kullanılması karşısında ilgili kişiye bir bedel ödenmelidir. İlgili kişi kişisel verilerini açıklama veya satma konusunda takdir yetkisine sahiptir. Veri sahibi sattığı kişisel verilerin karşılığı olarak bir bedel kazanırken, verileri satın alan kişi de bunlara bir bedel ödediği için verileri korumak isteyecektir. Böylece kişisel verilerin korunma mekanizması ortaya çıkacaktır. Ayrıca bu mekanizmanın işlemesi için yeni bir sistem de kurulmasına gerek yoktur çünkü ilgili kişi, kişisel verilerinin izinsiz

[146] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 66.
[147] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 67.

kullanımından kaynaklı çıkan uyuşmazlıklarda mülkiyet hakkından doğan davalara başvurarak hakkını arayabilecektir[148].

Mülkiyet hakkı görüşüne bazı hususlarda eleştiriler getirilmektedir. Öncelikle, mülkiyet hakkının, malikin zilyet olduğu şeyler üzerinde tesis edilebildiği, veri sahibinin ise kişisel verilerin zilyedi olmadığı ve veri kavramının soyut olduğu bu nedenle verinin mülkiyet hakkının konusu olamayacağı belirtilmektedir. Ayrıca mülkiyet hakkının, doğada sınırlı olan kaynakların dağılımını amaçladığını, kişisel verilerin ise kıt kaynaklı bir değer olmadığı, bu nedenle kişisel verilerin bir mal olarak görülmesinin, mülkiyet hakkının varoluş amacına uygun bir yaklaşım olmadığı görüşü de ileri sürülmektedir[149].

Kanaatimce, kişisel verilerin ekonomik değer kazandığı inkâr edilemez bir gerçektir. Ancak kişisel veriler bir mal gibi devir işlemine tabi olamaz. Kişi maliki olduğu eşyayı bir bedel karşılığı satıp yeni malike devrettiğinde o eşya üzerinde kullanma, yararlanma ve tasarrufta bulunma haklarını da kaybeder. Çünkü eşya artık elinde değildir yani kişi artık zilyet değildir. Ancak veri sahibinin kişisel verisini bir bedel karşılığı bir başka kişiye satmış olması durumunda, veri sahibin malik olma sıfatını kaybetmemektedir. Söz konusu kişisel veri hala ilgili kişinin kişisel verisidir. Veri sahibi aynı veriyi kendisi de kullanabileceği gibi aynı şekilde başkalarına da bedel karşılığı satabilir. Kişisel veriyi kullanma yetkisi birbirinden habersiz birçok kişiye verilmiş olabilir. Kişisel verilerin ilgili kişiden ayrılamaz oluşu ve verilerin çoğaltılabilmesi mülkiyet hakkıyla bağdaşmamaktadır. Bu nedenle kişisel verileri, ekonomik değer nedeniyle mülkiyet hakkı kapsamında değerlendiren görüşe katılmak mümkün değildir.

b. Fikri Mülkiyet Hakkı Görüşü

Fikri mülkiyet hakkı görüşünü savunanlar, fikri mülkiyet hakkının da bir bilginin korunmasını amaçladığını, kişisel verilerin korunması hakkının da bir bilginin korunmasını amaçladığını, bu benzerlik nedeniyle fikri mülkiyet hakkı ile bağlantı kurulması gerektiğini savunmaktadır. Bu görüşü eleştirenler ise, fikri mülkiyet hakkının koruduğu eserin bir çaba ile ortaya konulan bir değer olduğunu,

[148] Elif Küzeci, "Kişisel Verilerin Korunması", (Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2010), s. 69 vd.; Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 69

[149] Elif Küzeci, "Kişisel Verilerin Korunması", s. 71 vd.; Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 69.

kişisel verilerin ise çabasız bir şekilde kişiye bağlı olarak ortaya çıkan bir değer olduğunu, korunan değerlerin benzerlik göstermediğini dile getirmektedirler. Ayrıca fikri mülkiyet hakkının, kişilere bir eser ortaya koymaları için bir teşvik niteliğinde olduğu ancak kişisel verilerin korunmasında herhangi bir konuda teşvik amacı bulunmadığı gerekçesiyle aslında aynı amaca hizmet etmedikleri de söylenmektedir[150]. Her ne kadar her iki hak da bir bilginin korunmasını ve dağılmasını kontrol altına almayı amaçlasa da bilgiler arasında olan nitelik farkı, fikri mülkiyet hakkı görüşünü haklı kılmamaktadır.

2. İnsan Hakkı Yaklaşımı

Amerika hukuku kişisel verilerin güvenliğine ekonomik bir hak olarak yaklaşmış ve minimum düzeyde koruma sağlamış olsa da buna karşı olarak Avrupa hukuku kişisel verilerin güvenliğine insan hakları nazarından bakmaktadır. Kişisel verilerin korunması hakkı insan hakları belgelerinde doğrudan bağımsız bir hak olarak tanımlanmamış olsa da bağlantılı haklar kapsamında korunmaya alınmıştır. Teknolojinin gelişmesiyle kişisel veri kavramının önemi arttıkça ülkeler anayasalarında, kişisel verilerin korunmasını hakkını bağımsız bir hak olarak düzenlemeye gitmişlerdir. Örneğin ülkemiz 2010 yılında yapılan referandum neticesinde Anayasa'nın 20. maddesine 3. fıkrayı eklemek suretiyle kişisel verilerin korunmasını hakkını bağımsız bir hak olarak düzenlemiştir.

Kişisel verilerin güvenliğini bir insan hakkı kapsamında ele alınırken, konunun insan onuru, kişilik hakkı, özel hayatın gizliliği, fikir hürriyeti, din ve vicdan özgürlüğü, haberleşmenin gizliliği, bilgi edinme hakkı ile bağlantıları ilerleyen bölümlerde değerlendirilecektir.

[150]Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 86.

II. KİŞİSEL VERİLERİN KORUNMASI HAKKINA İLİŞKİN ULUSAL VE ULUSLARARASI DÜZENLEMELER

A. Ulusal Düzenlemeler

1. Anayasa

1982 Anayasası'nın 2010 tarihli değişikliğinden önce "*kişisel verilerin koruması hakkı*" münhasıran düzenlenmiş bir hak değildi. Kişisel verilerin koruması hakkı; hukuk devleti ilkesi (m.2), bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17), özel hayatın gizliliği hakkı (m.20), konut dokunulmazlığı (m.21), haberleşmenin gizliliği ilkesi (m.22), dini ve vicdani kanaat hürriyeti (m.24), düşünce ve kanaat hürriyeti (m.25) gibi hak ve hürriyetleri düzenleyen bu maddelere dayanılarak korunmaktaydı. 2010 yılında yapılan referandum ile Anayasa'nın 20. maddesine *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"* hükmü eklenerek kişisel verilerin korunması hakkı, diğer temel hak ve özgürlüklerden bağımsız olarak düzenlenmiştir[151].

Anayasa hükmü, sadece kişisel verilerin korunmasını değil bunun yanında ilgili kişinin kendisi hakkında veriyle ilgili olarak bilgi edinme, erişme, düzeltme veya silme talep etme ve veri kullanımının amacın sınırları içerisinde kalıp kalmadığı öğrenmeyi de kişisel verilerin korunması hakkı kapsamında değerlendirmiştir. Yapılan düzenlemede kişisel verinin tanımı yapılmamıştır ancak zaten doktrinde ve yargı kararlarında kişisel verilerin ne olduğu hususunda tartışma bulunmamakta yani bir fikir birliği bulunmaktadır. Bu nedenle kişisel verinin tanımının yapılmamış olması bir eksiklik değildir[152].

Kural olarak kişisel verilerin korunması esastır yani kişisel verilerin işlenmesi yasaktır ancak istisnai hallerde kişisel veriler işlenebilir. İstisnai hallerin neler olduğu

[151] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 146 vd.
[152] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 290 vd.

yani kişisel verilerin korunması hakkının sınırları anayasa hükmünde belirtilmiştir. Düzenlemeye göre kişisel veriler ancak kişinin açık rızasıyla veya kanuni düzenleme ile işlenebilir. Yapılan düzenlemede hakkın sınırlarının kanun ile ortaya konulacağı belirtilmiş ancak anayasal sınır çizilmemiştir. Bir başka ifadeyle, Anayasa bu hak açısından basit yasa kayıtlı sınırlama yaparak sınırların tespiti için kanun koyucuya takdir yetkisi bırakmıştır. Bu açıdan, yapılan düzenlemenin *"Temel hak ve hürriyetlerin sınırlanması"* başlıklı Anayasa'nın 13. maddesi ile çeliştiği değerlendirilmektedir. Çünkü Anayasa m.13'te temel hak ve özgürlüklerin, düzenlendiği maddelerde belirtilen sebeplere bağlı olarak sınırlandırılabileceği düzenlenmiştir ancak kişisel verilerin korunması hakkı için sınırlama sebepleri belirtilmemiştir. Her ne kadar özel sınırlama rejimi ortaya konulmamışsa da Anayasa m.13'te belirtilen genel sınırlama rejimi bu hak için de uygulanacaktır. Kişisel verileri koruma hakkı, *"Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı"* olarak sınırlandırılamaz. Ayrıca Anayasa Mahkemesi kararlarında belirtildiği gibi, her hakkın özü kendi sınırını oluşturmaktadır. Tüm bunların yanı sıra, yukarıda da bahsedildiği gibi kişisel verilerin korunması hakkı bağımsız olarak düzenlenmeden önce başka haklar ile temellendirilmekteydi. Bu hakların düzenlendiği maddelerde belirtilen sınırlama sebeplerine bağlı olarak hareket edilmesi gerektiği de düşünülmektedir[153].

2. Kişisel Verilerin Korunması Kanunu

Yukarıdaki bölümde de anlatıldığı gibi, 1982 Anayasası'nda 2010 değişikliği öncesinde de kişisel veriler koruma altındaydı ancak 2010 değişikliği ile bağımsız bir hak olarak tanımlanmıştır. Kanuni düzenlemeler açısında da bakılacak olursa, Türk Ceza Kanunu, İş Kanunu, Polis Vazife ve Salahiyetleri Kanunu gibi ve başkaca kanunlarda kişisel veriler koruma altına alınmıştı. Her kanun, kendi düzenleme alanı kapsamında veri koruması sağlamaktaydı yani bir bütün olarak kişisel verileri koruyan bir kanun 2016 yılına kadar yoktu. Devlet-birey ilişkilerinde kişisel verilerin korunması, insan hakları açsından önemli bir seviyedir ancak yetersizdir. Çünkü kişisel verilerin bire-birey arası ilişkiler de korunması gerekmektedir. OECD ve Avrupa Konseyi tarafından hazırlanan belgeler 1980li yıllardan itibaren uygulamaya

[153] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması", 150 vd.; Yüzbaşı Tobaz, "Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 291 vd.

konulmuş ve devletler bu belgeler doğrultusunda iç hukuklarında düzenlemeler yapmıştı. Türkiye'nin 2016 yılına kadar düzenleme yapmaması, dünya devletleri ile veri paylaşımı konusunda sorun çıkarmaktaydı. Nitekim Avrupa Birliği uyum sürecinde de Türkiye'den beklenen hususların biri de kişisel verileri koruma konusunda düzenleme yapılmasıydı. Dış baskıların yanı sıra içerde de kişisel verilerin korunmamasından dolayı kriz olan birçok olay yaşanmıştı. Devlet kurumları tarafından dijital ortama taşına bilgilerin yetkisiz olarak erişilip internette yayınlanması, yetkisiz erişim olmasa bile devlet kurumlarının açıklaması gereken bilgileri herkesin göreceği şekilde açıklaması, devlet kurumlarının veya özel kuruluşların sahip oldukları kişisel verileri başka kurum ve kuruluşları ile paylaşmaları, kişisel bilgilerini vermek istemeyen kişilere hizmet sunmayan özel kuruluşların varlığı gibi daha birçok sorun yaşanmaktaydı. Kişisel verileri koruyan özel bir kurum olmadığı için yaşanan bu sorunları hukuki ve ekonomik sorunları beraberinde getirmekteydi. Bu duruma engel olmak için kişisel verileri koruyan ayrı bir kanuni düzenleme çalışmaları başlamıştır. Uzun süren çalışmalar ve konjektürel nedenlerle yaşanan aksamalar nedeniyle bir türlü hayata geçirilemeyen çalışmalar nihayet 24 Mart 2016 tarihinde TBMM' de kabul edilen, 7 Nisan 2016 tarihinde de Resmî Gazete'de yayımlanarak yürürlüğe giren 6698 Sayılı Kişisel Verilerin Koruması Kanunu ile neticelenmiştir[154].

Kişisel Verilerin Koruması Kanunu'nda yer bakımından yetki düzenlemesi bulunmamaktadır. Bu nedenle yer bakımından kapsamın, mülkilik ilkesi gereği belirlenmesi gerekir. Bir başka ifadeyle kanun, Türkiye'de işlenen veriler için uygulanacaktır. Zaman açısından kapsama bakarsak, kanun yürürlüğe giriş tarihi 7 Nisan 2016 tarihinden itibaren uygulanacaktır. Bu tarihten önce işlenen kişisel verilerin 7 Nisan 2018 tarihine kadar kanuna uygun hale getirilmesi gerektiği, kanuna aykırı olan kişisel verilerin silme, yok etme veya anonim hale getirilmesi gerektiği düzenlenmiştir. Ayrıca hukuka uygun olarak daha önce alınan rızalar da 7 Nisan 2017 tarihine kadar, aksi beyan edilmedikçe kanuna uygun alınmış rıza beyanı olarak kabul edilmiştir[155].

[154] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 294 vd.
[155] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 304 vd.

Kanun kapsamında gerçek kişilerin verileri korunmuştur. Tüzel kişilerin verileri korunmamıştır ancak tüzel kişilerin verileri, gerçek kişilerle ilişkilendirilebilirse bu veriler koruma kapsamı dahilinde olacaktır. Veri işlemenin kamu sektörü tarafından veya özel sektör tarafından yapılmış olması kapsamı değiştirmeyecektir çünkü kanun veri işleyen kamu sektöründen de olsa özel sektörden de olsa işlenen veriler kanun kapsamındadır. Veri işleme yöntemi açısından hem otomatik yolla işlenen veriler hem de otomatik olmayan yollarla işlenen veriler kanun kapsamındadır. Ancak veri işleme faaliyetinin bir veri kayıt sistemi dahilinde işlenmesi gerekmektedir. Gelişigüzel bir şekilde belirli bir sistematiği olmaksızın, dosyalama olarak nitelendirilmeyecek veri yığınları kanun kapsamında değildir[156].

Konu bakımından kanun istisnalar getirmiştir. Kişinin kendisi veya aile fertleri ile ilgili faaliyetlerde işlenen veriler; araştırma, planlama ve istatistik gibi amaçlarla resmi istatistik ile anonimleştirilen veriler; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenen veriler; millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenen veriler; soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenen veriler, kanun kapsamında olmayıp tam istisna olarak görülen hallerdir. Ayrıca kısmi istisna halleri olarak nitelendirilen, veri sorumlusunun aydınlatma yükümlülüğü ile sicile kayıt yükümlülüğüne istisna getirilen durumlar da kanunda sayılmıştır. Bu haller, suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olan veriler; ilgili kişinin kendisi tarafından alenileştirilmiş kişisel veriler; görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olan veriler; bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olan verilerin

[156] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı",* s. 26.

işlenmesi durumlarıdır. Bu istisnai haller veriyi kişisel veri olmaktan çıkarmaz sadece kanun hükümlerinin uygulanmayacağı anlamına gelmektedir[157].

3. Diğer Kanunlar

5237 sayılı Türk Ceza Kanunu'nun (TCK) 135. maddesinde, kişisel verilerin kaydedilmesi, 136. maddesinde, verileri hukuka aykırı olarak verme veya ele geçirme, 138. maddesinde, verileri yok etmeme filleri suç olarak düzenlenmiştir. Ayrıca TCK'nın 140. maddesinde bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik tedbiri uygulanacağı hüküm altına alınmıştır.

5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 80. maddesinde, madde 75, 76 ve 78'e göre yapılan vücuttan kan ve benzeri biyolojik örnek alma, saç, tükürük, tırnak gibi örnek alma, iç beden muayenesi, moleküler genetik incelemeler neticesinde elde edilen verilerin, kişisel veri niteliğinde olduğu, başka bir amaçla kullanılamayacağı ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemeyeceği düzenlenmiştir.

4721 sayılı Türk Medeni Kanunu'nun (TMK) 23, 24 ve 25. maddeleri kapsamında kişiliğin korunması düzenlenmiş olup, kişisel verilerin korunması da bu kapsam da değerlendirilmektedir.

4857 sayılı İş Kanunu'nun 75. Maddesi'nde işverenin işçi özlük dosyası düzenleme yükümlülüğü düzenlenmiştir. İlgili maddede *"İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."* denilerek işçinin kişisel verilerine koruma sağlanmak istenmiştir.

6098 sayılı Türk Borçlar Kanunu'nun Hizmet Sözleşmesi'ni düzenleyen hükümleri arasında "*İşçinin Kişiliğinin Korunması*" başlıklı düzenlemeler altında "*Kişisel verilerin kullanılmasında*" başlıklı 419. maddede *"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir*." denilmektedir.

4982 sayılı Bilgi Edinme Kanunu'nun "*Özel hayatın gizliliği*" başlıklı 21. maddesi "*Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği*

[157] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", s. 27 vd.

kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir." şeklinde düzenlenmiştir.

213 sayılı Vergi Usul Kanunu'nun "Vergi Mahremiyeti" başlıklı 5. Maddesine göre, *"vergi muameleleri ve incelemeleri ile uğraşan memurlar, vergi mahkemeleri, bölge idare mahkemeleri ve Danıştay'da görevli olanlar, Vergi kanunlarına göre kurulan komisyonlara iştirak edenler ve vergi işlerinde görev alan bilirkişiler"* görevleri dolayısıyla öğrendikleri sır ve bilgileri görevlerinden ayrılsalar dahi ifşa edemez ve kendileri ya da üçüncü şahıslar yararına kullanamazlar. Bu yasak, sayıla görevliler görevden ayrılsa dahi devam eder.

5809 sayılı Elektronik Haberleşme Kanunu'nun 12. maddesi işletmecilere kişisel veri ve gizliliğin korunması yükümlülüğünü yüklemektedir. Kanunun 55. maddesi *"...abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz.*" şeklinde ve 56. maddesi de "*Abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz.*" şeklinde düzenlenmiştir.

5070 sayılı Elektronik İmza Kanunu'nun "*Bilgilerin Korunması*" başlıklı 12. maddesi, elektronik sertifika hizmet sağlayıcısının, elektronik sertifika talep eden kişiden gerekli bilgiler dışında başka bilgi talep edemeyeceği ve bu bilgileri kişinin izni olmadan elde edemeyeceği, sertifikayı erişilebilir ortamlarda saklayamayacağı, sertifika sahibinin onayı olmadan bilgileri üçüncü kişilere iletemeyeceği ve başka amaçlar için kullanamayacağı şeklinde düzenlemeler içermektedir.

B. Uluslararası Düzenlemeler

1. Birleşmiş Milletler Tarafından Yapılan Düzenlemeler

İnsan haklarının tanınması ve korunması bakımından önemli bir değeri bulunan, 10 Aralık 1948 tarihinde Birleşmiş Milletler Genel Kurulu'nda kabul edilen İnsan Hakları Evrensel Bildirgesi'nin 12. maddesinde *"Hiç kimsenin özel yaşamına, ailesine, konutuna ve haberleşmesine keyfi olarak karışılamaz, onur ve ününe saldırılamaz. Herkesin bu tür karışma ve saldırılara karşı yasal korunma hakkı vardır"* hükmü bulunmaktadır. Kişisel verilerin korunması hakkı şeklinde ayrı bir hak düzenlenmemiş olsa da kişisel verilerin korunması 12. madde kapsamında değerlendirilmiştir[158].

BM Genel Kurulu'nun 16 Aralık 1966 tarihli kararıyla kabul edilen Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin "*Mahremiyet Hakkı*" başlıklı 17. maddesinde *"1. Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. 2. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir."* denilmektedir. Türkiye Sözleşme'yi 15 Ağustos 2000 tarihinde imzalamış ve Sözleşme ülkemiz bakımından 23 Aralık 2003 tarihinden itibaren hüküm doğurmaya başlamıştır[159]. Bu Sözleşmede de kişisel verilerin korunması ayrı başlıkta ele alınmamıştır ancak 17. madde kapsamında olduğu kabul edilmektedir.

BM'nin Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri, 14 Aralık 1990 tarihli 45/95 sayılı Genel Kurul kararıyla kabul edilmiştir. Rehberdeki ilkeler şu şekildedir:

1- Hukuka Uygunluk İlkesi: Kişisel veriler yasa dışı yollarla toplanmamalı veya işlenmemeli, Birleşmiş Milletler Şartı'nın amaçlarına ve prensiplerine yani temel hak ve hürriyetlere aykırı amaçlar için kullanılmamalıdır.

2- Doğruluk İlkesi: Kaydedilen verilerin doğru olup olmadığı sorumlu kişilerce düzenli olarak kontrol edilmelidir. Veriler eksiksiz tutulmalı ve elde tutulduğu süre boyunca güncel olmalıdır.

---

[158] Murat Volkan Dülger, "*Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması*", Yaşar Hukuk Dergisi, C.1 S.2 (2019), s. 75.

[159] https://insanhaklarimerkezi.bilgi.edu.tr/tr/content/117-medeni-ve-siyasi-haklara-iliskin-uluslararas-sozlesme/ (Çevrimiçi Tarihi: 20.05.2023)

3- Belirli Amaç İlkesi: kişisel verilerin elde edilmesi belirli ve meşru bir amaç doğrultusunda olmalı ve bu amaç ilgili kişiye bildirilmelidir. Kaydedilen kişisel veriler amaca uygun ve yeterli olmalı, ilgili kişinin rızası dışında amacına aykırı bir şekilde kullanılmamalı ve ifşa edilmemeli, verileri tutma süresi de amaçla orantılı olmalıdır.

4- İlgili Kişilerin Erişimi İlkesi: Kişisel verilerin sahibi olan kişiler, kendileri hakkında veri işlenip işlenmediğini öğrenme, bu verileri makul bir süre içerisinde ve makul bir ücretle kendisine verilmesini isteme, veriler hukuka aykırı elde edilmiş, yanlış veya gereksiz ise silinmesini ve düzeltilmesini isteme, verilerin kiminle paylaşıldığını öğrenme hakkına sahip olmalıdır.

5- Ayrımcılık Yapmama İlkesi: Irk veya etnik köken, renk, cinsel yaşam, siyasi görüş, dini, felsefi ve diğer inançlar, bir dernek veya sendikaya üyeliği gibi, keyfi ayrımcılığa neden olabilecek veriler toplanmamalıdır.

6- Sınırlama Yetkisi: Yukarıda sayılan ilkelere, ulusal güvenlik, kamu düzeni, kamu sağlığı veya ahlakın korunması, diğer kişilerin hak ve özgürlüklerini korumak amacıyla istisna getirilebilir. Ancak bu istisnaların sınırları açıkça belirtilmiş ve uygun güvenceleri içeren bir kanunla düzenlemesi gerekmektedir. Ayrımcılık yapmama ilkesinin istisnası, bu şartlara ilaveten insan haklarının korunması ve ayrımcılığın önlenmesine dair hazırlanan belgelere uygun olmalıdır.

7- Güvenlik İlkesi: Kişisel veriler kazara silinme, izinsiz erişim, kötüye kullanma, virüs bulaşma gibi risklere karşı korunmalıdır.

8- Denetim ve Yaptırım: Yukarıda sayılan ilkele uyulmasını denetlemek amacıyla bağımsız, tarafsız ve teknik yeterliliğe sahip yetkili bir makam belirlenmelidir. İlkelerin ihlal edilmesi durumunda bireysel çözümlerle birlikte cezai veya diğer yaptırımlar öngörülmelidir.

9- Sınır Ötesi Veri Akışı: Ülkelerin yasaları, gizliliğin korunması için benzer güvenceler sunuyorsa ülkeler arası veri akışı mümkün olmalıdır. Karşılıklı güvenceler bulunmuyorsa veri dolaşımının sınırlanması veri gizliliğinin korunması gerektiği ölçüde olmalıdır.

10- Uygulama Alanı: Belirtilen ilkeler tüm kamu ve özel bilgisayarlı dosyalara uygulanır, isteğe bağlı olarak manuel dosyalara uygulanabilir hale

getirilerek kapsam genişletilebilir. Özellikle bireylerle ilgili bazı bilgiler içerdiklerinde, tüzel kişiler hakkındaki dosyalar için de uygulanacak şekilde genişletilebilir.

İlkeler ortaya konulduktan sonra bu ilkeleri uluslararası kuruluşlar tarafından da uygulanması gerektiği belirtilmiştir.

2. OECD Tarafından Yapılan Düzenlemeler

İkinci Dünya Savaşı'ndan sonra Avrupa'nın yeniden inşası için kurulan Avrupa Ekonomik İşbirliği Teşkilatı (OEEC), 14 Aralık 1960'ta Paris'te imzalanan ve 30 Eylül 1961'de yürürlüğe giren antlaşma ile Ekonomik İşbirliği ve Kalkınma Örgütü'ne (OECD) dönüşmüştür. Kurulduğu günden beri OECD (Organisation for Economic Co-operation and Development), dünya çapında daha fazla refah sağlamayı amaçlamış ve bunun için hükümetlere dayanıklı, kapsayıcı ve sürdürülebilir büyümeyi destekleyen politikalar konusunda tavsiyelerde bulunmuştur. Küresel çapta politika izleyen diğer uluslararası kuruluşlarla yakın iş birliği yaparak yeniliklerin ilerlemesine ve küresel sorunların çözülmesine yönelik ufuk açıcı çalışmalar yürütmektedir. OECD, refah ve gelir eşitsizliğini gündeme getirmek, vergi iş birliği yoluyla daha adil toplumlar inşa etmek, dijital dönüşümün ve yeni teknolojilerin etkilerinin anlaşılması için ülkelere destek sağlamak gibi çalışmalar yapmaktadır[160].

Yeni teknolojiler yaşama ve çalışma şeklimizi değiştirirken, OECD de dijitalleşmenin faydalarının geniş çapta paylaşılmasını sağlamak için hükümetlere veri gizliliği, dijital refah, çevrimiçi alışveriş veya yapay zeka konularında politika tavsiyeleri vermektedir[161]. OECD'nin veri yönetişimi ve gizliliği konusundaki çalışmaları, OECD Dijital Ekonomi Politikası Komitesi'ne (CDEP/ Committee on Digital Economy Policy) bağlı olan Dijital Ekonomide Veri Yönetişimi ve Gizliliği Çalışma Grubu (DGP/ Working Party on Data Governance and Privacy in the Digital Economy) tarafından yürütülmektedir. OECD kişilerin güvenliklerini, onurlarını, düşünce ve ifade özgürlüklerini güvence altına aldığı için mahremiyete önem vermektedir.

[160] https://www.oecd.org/60-years/ (Çevrimiçi Tarihi: 07.05.2023)
[161] https://www.oecd.org/60-years/timeline/#selectorBlock (Çevrimiçi Tarihi: 07.05.2023)

a. Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri

Bu kapsamda yapılan çalışmalar 1970'lerde başlamış olup çalışmaların ilk meyvesi 23/09/1980 tarihinde kabul edilen Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri (Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data) olmuştur. 1980 İlkeleri, kişisel verilerin artan kullanımından kaynaklanan endişeleri ve sınır ötesi bilgi akışına yönelik kısıtlamalardan kaynaklanan küresel ekonomiler üzerindeki riski ele almak için kabul edilmiştir. Bu ilkeler, uluslararası düzeyde üzerinde anlaşmaya varılan ilk gizlilik ilkeleri olup başta OECD üyesi ülkeler olmak üzere birçok ülkede yapılan yasal düzenlemeleri etkilemiştir. Bununla birlikte, kişisel veri kullanımındaki değişiklikler ve gizliliğin korunmasına yönelik yeni yaklaşımlar nedeniyle 11/07/2013 tarihinde güncellenmiştir.

Bu ilkeler hukuki açıdan tavsiye niteliğinde olup şu şekildedir:

1- Sınırlı Toplama İlkesi: Kişisel verilerin toplanmasına ilişkin sınırlamalar olmalı, veriler yasal, adil olarak ve gerekirse veri sahibinin bilgisi ve onayı ile elde edilmelidir.
2- Veri Kalitesi İlkesi: Kişisel veriler, kullanım amaçlarıyla ilişkili olmalı ve bu amaçlar için gerektiği kadar doğruluk, bütünlük ve güncellik özelliklerini muhafaza etmelidir.
3- Belirli Amaç İlkesi: Kişisel verilerin toplanma amaçları, en geç veri toplama sırasında belirtilmeli, veri toplandıktan sonraki kullanımlar bu amaçla sınırlı olmalıdır.
4- Sınırlı Kullanım İlkesi: Kişisel veriler, ilginin rızası veya kanun verdiği yetkiyi kullanma hallerinde dışında, toplanma amacına aykırı olarak ifşa edilmemeli, erişebilir olmamalı veya başka amaçla kullanılmamalıdır.
5- Veri Güvenliği İlkesi: Kişisel veriler, verilerin kaybı veya yetkisiz erişim, imha, kullanım, değişiklik veya ifşa gibi risklere karşı makul güvenlik önlemleriyle korunmalıdır.
6- Açıklık İlkesi: Kişisel verilere ilişkin gelişmeler, uygulamalar ve politikalar hakkında genel bir açıklık politikası olmalı ve bu politikaya uygun olarak denetim araçları hazır olmalıdır.

7- Bireysel Katılım İlkesi: Bireylere, kendileri hakkında veri olup olmadığına dair teyit alma, kendileri hakkındaki bilgilerin makul bir süre içerisinde, makul bir ücret karşılığı, makul bir şekilde ve anlaşılır biçimde kendilerine verilmesini isteme, bu istek reddedildiği takdirde ret gerekçesini öğrenme ve karara itiraz edebilme, kendileri ile ilgili verilerin silinmesini, düzeltilmesini, tamamlanmasını veya değiştirilmesini sağlama haklarına sahip olmalıdır.
8- Hesap Verebilirlik İlkesi: Veri sorumlusunun, belirlenen ilkelere uygun hareket edip etmediğinin denetimi yapılmalıdır.

Ortaya konulan bu sekiz ilkeye ilaveten, bir veri denetleyicisinin bir gizlilik yönetimi programına sahip olması gerektiği belirtilmiştir. Bu gizlilik yönetimi programı, yapılan işlerin yapısı, ölçeği, hacmi ve hassasiyetine uygun olarak düzenlenmiş, mahremiyet risk değerlendirmesine dayalı olarak uygun koruma önlemleri sağlayan, yönetişim yapısına entegre edilmiş ve iç denetim mekanizmaları kurmuş, soruşturmalara ve olaylara yanıt verme planlarını içeren, izleme ve değerlendirme süreci sonunda güncellenen bir program olmalıdır. Ayrıca bu program, yetkili kamu makamlarının talebi üzerine gösterilmeye hazır tutulmalıdır. Veri denetleyicisi, veri ihlali olduğunda ilgili makamlara ve ilgili kişinin ihlal nedeniyle zarara uğrama ihtimali varsa ilgili kişiye bildirimde bulunmaları da ilkeler arasında bulunmaktadır.

Uluslararası uygulamanın temel ilkeleri olarak, yeterli güvencenin bulunduğu durumlarda ülkeler arası veri akışının kısıtlanmasından kaçınmaları, şayet bir kısıtlama getirilecekse de verilerin hassasiyetini, işlemenin amacını ve bağlamını dikkate alarak sunulan risklere orantılı olması gerektiği belirtilmiştir.

Ulusal uygulamalar kapsamında ülkelere, ulusal gizlilik stratejileri geliştirme, mahremiyeti koruyan kanunlar yapma, mahremiyeti uygulayacak kamu makamlara kurma, bireylerin haklarını kullanmaları için makul araçlar sağlama ve veri sahiplerine karşı haksız ayrımcılık yapılmamasını sağlama yükümlülüğüne yer verilmiştir. Son olarak da ülkelere, bu konuda uluslararası iş birliğine açık olmaları tavsiye edilmiştir[162].

[162] Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, ID: OECD/LEGAL/0188, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Çevrimiçi Tarihi: 07.05.2023)

b. Mahremiyeti Koruyan Yasaların Uygulanmasında Sınır Ötesi İşbirliğine İlişkin Konsey Tavsiyesi

Kişisel verileri koruma adına OECD tarafından yapılan bir diğer çalışma 12/06/2007 tarihinde kabul edilen "*Mahremiyeti Koruyan Yasaların Uygulanmasında Sınır Ötesi İşbirliğine İlişkin Konsey Tavsiyesi*"dir. Bu Tavsiye Kararı, kişisel verileri daha iyi korumak ve sınır ötesi veri akışlarındaki kesintileri en aza indirmek için, ülkeler arası mahremiyet kanunu uygulama makamları arasında uluslararası iş birliğini geliştirmeyi amaçlamaktadır. Tavsiye Kararı'nda özetle, uygun önlemlere tabi olarak bildirim, şikâyet yönlendirme, soruşturma yardımı ve bilgi paylaşımı dahil olmak üzere ülkelerle karşılıklı yardım sağlamak gibi konularda etkili işbirliği mekanizmaları geliştirmeleri üye ülkelere tavsiye edilmiştir[163].

c. Özel Sektör Kuruluşları Tarafından Tutulan Kişisel Verilere Devlet Erişimi Deklarasyonu

En son 2013'te yenilenen Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelere Dair 1980 tarihli Tavsiye Kararı, demokratik değerleri, hukukun üstünlüğünü, hak ve özgürlükleri koruyarak sınır ötesi veri akışını kolaylaştırmayı amaçlamaktadır. Bu amaç doğrultusunda kişisel verilerin korunması için ortak bir referans noktası sağlamaktadır. Ancak bu ilkeler, devletlerin ulusal güvenlik ve soruşturma yürütme ile ilgili egemenlik sorumluluğunu yerine getirirken yürütmüş olduğu kolluk faaliyetleri kapsamında genel güvenliğin sebep gösterilerek veri gizliliğinin ihlal edilmesine karşı, kişisel verileri koruma mekanizması getirmemektedir. Bu alanda ortak kriterlerin bulunmaması veri akışlarında gereksiz kısıtlamalara yol açabileceğine dair endişeleri artırmaktadır. OECD, küresel ekonominin dijital dönüşümü sürecinde çok önemli bir husus olan sınır ötesi veri akışlarına olan güveni artırma konusunda, kolluk mensuplarının mevcut yasal çerçeveler altında kişisel verilere nasıl erişebileceğini açıklığa kavuşturarak, 1980 ilkelerini tamamlayıcı ilkeleri ortaya koymak için çalışmalar yapmıştır. Veri koruma, ulusal güvenlik ve kolluk kuvvetleri konularında bir grup ülke uzmanıyla yapılan iki yıllık çalışmanın sonucu olarak, mahremiyetin ve diğer insan hak ve özgürlüklerinin korunmasında birbirini tamamlayan bir dizi ortak ilkeler ortaya konulmuştur.

[163] Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, ID: OECD/LEGAL/0352, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0352 (Çevrimiçi Tarihi: 07.05.2023)

OECD üye ülkeleri ve Avrupa Birliği'nin bakanları ve üst düzey temsilcileri tarafından 14 Aralık 2022 tarihinde İspanya'nın Gran Canaria adasında düzenlenen Dijital Ekonomi Politikası Komitesi (CDEP) Bakanlar Toplantısı'nda (OECD Digital Economy Ministerial Meeting) kabul edilen Özel Sektör Kuruluşları Tarafından Tutulan Kişisel Verilere Devlet Erişimi Deklarasyonu ile ulusal güvenlik ve kolluk kuvvetlerinin mevcut yasal çerçeveler altında kişisel verilere nasıl erişebileceğini açıklığa kavuşturmuştur. Deklarasyon, hükümetlerin demokratik değerlere ve hukukun üstünlüğüne aykırı bir şekilde kişisel verilere erişimini reddetmektedir. 14/12/2022 tarihinde OECD ülkeleri tarafından, ulusal güvenlik ve kolluk faaliyetleri amacıyla kişisel verilere erişirken gizliliğin ve diğer insan hak ve özgürlüklerinin korunmasına yönelik ortak yaklaşımlara ilişkin ilk hükümetler arası anlaşma kabul edilmiştir[164].

Bildiride ortaya konulan ilkeler özel sektör kuruluşlarının mülkiyetinde veya kontrolünde bulunan kişisel verilere devletin erişmesi ve bunları işlemesi için geçerlidir. Özel sektör kuruluşlarından kastedilen şey, bireyler ve kâr amacı güden veya gütmeyen her türlü sivil toplum kuruluşlarıdır. İlkeler şu şekildedir:

1- Yasallık İlkesi: Özel sektör kuruluşları tarafından tutulan kişisel verilere devletin erişimi, demokratik olarak kurulmuş ve hukuk kurallarına bağlı olarak faaliyet gösteren kurumlar tarafından benimsenmiş, uygulanabilir ve bağlayıcı bir yasal zemine oturtulmalıdır. Bu yasal çerçeve, kişisel verilerin yanlış kullanım ve suiistimal edilme riskine karşı güvence olması için devlet erişiminin amacını, şartlarını ve sınırlarını belirler.
2- Meşru Amaç İlkesi: Hükümetler, muhalif görüşleri baskı altına almak için veya yaş, engellilik, etnik köken, memleket, cinsiyet, cinsel yönelim, siyasi veya dini görüş gibi nedenlere bağlı olarak ayrımcılık yapmak için kişisel verilere erişmeye çalışamaz. Devlet erişimin, ölçülü, kötüye kullanıma karşı korunmuş, hukukun uygun gördüğü, meşru bir amacı olması gerekir.
3- Onay (Karar) İlkesi: Kişisel verilere devletin erişiminin belirli standartlarda ve prosedürde olması için gerekli olan bir ilkedir. Bu ilkeye göre yapılan yasal düzenlemede, veri erişimi sonrası ortaya çıkacak hak ihlalinin boyutuyla ölçülü olarak, karar talep etme ve talep verme kriterleri, izlenecek

164 https://www.oecd.org/digital/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm (Çevrimiçi Tarihi: 10.05.2023)

usul ve kararı verecek makam tespit edilir. Hakka müdahalenin ciddi boyutu varacak olması durumunda yargı makamlarından veya tarafsız olan yargı dışı makamlardan onay alma gerekliliği içerebilir. Ayrıca acil durumlarda istisnai olarak nasıl hareket edilmesi gerektiği de belirtilir. Onay kararları belgelenir. Somut ve meşru bir amaç için karar talep edilir ve gereklilikler karşılandığı durumda erişim kararı verilir. Karar almanın gerekli olmadığı durumlarda, veri erişimine şartlar ve sınırlamalar getirilerek ve denetim mekanizmaları kurularak, veri erişim yetkisinin kötüye kullanılmasının önüne geçilir.

4- Veri İşleme İlkesi: Hükümet erişimi yoluyla elde edilen kişisel veriler yalnızca yetkili personel tarafından işlenebilir ve yönetilebilir. Bu işleme ve yönetme işlemleri, gizlilik, güvenlik ve veri bütünlüğünü sağlamak için yasal çerçevede belirtilen gerekliliklere tabidir. Ayrıca, kişisel verilerin yasaya uygun şekilde işlenmesini, yasal çerçevede belirtilen süre boyunca saklanmasını, uygun olduğu ölçüde doğru ve güncel tutulmasını sağlamak için mekanizmaları içerir. Verinin kaybını, sızıntısını, yok olmasını, izinsiz kullanılmasını, değiştirilmesini veya ifşa edilmesini önlemek ve önlenemediyse bu durumu tespit etmek için iç kontroller oluşturulur ve bu tür durumları denetim kurumlarına bildirmek için raporlama mekanizmaları bulunur.

5- Şeffaflık İlkesi: bu konu için hazırlanan yasak düzenleme erişilebilir olmalıdır. Bireylerin ve halkın bilgilendirilme ihtiyacı ile ulusal güvenliği veya yasal yürütme faaliyetlerini zarara uğratacak bilgilerin açıklanmasını önleme ihtiyacı arasında denge sağlayan bir şeffaflık modeli benimsenir. Denetim kurumlarının raporları halka açık olarak paylaşılır, hükümet kayıtlarına erişim mekanizmaları kurulur, hükümet tarafından hazırlanan raporlar düzenli olarak paylaşılır ayrıca özel sektör kuruluşları da yasal çerçeveye uygun olarak hükümet erişim talepleriyle ilgili toplu istatistiksel raporlar yayınlayabilir.

6- Gözetim İlkesi: Hükümet erişiminin yasal çerçeveye uygun olduğunu sağlamak için etkili ve tarafsız denetim mekanizmaları bulunmalıdır. Denetim, iç birimler, mahkemeler, yasama komiteleri ve bağımsız idari otoriteler gibi kurumlar aracılığıyla sağlanmalıdır. Ülkelerin denetim sistemleri, kendi yetki alanlarına göre hareket eden ve ilgili bilgilere erişme ve inceleme, soruşturma veya sorgulama yapma, hükümet birimleriyle

iletişim kurma gibi yetkilere sahip olan bu kurumları içermektedir. Ayrıca, bu kurumlar, hükümet birimlerinin hesap verebilir olmasını sağlamak için uyumsuzluk raporlarını alıp yanıtlarlar ve bireylerin şikayetlerine yanıt olarak tazminat işlevlerini de yerine getirebilirler. Denetim kurumları, görevlerini yerine getirirken dış müdahalelerden korunur. Kurumların mali, personel ve teknik kaynakları olmalıdır. Bulgularını belgeleyerek raporlar üretir ve önerilerde bulunur, bu raporlar mümkün olan en geniş ölçüde halka açıklanır.

7- Tazminat İlkesi: Yasal çerçeve, bireylerin ulusal yasal düzenlemelerin ihlallerini tespit etmek ve düzeltmek için etkili yargısal ve yargı dışı tazminat mekanizmalarına sahip olmalarını sağlar. Ulusal güvenlik ve hukuki faaliyetlerinin gizliliğini koruma ihtiyacını dikkate alarak, bireylere verilerinin erişilip erişilmediği veya bir ihlal olup olmadığı konusunda bilgi verme imkanına sınırlama getirilebilir. Erişimi sona erdirme, yanlış erişilen veya saklanan verilerin silinmesi, verilerin bütünlüğünün geri kazanılması ve hukuka aykırı işlemlerin sona erdirilmesini gibi çözümler uygulanır. Ayrıca, duruma göre, bir bireyin maruz kaldığı zararlar için tazminat da içerebilir[165].

3. Avrupa Konseyi Tarafından Yapılan Düzenlemeler

a. Avrupa İnsan Hakları Sözleşmesi

Avrupa İnsan Hakları Sözleşmesi 8. maddesi özel ve aile yaşamını, konutu ve haberleşme özgürlüğünü korumaktadır. Kaynağını İnsan Hakları Evrensel Beyannamesi 12. maddeden alan AİHS m.8'te korunan bu hakların net olarak tanımları yoktur ve kapsamları kesin olarak belirlenemez. Her somut olay kendi durumuna göre yorumlanır[166]. Avrupa İnsan Hakları Mahkemesi kavramlara içerik kazandırırken, olayların koşulları ve zamanın gerekliliğine göre geliştirici ve ileri taşıyıcı bir yorum metodu uygulamaktadır.

Anayasa Mahkemesi'ne göre, özel hayat kavramı geniş yorumlanmalıdır[167]. Kişisel nitelikli verilerin korunması, özel hayatın korunması hakkının kapsamında değerlendirilmektedir. Avrupa İnsan Hakları Mahkemesi kararlarında, kişisel

---

[165] Declaration on Government Access to Personal Data Held by Private Sector Entities, ID: OECD/LEGAL/0487, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 (Çevrimiçi Tarihi: 10.05.2023)

[166] Durmuş Tezcan, M.Ruhan Erdem, Oğuz Sancakdar, R.Murat Önok, "*İnsan Hakları El Kitabı*", 9. bs., Seçkin Yayıncılık, Ankara, 2021, s. 425.

[167] AYM, Ali Sarıpınar Kararı, B.No:2013/5973, 17/12/2015.

verilerin yasal dayanağı olmaksızın toplanmasını ve saklanmasını, özel hayatın koruma alanına müdahale olarak değerlendirmektedir[168].

AİHM, kişinin özel hayatı ile ilgili verilerin saklanmasını 8. madde kapsamında olduğunu kabul etmektedir[169]. Özel hayat kavramı, sınırlayıcı bir şekilde yorumlanmamalıdır. 28 Ocak 1981 tarihli Avrupa Konseyi Antlaşması olan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin "*Tanımlar*" başlıklı 2. maddesinde *"kişisel veriler, kimliği belirli veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgileri ifade eder*"; *"Konu ve Amaç"* başlıklı 1. maddesinde "*sözleşmenin amacı, her bir Tarafın ülkesinde,… her gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır"* denilmektedir. AİHM'nin özel hayat kavramını geniş yorumlaması ve kişisel verileri bu bağlamda değerlendirmesi, 1981 tarihli sözleşmedeki yorum ile de örtüşmektedir[170].

AİHM içtihatlarına göre; kişinin adı, resmi, cinsiyeti, cinsel yaşamı, ticari/mesleki faaliyetleri gibi hususları Sözleşme'nin 8. maddesinde korunan değerler olarak görmektedir. Sadece özel mülk içerisinde değil kamusal alanda da makul düzeyde bir özel hayata saygı hakkı beklentisi varsa, kamusal alanda kişisel verilerin toplanması, saklanması veya ifşa edilmesi AİHS'in 8. maddesine aykırılık teşkil edebilecektir[171].

AİHS'nin 8. maddesinin ilk fıkrasında hakkın tanımı yapılmış, ikinci fıkrasında ise sınırlama nedenleri belirlenmiştir. İkinci fıkraya göre müdahale ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için ancak yasayla öngörülmüş ve demokratik bir toplumda gerekli durumlarda söz konusu olabilir.

AİHM'e göre AİHS'nin 8. maddesi devletlere hem negatif hem pozitif yükümlülük yüklemektedir. Maddenin amacı, esasen bireyi kamu makamlarının

---

[168] Tezcan, Erdem, Sancakdar, Önok, "*İnsan Hakları El Kitabı*", s. 428; AİHM, Segerstedt-Wiberg ve D.- İsveç Kararı, B. No:62332/00, 06/06/2006

[169] AİHM, Leander – İsveç Kararı, B. No:9248/81, 26/03/1987, § 48.

[170] AİHM, Amann – İsviçre Kararı, B. No: 27798/95, 16/02/2000, § 65.

[171] Ayla Çalışkan, "*Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*", https://www.jurix.com.tr/article/20726, 3.

keyfi müdahalesine karşı korumak olmakla birlikte, buna ek olarak, özel hayata etkin biçimde saygıya içkin pozitif yükümlülükler bulunabilir. Bu yükümlülükler, bireylerin kendi aralarındaki ilişkiler alanında bile özel hayata saygı gösterilmesini sağlamak için tasarlanmış önlemlerin kabul edilmesini içerebilir. Hak kapsamındaki pozitif ve negatif yükümlülükleri arasındaki sınırlar kesin olarak çizilememektedir.[172] Bir devletin Sözleşme kapsamındaki pozitif ve negatif yükümlülüklerini değerlendirirken uygulanan prensipler benzerdir. Madde 8'in ikinci fıkrasındaki amaçlar belli oranda geçerli olmak üzere, birey ile bir bütün olarak toplumun yarışan menfaatleri arasında kurulması gereken adil dengeye dikkat edilmelidir[173].

AİHM negatif yükümlülüklere ilişkin bir inceleme yaparken, müdahalenin 8. maddenin 2. Fıkrası'nda öngörülen gerekliliklerle uygun olup olmadığını, yani hukuka uygun olup olmadığını, meşru bir amaç güdüp gütmediğini ve demokratik bir toplumda gerekli olup olmadığını incelemektedir. Pozitif yükümlülüğün söz konusu olması halinde Mahkeme, bahse konu menfaatin öneminin, başvurucu tarafından beklenen pozitif yükümlülüğün dayatılmasını gerekli kılıp kılmadığını dikkate almaktadır. Devletler üzerindeki pozitif yükümlülüğün içeriğinin incelenmesinde; ulusal sistemdeki idarenin ve hukuki pratiklerin uyumunu, tehlike altındaki menfaatlerin önemini ve özel hayatın "*temel değerleri*" veya "*esaslı yönlerinin*" bahse konu olup olmadığını veya sosyal gerçeklik ile hukuk arasındaki bir uyumsuzluğun başvurucu üzerindeki etkisini dikkate almaktadır[174].

Devletler negatif ve pozitif yükümlülüklerini yerine getirirken belli bir takdir yetkisine sahiptir. Bireylerin eylemlerine karşı koruma bakımından Madde 8'e uyulmasını güvence altına almaya yönelik yöntemleri seçmek, ilke olarak devletlerin takdir yetkisindedir. Ancak temel değerlerin ve özel hayatın asli yönlerinin tehlikede olduğu ağır eylemler karşısında etkin caydırıcılık, etkili ceza hukuku hükümlerini zorunlu kılmaktadır. Bu nedenle devlet, tecavüzü cezalandıran ceza hukuku hükümlerini yasalaştırma ve bu hükümleri etkili soruşturma ve kovuşturma ile

[172] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", 2019, 8. Link: https://www.echr.coe.int/documents/d/echr/Guide_Art_8_TUR (Çevrimiçi Tarihi: 19.07.2023).; Evans - Birleşik Krallık, B. No: 6339/05, 10/04/2007, § 75.
[173] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi"*, s. 8; Hämäläinen - Finlandiya, B. No: 37359/09, 16/07/2014, § 65.
[174] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 9; Hämäläinen - Finlandiya, B. No: 37359/09, 16/07/2014, § 66.

pratikte uygulama şeklinde pozitif bir yükümlülüğe sahiptir[175]. Örneğin bir davada Mahkeme, kişilerin dairelerinin içine gizli kablo ve kameraların yerleştirilmesini, hayatın en özel yönlerinin izinsiz şekilde kaydedilmesini ve elde edilen video görüntülerinin kamuya dağıtılmasını ağır ve insan onurunu küçük düşürücü olarak nitelendirmiştir[176]. Bu nedenle devletlerden insan onuruna yönelik saldırıları engellemek adına caydırıcı cezai hükümleri düzenlemeleri beklenmektedir.

AİHM hakka yapılan müdahaleyi incelerken şu testi uygulamaktadır:

1- Yasallık Şartı: Müdahalenin ulusal hukukta yasal bir dayanağının olup olmadığı sorgulanır. Kanunilik ilkesi olarak da adlandırılan bu şartta, bulunması gereken yasa şekli anlamda değil maddi anlamdadır. Bir başka ifadeyle, sadece yasama organı tarafından çıkartılan kanunlar değil ayrıca uluslararası antlaşmalar, yönetmelikler ve mahkeme içtihatları da bu kapsamda düşünülmektedir. Önemli olan düzenlemenin, hukukun üstünlüğüne uygun bir biçimde kaliteli bir hukuk olmasıdır[177].

   Ulusal hukuk açık, öngörülebilir ve yeterince erişilebilir olmalıdır[178]. Bireylerin hukuka uygun şekilde hareket etmesini sağlayabilecek ölçüde öngörülebilir olmalı ve kamu makamlarının takdir yetkisinin kapsamını açıkça belirlemelidir. Örneğin, Mahkeme'nin izleme faaliyetleri bağlamında açıkça ifade ettiği üzere hukuk, hükümleri yönünden vatandaşlara, makamların herhangi bir gizli izleme ve veri toplama faaliyetine başvurmaya yetkili olduğu koşullara ve durumlara ilişkin yeterli bir gösterge sağlayacak ölçüde açık olmalıdır[179].

   Açıklık gerekliliği, kamu makamlarınca kullanılan takdir yetkisinin kapsamı bakımından uygulanır. Ulusal hukuk, bireylere demokratik bir toplumda hukukun üstünlüğü uyarınca hak ettikleri asgari koruma

[175] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 9; M.C. - Bulgaristan, B. No: 39272/98, 04/12/2003.
[176] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 9; Khadija Ismayilova - Azerbaycan, B. No: 65286/13 ve 57270/14, 10/01/2019, § 116
[177] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 10; Halford - Birleşik Krallık, B. No: 20605/92, 25/06/1997, § 49.
[178] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 10; Silver ve Diğerleri - Birleşik Krallık, B. No: 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25/03/1983.
[179] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 10.; Shİmovolos - Rusya, B. No: 30194/09, 21/06/2011, § 68.

düzeyinin temini için, kamu makamlarına tanınan bahis konusu takdir yetkisinin kapsamını ve kullanılma şeklini makul ölçüde açık biçimde göstermelidir[180].

Dolayısıyla, öngörülebilirlik açısından "*hukuka uygun*" tabiri, diğer hususların yanı sıra bireylere ulusal hukukun, kamu makamlarının hangi koşul ve durumlar altında kendilerinin Sözleşme ile tanınan haklarını etkileyen tedbirlere başvurabileceğine dair yeterli bir gösterge sağlayacak ölçüde öngörülebilir olması gereğini anlatmaktadır[181]. Öngörülebilirlik kesin olmak zorunda değildir. Başvurucular, en azından hukuk uzmanlarının yardımıyla, makul bir derecede, hukukun kapsamına öngörebilmeliler[182].

Olayların gerçekleştiği dönemde yürürlükte olan ulusal hükmün lafzının ve ruhunun yeterli ölçüde açık olduğu durumda bile, bunun ulusal mahkemelerce yorumlanması ve başvurucunun davasının koşullarına uygulanması açıkça mantıksız ve dolayısıyla Madde 8 uyarınca öngörülemez olmamalıdır[183].

2- Meşru amaç şartı: Müdahalenin amacı, AİHS 8. Maddesi'nin 2. Fıkrası'nda sayılan nedenlerden biri olmalıdır. Sözleşmede bu nedenler *"ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumu"* olarak sayılmıştır.

Belirtilen kavramlar soyut kavramlar olup Mahkeme önüne gelen dosyalarda taraf devletler, yapılan müdahalenin hangi meşru amaçla

[180] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 13.; Piechowicz - Polonya, B. No: 20071/07, 17/04/2012, § 212.
[181] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 11.; Fernández Martínez - İspanya, B. No: 56030/07, 12/06/2014, § 117.
[182] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 11.; Slivenko - Letonya, B. No: 48321/99, 09/10/2003.
[183] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 11.; Altay – Türkiye (No. 2), B. No: 11236/09, 09/04/2019, § 57.

yapıldığını izah etmektedir. Devletler meşru amacı belirtmediği durumlarda Mahkeme resen meşru amaç taşıdığına karar verebilir[184].

3- Demokratik bir toplumda gerekli olma şartı: Ölçülülük ilkesi olarak da bilinen bu şart, meşru amacın gerçekleştirilmesinde yapılan müdahalenin elverişli, orantılı ve gerekli olması şartlarını bir arada bulundurması anlamına gelmektedir. Bireyin menfaatinden daha ağır basan bir toplumsal menfaat olmalı, bireyin menfaati ile toplumsal menfaat arasında adil bir denge kurulmalıdır. Müdahale, hakkın özüne dokunacak kadar gereğinden fazla olmamalı, asgari düzeyde kalmalıdır.[185]

Mahkeme "*demokratik bir toplumda gerekli*" olup olmadığını tespit etmek için üye devletin menfaatleri ile başvurucunun hakları arasında dengeyi tespit etmeye çalışmaktadır. Mahkeme için, "*gereklilik*" ifadesi "*işe yarar*", "*makul*" veya "*arzu edilen*" anlamına gelmemektedir, "*gereklilik*" bir "zorunlu toplumsal ihtiyacın" varlığını ifade etmektedir. Her olayda zorunlu toplumsal ihtiyaç bakımından ilk değerlendirmeyi ulusal makamlar yapmaktadır, dolayısıyla bu makamlara bir takdir yetkisi verilmiştir. Ancak makamların kararı Mahkeme'nin incelemesine tabidir. Bir Sözleşme hakkının sınırlandırılması, diğer hususlarla birlikte, güdülen meşru amaçla orantılı olmadığı sürece "*demokratik bir toplumda gerekli*" kabul edilemez[186].

AİHM demokratik toplumda gereklilik kavramını incelerken şu iki şartı aramaktadır: birincisi, hakkı sınırlayan eylemin acil bir toplumsal gereklilikten doğması; ikincisi, amaç ile orantılı olması yani istenen amaca erişmek için uygun olan ve hakka en az müdahale eden eylemin tercih edilmesi gerekmektedir. Bu iki şartı beraber sağlayan eylemler, demokratik toplumda gerekli kabul edilmektedir[187].

---

[184] Çalışkan, "*Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*", s. 4.
[185] Osman Doğru, Atilla Nalbant, "*İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar*", C. 2, 1. bs., Pozitif Matbaa, Ankara, 2013, s. 15 vd.
[186] AİHM, Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi, 12.; Dudgeon - Birleşik Krallık, B. No: 7525/76, 22/10/1981, §§ 51-53.
[187] AİHM, Nada - İsviçre, B. No: 10593/08, 12/9/2012, § 183; AİHM, Silver ve Diğerleri - Birleşik Krallık, B. No: 5947/72, 25/3/1983, § 97

Ayrıca Mahkeme, davayı bir bütün olarak incelediğinde, müdahaleyi meşru kılmak için sunulan gerekçelerin ilgili ve yeterli, tedbirlerin güdülen meşru amaçlarla orantılı olup olmadığını dikkate almaktadır[188]. Bir müdahalenin "*gerekli*" olup olmadığını belirlerken Mahkeme, ulusal makamlarına verilen takdir yetkisini gözetecektir fakat müdahalenin ardındaki zorunlu toplumsal ihtiyacı göstermek davalı devletin bir görevidir[189].

b. 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Bilgi ve iletişim teknolojisi alanında 1960'lı yıllarda yaşanan gelişmelerle, kişisel verilerin dijital ortama işlenmesi süreci başlanmış ve bu süreçte kişisel verilerin gizliliği için gerek hukuki gerek teknik alanda çalışmalar yapılmaya başlanmıştır. Avrupa Konseyi de bu konuya kayıtsız kalmamıştır. Yapılan çalışmalar sonucunda "*108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi*" 28 Ocak 1981 tarihinde Strazburg'da imzaya açılmış ve 1 Ekim 1985 tarihinde yürürlüğe girmiştir[190].

Sözleşme, üye ülkelerde uyruk ve ikamet yeri fark etmeksizin tüm gerçek kişilerin özel hayata saygı hakkı başta olmak üzere temel hak ve özgürlüklerini güvence altına almayı amaçlamaktadır. Sözleşme, kamu sektöründe ve özel sektörde, otomatik kişisel veri dosyaları ve kişisel verilerin otomatik işleme tabi tutulması konusu ile kapsamı dar tutmuştur. Ancak üye ülkelerin sözleşme hükümlerini, tüzel kişiliğe sahip olan veya olmayan her çeşit kuruluş hakkında uygulamasına veya otomatik bilgi işleme konu olmayan kişisel veri dosyaları hakkında da uygulamasına engel bir şey yoktur.

Sözleşmede "*otomatik işlem*", verilerin kaydı, değiştirilmesi, silinmesi, geri elde edilmesi, dağıtılması veya verilere mantıksal ve aritmetik işlem uygulanmasının,

---

[188] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 11.; Z - Finlandiya, B. No: 22009/93, 25/02/1997, § 94.
[189] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 13.; Piechowıcz - Polonya, B. No: 20071/07, 17/04/2012, § 212.
[190] Kişisel Verileri Koruma Kurumu, "*Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*", https://www.kvkk.gov.tr/Icerik/2030/Rehberler?&page=3 (Çevrimiçi Tarihi: 11.05.2023)

tamamen veya kısmen otomatik yöntemlerle gerçekleştirilmesini ifade eder. Otomatik işleme konu olan bilgiler "*otomatik veri dosyası*", bu dosyaların amacını belirleyen, kaydedilen verinin kategorisini ve verilere yapılacak işlemi belirleyen gerçek veya tüzel kişi, kamu kurumu veya yetkilendirilmiş diğer kuruluşlar "*dosya yöneticisi*" olarak tanımlanmıştır.

Sözleşme'nin "*Verilerin Niteliği*" başlıklı 5. maddesinde otomatik veri dosyası olan kişisel veriler hakkında temel ilkeleri ortaya koymaktadır. Bu maddeye göre;

1- Veriler hukuka uygun olarak elde edilmeli ve işlenmelidir.
2- Veriler belli ve meşru amaçlar için kaydedilmeli ve bu amaçlara uygun olarak kullanılmalı ve amaçlara elverişli olacak büyüklükte olmalı yani gereğinden fazla olmamalıdır.
3- Verilerin bilgileri doğru ve günceldir.
4- Veriler, ilgili kişilerin kimliklerini belirleyebilecek şekilde ve kaydedilme amaçlarına uygun bir süre saklanır.

Sözleşme, kişinin ırksal kökeni, siyasi düşüncesi, din ve inancı hakkında bilgi veren, sağlık veya cinsel hayat ile ilgili ve ceza mahkumiyetiyle ilgili kişisel verileri "*özel veri*" kategorisinde görmüş ve bu kişisel verilerin otomatik işleme tabi tutulmasını yasaklamıştır. Ancak iç hukukta uygun güvenceler sağlandığı takdirde özel verilerin otomatik işleme tabi olabileceği de sözleşmede belirtilmiştir.

Kişisel verilerin yanlışlıkla imha edilmesi, kaybolması veya izinsiz olarak yok edilmesi, elde edilmesi, değiştirilmesi ve dağıtılmasına karşı gerekli güvenlik tedbirlerinin alınması sözleşmeye taraf devletler için bir yükümlülüktür.

Sözleşme 8. maddesinde ilave güvenceler sağlamak amacıyla ilgili kişiye birtakım haklar vermiştir. Bu maddeye göre herkes;

1- Otomatik kişisel veri dosyasının olup olmadığını, varsa temel amacını, dosya yöneticisinin kimlik, ikamet ve iş yeri bilgilerini öğrenmek,
2- Otomatik dosyada kendisine ait kişisel verilerin bulunup bulunmadığını öğrenme ve bu bilgileri makul sıklıkta ve sürede, uygun ücretle kendisine iletilmesini isteme,

3- Kişisel verileri düzelttirme ve sözleşmede ortaya konulan ilkelere aykırı bir biçimde işlenmiş olması halinde sildirme,
4- Kendisi hakkındaki verilerin teyit edilmesi, düzeltilmemesi, sildirilmesi talebinin yerine getirilmemesi durumunda bir başvuru yolundan yararlanma haklarına sahiptir.

Sözleşmede ortaya konulan ve yukarıda bahsedilen güvenceler mutlak değildir yani kısıtlanabilir ve istisna getirilebilir. Ancak bu kısıtlama ve istisnaların hangi durumlarda olacağı da Sözleşme'nin 9. maddesinde belirtilmiştir ve belirtilen hususlar haricinde başkaca bir gerekçe olamayacağı vurgulanmıştır. Devlet güvenliğinin ve ekonomik çıkarlarının korunması, kamu güvenliği ve suçların önlenmesi, veri sahibi veya başka kişinin hak ve özgürlüklerin korunması amacıyla sözleşmede ortaya konulan güvenceler kısıtlanabilir. Ancak bu istisna getirme ve kısıtlamanın, yasayla öngörülmüş ve demokratik toplumda gerekli olması gerekmektedir. İlgili kişilere kendi kişisel verileri ile ilgili olarak tanınan haklar açısından da özel hayata tecavüz tehlikesi bulunmadığı aşikâr ise, bilimsel çalışmalarda ve istatistiki veri olarak kullanılan veriler hakkında yasayla kısıtlama getirilebilir.

Sözleşme, taraf devletler arası veri akışının yasaklanmasını ve izne tabi olmasını yasaklamıştır ancak bu kurala istisna getirmiştir. Bir ülkenin kendi mevzuatı, belli kişisel veri veya otomatik veri dosyası kategorisi için bunların doğası gereği özel düzenlemeler içeriyorsa veya diğer devletin mevzuatı aynı değerde bir koruma sağlamıyorsa, veri akışı yasaklanabilir veya izne tabi tutulabilir. Ayrıca veri akışının bir taraf ülke üzerinden üçüncü bir taraf olmayan ülkeye yapılması durumunda, veri çıkışının olacağı kaynak ülkenin mevzuatında bulunan boşluktan faydalanacak şekilde veri transferi yapılıyorsa, bu durumda da veri akışı yasaklanabilir veya izne tabi tutulabilir. Sözleşme, taraf ülkelere birbirlerine yardımcı olma yükümlülüğü yüklemiş ve bu kapsamda kurulacak iletişim kanalları hakkında birtakım düzenlemeler yapmıştır.

Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme, kişisel verilen korunması konusunda

bağlayıcı olan ilk uluslararası belgedir[191]. Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi imzalayan ilk ülkelerden birisidir ancak 29/02/2016 tarihinde kararlaştırılmıştır. 17 Mart 2016 tarih ve 29656 sayılı Resmî Gazete'de yayımlanarak iç hukuka dâhil edilmiştir.

c. 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

Bu protokolde taraf devletler, kişisel verilerin işlenmesi karşısında bireylerin etkili şekilde korunması için, kişisel verilerin korunması alanında ülkelerinde uygulanmak üzere görevlerini tam bağımsızlıkla yerine getirecek, her kişinin haklarının ve temel özgürlüklerinin korunmasına dair taleplerini dinleyecek denetleyici makam kurmayı taahhüt etmiştir. Ayrıca bu protokolde, taraf devletlerden sözleşmeye taraf olmayan başka bir devlette bulunan alıcıya sınır ötesi veri akışının, verilerin yeterli seviyede korunmasını garanti edildiği durumunda yapılması gerektiğini düzenlemiştir.

Türkiye, bu protokolü 8 Kasım 2001 tarihinde imzalamıştır. Protokol, 5 Mayıs 2016 tarih ve 29703 sayılı Resmî Gazete'de yayımlanarak iç hukuka dâhil edilmiştir[192].

4. Avrupa Birliği Tarafından Yapılan Düzenlemeler

a. 95/46EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif

108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ile Avrupa devletleri iç hukuklarında kişisel verileri koruma kapsamında düzenlemeler yapmıştı ancak yapılan düzenlemelerde bir bütünlük bulunmamaktaydı. 7 Şubat 1992'de imzalanan ve Kasım 1993'te yürürlüğe giren Maastricht Antlaşması ile ekonomik ve parasal birlik yani bir ortak pazar kurulması hedeflenmişti. Bu hedef açısından, birliğe üye ülkelerde kişisel

[191] Songül Atak, "*Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler*", TBB Dergisi, S. 87, 2010, s. 90

[192] Kişisel Verileri Koruma Kurumu, "*Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*", https://www.kvkk.gov.tr/Icerik/2030/Rehberler?&page=3 (Çevrimiçi Tarihi: 11.05.2023)

verileri koruma hukukunun farklı düzenlenmiş olması bir eksiklik olarak görüldü. Üye ülkelerin kişisel verileri koruma düzenlemeleri arasındaki farklılık ve çelişkilerin giderilmesi için birlik bünyesinde bir düzenleme yapma ihtiyacı duyulmuştur. Yapılan çalışmalar neticesinde 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Yönergesi (Directive 95/46/EC Of The European Parliament And Of The Council) 24 Ekim 1995 tarihinde yürürlüğe girmiştir[193].

Direktifin amacı, başta kişisel verilerin işlenmesiyle ilgili olarak mahremiyet hakkı olmak üzere temel hak ve özgürlüklerini korumak ve birliğe üye devletler arasında kişisel verilerin serbest akışını sağlamaktır. Direktifin 3. maddesinde kapsam belirtilmiş olup, sadece tamamen veya kısmen otomatik yollarla işlenen veriler değil otomatik olmayan yollarla işlenen veriler de kapsam dahilinde olduğu belirtilmiştir. Direktif bu hususta 108 Sayılı Sözleşme'den farklılaşmıştır. 108 Sayılı Sözleşme'nin kapsamı otomatik yollarla işlenen veriler iken 95/46/EC Sayılı Direktif otomatik olmayan yollarla işlenen verileri de düzenleme içerisine alarak, bu açıdan kapsamı daha da geniş tutmuştur. Avrupa Birliği hukuku kapsamı dışında kalan bir faaliyet, kamu güvenliği, savunma, devlet güvenliği ve devlet güvenliği ile ilgili ekonomik faaliyet, ceza hukuku faaliyetleri esnasında işlenen veriler ile tamamen kişisel veya ev işleri ile ilgili olarak gerçek kişi tarafından işlenen veriler kapsam dışı bırakılmıştır.

95/46/EC Sayılı Direktif günümüzde yürürlükte değildir. 2016/679 sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) yürürlüğe konulduğunda hükümsüz kılınmıştır[194]. Bu nedenle 95/46/EC Sayılı Direktif ile yapılan düzenlemelere burada detaylıca yer verilmeyecektir.

b. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

95/46/EC Sayılı Direktif ile Avrupa Birliği ülkeleri aynı temel prensipler paydasında buluşmuş olsalar da, her ülkenin farklı düzenleme yapması nedeniyle yeknesaklık sağlanamamıştır. Ayrıca geçen sürede teknolojinin daha da gelişmiş olması nedeniyle veri kayıtları hayatın her alanında yayılmıştır. Bu nedenlerle

[193] Senem Ovalıoğlu, "*Avrupa Birliği Hukukunda Kişisel Verilerin Korunması*", (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir 2021), s. 57 vd.
[194] Ovalıoğlu, "*Avrupa Birliği Hukukunda Kişisel Verilerin Korunması*", s. 59 vd.

95/46/EC Sayılı Direktif'i güncelleme çalışmaları yapılmıştır. Çalışmalar neticesinde iki çıktı alınmıştır: Birincisi 2016/679 Sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation), diğeri ise 2016/680 Sayılı Veri Koruma Direktifi'dir. Normlar hiyerarşisi açısından tüzük seviyesinde bağlayıcı ve doğrudan bir düzenleme olarak 2016/679 Sayılı Genel Veri Koruma Tüzüğü (GDPR) 25 Mayıs 2018 tarihinde yürürlüğe girmiştir[195].

Tüzük, gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunmasına ve kişisel verilerin serbest dolaşımına ilişkin kuralları konu edinmiştir. Tüzüğün amacı ise, başta kişisel verilerin korunması hakkı olmak üzere kişilerin temel hakları ve özgürlükleri korumak ve Birlik içerisinde kişisel verilerin serbest dolaşımını sağlamaktır.

Kişisel verilerin otomatik olan veya olmayan yollarla işlenmiş olması fark etmeksizin, bir dosyalama sisteminin parçasını oluşturan veya oluşturması amaçlanan araçlarla işlenmesi durumunda tüzük uygulanacaktır. Ancak Birlik hukuku dahilinde olmayan bir konuda, Birlik üyelerinin ortak dış ve güvenlik politikaları ile ilgili konularda, gerçek kişinin kişisel ve ev faaliyeti esnasında yapmış olduğu veri kayıtlarında, yetkili makamlar tarafından yapılan suç önleme, tespit, soruşturma, kovuşturma ve cezaların infaz edilmesi işlemlerinde tüzük kuralları istisna tutulmuştur.

Yer açısından kapsam konusunda tüzük coğrafi bir sınır çizmemiştir. Kriter olarak "*Birlik içerisindeki bir kontrolör veya işleyicinin işletmesi*" faktörü belirlenmiş olup bunların faaliyetleri Birlik içerisinde gerçekleşmemiş olsa bile kapsam dahiline alınmıştır. Birlik içerisinde bulunan veri sahiplerine mal ve hizmet sunulması ve veri sahiplerinin davranışlarının izlenmesi durumlarında da tüzük uygulanacaktır. Kişi açısından Birliğe üye devletlerin vatandaşı olup olmama önem taşımamaktadır. Yer açısından sınır Birliğe üye devletlerin sınırları değil bir üye devletin hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı her yerde uygulama alanı bulacaktır. Görüldüğü gibi GDPR'ın uygulama alanı Birlik sınırları ile sınırlı değildir, kapsam bayağı geniş tutulmuştur.

[195] Tüze Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir 2022), s. 26.

Kapsam konusu haricinde GDPR'ın getirdiği başka yenilikler de bulunmaktadır. Örneğin veri koruma görevlisi ve unutulma hakkı kavramları ile bu tüzükte yeni karşılaşılmıştır. Unutulma hakkı, veri sahibinin kişisel bilgilerini dijital platformdan kalıcı bir şekilde sildirme hakkı olarak tanımlanabilir. İlgili kişinin hakları ile ilgili ortaya çıkabilecek hukuka aykırılıklarda 95/46/EC Sayılı Direktif sadece veri kontrolünü sorumlu tutarken, GDPR sorumluları genişleterek veri işleyen birey veya kurumun da sorumlu tutulacağı düzenlenmiştir[196].

III. KİŞİSEL VERİLERİN KORUNMASI HAKKININ TESİSİNDE GEREKLİ OLAN TEDBİRLER

A. İdari Tedbirler

Kişisel Verileri Koruma Kurumu tarafından hazırlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) isimli dokümanda kişisel verilerin güvenliğine ilişkin idari tedbirler şu şekilde açıklanmıştır:

- Mevcut Risk ve Tehditlerin Belirlenmesi: Kişisel verilerin türü, sağlanması gereken gizlilik seviyesi, güvenlik ihlali durumunda ortaya çıkabilecek zararın boyutu dikkate alınarak, risk yönetimi çerçevesinde denetleme ve çözüm alternatifleri düşünülmeli ve uygulanmalıdır.
- Çalışanların Eğitilmesi ve Farkındalık Çalışmaları: Personele az da olsa siber güvenlik konusunda, saldırıyı tanıma ve saldırıya ilk müdahaleyi yapma eğitimi verilmeli, kişisel verilerin kasten veya taksirle açıklanması ve paylaşılmasını engelleyecek şekilde iş paylaşımı ve denetim mekanizması geliştirilmeli, güvenlik politikasına uymayan personel hakkında yürütülecek disiplin prosedürleri belirlenmelidir.
- Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi: Güvenlik politikası ve prosedürlerini önceden belirli olması, ortaya çıkabilecek risklerin de önceden öngörülebilir olmasına ve personelin de istikrarlı bir şekilde dikkatli olmasına fayda sağlayacaktır. Politika ve

[196] Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", s. 27 vd.

prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.

- Kişisel Verilerin Mümkün Olduğunca Azaltılması: Doğru ve güncel olmayan, herhangi bir amaç için kullanılmayan kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir.
- Veri İşleyenler ile İlişkilerin Yönetimi: Veri işleyen ile veri sorumlusu arasında yazılı bir sözleşme yapılmalı, bu sözleşmede veri işleyenin, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağı ve veri ihlali olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olduğu belirtilmelidir. Veri sorumlusunun veri işleyeni denetleyebileceği ve inceleyebileceği alt yapı hazırlanmalıdır.

B. Hukuki Tedbirler

Kişisel Verilerin Korunması Kanunu'nun beşinci bölümü suçlar ve kabahatleri düzenlemiştir. Kanunun 17. maddesiyle kişisel verilere ilişkin suçlar ve cezai yaptırımlar 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümlerine atıf yapılmıştır.

Kanunda öngörülen yükümlülüklere aykırı davranılması halinde KVKK'nın 18. maddesince, idari yaptırımlar uygulanacaktır. İdari yaptırımlara Kişisel Verileri Koruma Kurulu karar vermektedir. Kurulun, failin kusuru ve ekonomik durumunu göz önünde bulundurarak hakkaniyetli karar alması için, kabahatler için öngörülen idari para cezalarının alt ve üst sınırları arasındaki makas geniş tutulmuştur. Gerçek kişilerin ekonomik güçlerinin farklı olduğu veya ülke çapında faaliyet gösteren tüzel kişi ile bir ilçede faaliyet gösteren tüzel kişinin güçlerinin farklı olduğu düşünüldüğünde, düzenlemenin hakkaniyete uygun olduğu kanaatine varılmaktadır.

Veri sorumlusu gerçek kişi veya özel hukuk tüzel kişisi olduğunda idari para cezasına karar verilir. Ancak veri sorumlusunun idare olması durumunda kabahat olarak düzenlenen eylemlerin işlendiğinde ise Kurulun yapacağı bildirim üzerine, ilgili devlet kurumu memurları ve diğer kamu görevlileri ile kamu kurumu

niteliğindeki meslek kuruluşları personeli hakkında disiplin soruşturması yapılacaktır.

Verilen yaptırım kararlarına karşı idari yargı yolu açıktır.

C. Teknik Tedbirler

Kişisel Verileri Koruma Kurumu tarafından hazırlanan Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) isimli dokümanda kişisel verilerin güvenliğine ilişkin idari tedbirler şu şekilde açıklanmıştır:

Siber güvenliğin sağlanması için, tehditlerin sürekli olarak değiştiği ve genişlediği göz önünde bulundurularak, çeşitli tedbirler uygulanmalıdır. Bu tedbirler arasında güvenlik duvarı, ağ geçidi, yazılım güncellemeleri, yama yönetimi, erişim sınırlamaları, güçlü şifreler ve parolalar kullanımı, kaba kuvvet algoritması, kötü amaçlı yazılımlardan korunma ve SSL gibi önlemler yer almaktadır. Bu tedbirlerin düzenli olarak kontrol edilmesi ve güncellenmesi önemlidir. Kişisel veri içeren sistemlere erişimin sınırlı olması ve kullanıcı yetkilendirmesi de gerekmektedir.

Kişisel veri güvenliğinin takibi yapılmalıdır. Bilişim ağlarında kullanılan yazılım ve servislerin kontrol edilmesi, izinsiz erişimlerin tespit edilmesi, kullanıcı işlemlerinin düzenli olarak kaydedilmesi, güvenlik sorunlarının hızlı bir şekilde raporlanması ve çalışanların güvenlik zafiyetlerini bildirebilmeleri için resmi bir raporlama prosedürünün oluşturulması gerekmektedir. Ayrıca, güvenlik yazılımı mesajları ve erişim kontrolü kayıtlarının düzenli olarak kontrol edilmesi, zafiyet taramaları ve sızma testlerinin yapılması ve ortaya çıkan güvenlik açıklarına göre değerlendirmeler yapılmalıdır.

Kişisel verilerin korunması için fiziksel ve elektronik ortamlarda güvenlik önlemleri alınmalıdır. Fiziksel ortamda, verilerin saklandığı cihazlar ve kağıtların çalınma veya kaybolma riskine karşı korunması, dış risklere karşı (yangın, sel gibi) fiziksel ortamların korunması ve giriş/çıkışların kontrol altına alınması gerekmektedir. Elektronik ortamda, veri güvenliği ihlallerini önlemek için erişim sınırlamaları ve ağ bileşenlerinin ayrılması gibi önlemler alınabilir. Kişisel veri içeren cihazların çalınması veya kaybolması gibi durumlara karşı şifreleme ve erişim kontrolü gibi önlemlerin alınması gerekmektedir. Şifreleme yöntemlerinin kullanımında, uluslararası kabul gören şifreleme programlarının tercih edilmeli ve

asimetrik şifreleme yöntemi kullanılıyorsa anahtar yönetimi süreçlerine dikkat edilmelidir.

Kişisel verilerin bulutta depolanması durumunda, bulutta depolanan kişisel verilerin ayrıntılı bir şekilde bilinmesi, yedeklenmesi ve senkronize edilmesi gerekmektedir. Uzaktan erişim durumunda, iki kademeli kimlik doğrulama kontrolü uygulanmalıdır. Kişisel verilerin bulut sistemlerinde depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmeleri gerekmektedir. Bulut ortamlarına şifrelenmiş şekilde aktarılmalı ve her bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılmalıdır. Bulut bilişim hizmet ilişkisi sona erdiğinde, şifreleme anahtarlarının tüm kopyaları yok edilmelidir.

Bilgi teknolojileri sistemleri tedariği, geliştirme ve bakımı açısından; işlem sırasında oluşabilecek hataların veri bütünlüğünü bozma olasılığını en aza indirecek şekilde uygulamalar tasarlanmalıdır. Kişisel veri içeren cihazların üretici, satıcı veya servis gibi üçüncü kurumlara gönderilmeden önce, veri saklama ortamı sökülerek güvenli bir şekilde saklanmalı ve sadece arızalı parçalar gönderilmelidir. Bakım veya onarım amacıyla dışarıdan personel gelirse, kişisel verilerin kopyalanarak kurum dışına çıkarılmasını engellemek için gerekli önlemler alınmalıdır.

Kişisel veriler, sadece sistem yöneticisinin erişebileceği şekilde, ağ dışında yedeklenmelidir. Kişisel verilerin herhangi bir nedenle zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir

IV. AKILLI ŞEHİRLERDE VERİ GÜVENLİĞİNİN SAĞLANMASI

A. Akıllı Şehirlerde Veri Güvenliği ve Önemi

Akıllı şehirler, kaynakları verimli kullanmak, insanlar tarafından talep edilen hizmetin kalitesini artırmak ve yaşam kalitesini yükseltmek gibi hedeflenen amaçlara ulaşmak için sensörler veya başka teknolojik imkanlar vasıtasıyla insanlardan, binalardan, çevreden veya altyapıdan veri toplayan şehirlerdir. Toplanan bu veriler, enerji üretimi ve dağıtımı, atıkların toplanması ve geri dönüşümü, asayişin

sağlanması ve suçun tespiti, ulaşımın düzenlenmesi, kamu sağlığının sağlanması gibi amaçlarla kullanılır. Akıllı şehir fonksiyonlarının verimli bir şekilde yerine getirilmesi için nesneler arası ağ ile bilgi teknolojileri cihazları arası bağ kurulur, bu teknolojik alt yapı sayesinde hem şehide yaşayan insanların hem de şehrin altyapısının durumu takip edilir[197].

Akıllı şehirler, farklı sistemlerden toplanan verilerin bir araya getirilmesi ve analizi ile şehir faaliyetlerinin daha iyi yönetilmesini ve sürdürülebilirliğin artırılmasını hedeflediği ifade edilmektedir. Ayrıca, bu yaklaşımın, sınırlı kaynakların etkin bir şekilde kullanılmasına ve şehir hizmetlerinin daha verimli hale getirilmesine olanak tanıdığı belirtilmektedir.

Akıllı şehirlerdeki söz konusu gelişmeler, tüm toplumun iyileştirilmesine önemli katkı sağlamış olsa da neredeyse her akıllı uygulama, arka planda siber saldırılara karşı savunmasızdır[198]. Bu kapsamda akıllı şehir uygulamaları çok fazla saldırı türü ile karşı karşıya kalabilir ve istenmeyen sonuçlar ortaya çıkabilir.

- Kötü niyetli siber suçlular, casuslar veya yabancı devletler, güvenlik duvarlarını, şifreleme yöntemlerini veya diğer savunma mekanizmalarını aşmak için bir araya gelerek, akıllı şehirlere karşı koordineli bir şekilde iş birliği saldırısı yaparak büyük zararlar verebilir.
- Ağ üzerinde iletişim halinde olan iki ya da daha fazla cihaz arasındaki trafiği izleme amacıyla hedef cihazların arasına bir araç veya yazılım yerleştirmek suretiyle dinleme saldırı yapılabilir. Bu şekilde saldırgan gizli bilgilere erişebilir ve bu bilgileri kötü amaçlı amaçlarla kullanabilir.
- E-posta, anlık mesajlaşma, forumlar veya diğer çevrimiçi iletişim araçları yoluyla, zararlı yazılımların yayılması ve dolandırıcılık gibi amaçlarla birçok hedefe istenmeyen ve gereksiz mesajlar gönderilerek bir spam saldırısı gerçekleştirilebilir.

Sosyal medya ve diğer online platformlarda yer alan içeriklerin beğenme, takip etme veya yorum yapma gibi özelliklerini kötüye kullanarak manipüle etme girişimleri olabilir. Beğenme saldırıları, genellikle bir kişi veya bir grup tarafından,

[197] Barutçu, "*Akıllı Şehirler Üzerine Sistemik Bir Literatür Taraması ve Akıllı Şehirlerde Endüstri Mühendisliği Uygulama Alanları*", s. 3.
[198] Lei Cui, Gang Xie, Youyang Qu, Longxiang Gao, Yunyun Yang, "*Security and Privacy in Smart Cities:Challenges and Opportunities*", IEEE Access, C. 6, 2018, s. 46137.

bir siyasi görüşü desteklemek veya bir ürünü tanıtmak için yapay bir popülerlik yaratmak gibi amaçlar için gerçekleştirilir. Bu tür saldırılar, gerçek kullanıcıların davranışlarını yanıltabilir ve sahte bir algı yaratabilir, bu nedenle platformların güvenliği ve güvenilirliği açısından bir tehdit oluşturabilir.

Akıllı şehir sakinlerinden bir kişinin kimlik bilgileri ele geçirilip onun yerine geçerek veya sahte kimlik bilgileri kullanılarak, o kişinin hesapları ele geçirmek veya özel bilgilerine erişerek hukuka aykırı işlemler yapmak amacıyla kimlik saldırıları gerçekleştirilebilir. Bu saldırı türleri genellikle şifre, kullanıcı adı, doğum tarihi, sosyal güvenlik numarası gibi kişisel bilgileri hedef alır. Saldırganlar, bu bilgileri ele geçirdikten sonra birçok hizmette o kişinin yerine geçebilirler veya onun hesaplarına erişebilirler. Bu tür saldırılar, finansal suistimal, kimlik hırsızlığı ve siber suçlar gibi birçok amaç için kullanılabilir.

Akıllı şehir uygulamalarının üreticileri, hizmet sağlayıcılar ve bunları denetleyen kamu kurumlarının çalışanları, kaynaklara ve verilere erişim hakkına sahip oldukları için, bu haklarını kötüye kullanarak izinsiz olarak verilere erişmeye çalışabilir veya bu verileri yasadışı şekilde paylaşabilir. Örneğin, akıllı şebekelerdeki akıllı ölçüm altyapısı, sakinlerin yaşam alışkanlıklarını ve çalışma saatlerini de içeren özel hayatlarını izleyebilir. Akıllı mobilite uygulamaları tarafından toplanan büyük miktardaki rota bilgisi, bir kullanıcının konumunu ve hareketlilik desenlerini çıkarabilmek için kullanılabilir. Benzer şekilde, akıllı evler ve akıllı sağlık uygulamaları bağlamında, cihaz üreticileri ve hizmet sağlayıcıları hassas verilere erişebilir, kişisel verileri hızlı bir şekilde analiz edip hizmetlerin birincil amaçlarını aşan hassas bilgiler çıkarmak için veri madenciliği teknolojilerini kullanabilirler[199].

IoT tabanlı akıllı şehirlerde "*Botnet Faaliyetleri*" yapılabilir. Yani siber suçluların kontrolünde olan ve kendi kötü amaçları için kullanılmak üzere giren internete bağlı cihazlar, IoT ekosisteminde bulunan IP kameralar, web kameraları, yazıcılar, video kayıt sistemleri ve yönlendiriciler gibi cihazlar ile iletişime geçerek, bu cihazlara enfeksiyon yayabilir. Bu nedenle IoT botnetler, IoT sistemlerine ciddi tehditler oluşturmuştur. IoT cihazların güvenlik tasarımları bilgisayarlar ve akıllı telefonlara göre daha zayıftır. Maalesef, bu tehlike 2016'nın ikinci yarısına kadar fark

[199] Cui, Xie, Qu, Gao, Yang, "*Security and Privacy in Smart Cities:Challenges and Opportunities*", s. 46137.

edilmemiştir. Bu nedenle, siber saldırılar, IoT destekli ekosistem üzerinde yıkıcı bir etkiye sahip olabilir[200].

Akıllı şehirlerde trafik kazalarını azaltmak ve daha temiz çevre için geliştirilen sürücüsüz arabalar hacklendiği takdirde hem yaşam güvenliği hem de veri gizliliği için ciddi tehditler doğurabilir. Hackerlar uzaktan saldırılar gerçekleştirerek fren, direksiyon ve motoru kontrol edebilir. Akıllı şehir uygulamalarının tamamında sensörler tarafından depolanan veriler, gizlilik sızıntısı tehdidi altındadır. Çünkü her bir verinin hacklenip elde edilme ihtimali her zaman vardır[201].

Akıllı şehir uygulamalarındaki veriler, değiştirilmeye, bozulmaya, incelenmeye, yetkisiz erişime, açığa çıkarılmaya ve yok edilmeye karşı dayanıklı olmalıdır. Uygulamaların veriler için gizlilik, bütünlük, erişilebilirlik, inkar edilemezlik ve gizlilik gereksinimi karşılaması temel bir konudur. Akıllı şehir uygulamalarındaki zafiyetler nedeniyle akıllı şehir sakinleri güvenlik ve gizlilik sorunlarıyla karşı karşıya kalabilirler. Veri güvenliği ve gizliliği sağlanamazsa, halk akıllı şehir mobil uygulamalarını kullanmaktan çekinebilir. Birçok çalışma, vatandaşlar tarafından algılanan güvenlik ve gizliliğin akıllı şehir hizmetlerinde önemli olduğuna dikkat çekmektedir. Çalışmalar, teknoloji türüne, veri kullanımına ve konuma bağlı olarak gizlilik endişelerinin derecesinde farklılıklar olduğunu belirtmektedir. Akıllı şehirlerde insanlar kişisel olmayan verilerin amacı dışında kullanılmasından endişe ederken, kişisel verilerle ilgili de bir gözetim aracı olarak kullanılmasından endişe etmektedir. Kamuya açık alanlarda (örneğin tren istasyonları veya parklar gibi) suç tehdidi bulunduğunda, gözetim teknolojileri toplum tarafından kabul edilmektedir; ancak, algılanan tehdidin nispeten düşük olduğu daha özel alanlarda kamera veya mikrofonlar kullanılması açıkça reddedilmektedir[202].

Bu bulgular, vatandaşların gizliliğini korumak için yasal düzenlemelerin ve ihtiyaca uygun teknolojinin uygulanmasının önemini vurgulamaktadır. Bazı ülkeler, vatandaşlarının gizlilik haklarını yasal olarak korumaya yardımcı olan çeşitli yasalar geliştirmişlerdir. Örneğin, AB Genel Veri Koruma Tüzüğü (GDPR), IoT

[200] Cui, Xie, Qu, Gao, Yang, "*Security and Privacy in Smart Cities:Challenges and* Opportunities", s. 46137.
[201] Cui, Xie, Qu, Gao, Yang, "*Security and Privacy in Smart Cities:Challenges and Opportunities*", s. 46138.
[202] Elvira Ismagilova, Laurie Hughes, Nripendra P. Rana, Yogesh K. Dwivedi, "*Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework*", Information Systems Frontiers, 2022, s. 401.

sağlayıcılarının ve kullanıcılarının çıkarları arasında adil bir denge sağlamak için temel rehberlik sağlamaktadır[203].

B. Akıllı Şehirler ve Gözetim Toplumu

Gözetim, sistematik bir biçimde kişilerin hareketlerinin ve iletişiminin izlenmesidir. Bir başka açıdan bakılacak olursa, gözetim kişisel veri toplama işlemidir[204].

Gözetim kavramı insanlık tarihi kadar eski bir kavramdır. Gözetim kabile toplumlarında ve imparatorluklarda, toplumu kontrol altında tutmak için kullanılan ve egemenliği sağlama işlevi bulunan bir sistemdir. Anthony Giddens, Ugarit'teki bir arkeolojik çalışmada bulunan 508 tabletten 318 tanesinde ticari, idari ve istatistiksel bilgiler olduğunu göz önünde bulundurarak, yazının gözetimi kolaylaştırdığını ve modern olmayan devletlerde kayıt sisteminin uygulanmasının resmi olarak gözetim başlattığını ileri sürmektedir. Geleneksel toplumlarda gözetim, yönetici tarafından himayesi altında bulunan insanların denetim altında olması için yapılan, muhalif görüş ortaya çıktığında yöneticinin gücünü gösterecek şekilde varlığını hissettiren bir olgudur[205].

Modern öncesi toplumlarda gözetim, casusluk, dinleme ve röntgencilik şeklinde yapılmaktaydı.[206] Modern dünyada ise gözetim, teknolojik imkanların artması nedeniyle insanlar tarafından kabullenilen hatta yapılması talep edilen bir faaliyet haline gelmiştir. Özellikle büyük şiddet ve terör eylemlerinin artması sonucu insanlar güvenlik ihtiyaçlarının karşılanması için mahremiyetlerinden fedakârlık yaparak gözetlenmeye razı olmuşlardır[207].

Karl Marx'a göre gözetim, kapitalizmin doğması ile işçilerin fabrikada üretim kapasitelerini artırmak, fabrikadaki düzeni sağlamak ve üretim araçlarının

---

[203] Ismagilova, Hughes, Rana, Dwivedi, "*Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework*", s. 400.
[204] Elif Küzeci, "*Kişisel Verilerin Korunması*", s. 21.
[205] Yavuz Selim Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", (Yüksek Lisans Tezi, Muğla Sıtkı Koçman Üniversitesi Sosyal Bilimler Enstitüsü, Muğla 2022), s. 16 vd.
[206] Murat Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", (Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2022), s. 26.
[207] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 18.

mülkiyetlerini ele geçirmesini engellemek amacıyla sermayenin emek üzerinde kurduğu bir denetim sistemdir[208]. Modern dönemin merkezine bürokratik örgütlenmeyi koyan Max Weber'e göre gözetim, bürokrasiye doğrudan bağlıdır ve bürokrasinin oluşmasında önemli etkenlerden biridir. Bürokratik yönetim birey üzerinde dosyalama ve kayıt yaparak bir gözetim mekanizması geliştirmiştir[209].

Tarihsel bazda gözetim üç başlıkta ele alınmaktadır:

1- "*Pastoral Nitelikli Gözetim*": Kilise ve imparator gibi gücü elinde bulunduran yönetici kuruma bağlı bir şekilde itaat eden bireylerin denetimi söz konusudur.
2- "*Teknik Gözetim*": Devletler açısından bakıldığında iktidarın devamı ve devlet işleyişinin kontrol altında tutulması, kapitalimiz açısından bakıldığında da ekonomik gücün devamı için yapılan sistematik izlemedir.
3- "*Enformatik Gözetim*": Toplumsal algıların ve tercihlerin yönetilmesi için günümüz teknolojilerinin kullanılmasıyla yapılan gözetimi ifade eder[210].

Anthony Giddens'e göre toplumsal gözetimin "*veri toplamaya dayalı gözetim*" ve "*denetleyen gözetim*" olmak üzere iki görünümü bulunmaktadır. Gözetim bir kurum veya topluluk tarafından bireylerin eylemlerini yönetmek için, bireyler hakkında toplanan, depolanan ve sembollerle kodlanıp şifrelenen bilgi birikimi söz konusu ise "*veri toplama dayalı gözetim*"; otorite konumunda olan bireyin diğer bireylerin toplum içerisindeki eylemlerini izlediği ve bu şekilde bireylerin koordine edilmesi söz konusu ise "*denetleyen gözetim*" olarak nitelendirmiştir[211]. Bu ayrıma göre akıllı şehirlerdeki gözetim "*denetleyen gözetim*" değil "*veri toplamaya dayalı gözetim*" olmalıdır. Çünkü akıllı şehirlerde kurulan teknolojik altyapını amacı, bireylerin eylemlerini izlemek için değil veri analizi ile ortaya çıkacak optimum çıkarım doğrultusunda bireylerin eylemlerini yönlendirmek içindir.

---

[208] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 20.
[209] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 28.
[210] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 13.
[211] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 8.

Panoptikon, Jeremy Bentham tarafından tasarlanan, herkesi görebilecek bir konumda bulunan gözetleme kulesinin olduğu ancak bu kulede bulunan denetçinin görünmediği mimari yapıyı ifade etmektedir. Bentham gözetimi *"bugüne kadar örneği olmayan, zihin üzerinde zihinsel iktidar elde eden yeni bir yöntem"* şeklinde tanımlamaktadır. Panoptikon'un en önemli özelliği, hücrelerin içerisindeki mahkumların, her an gözetlenebilir olduklarını bilmesidir. Kuledeki gözetleyici, mahkumları her an izleyebilir, ancak mahkumlar gözetleyicinin kulede olup olmadığını bilemezler. Mahkumlar, potansiyel gözetimden dolayı kendilerini sürekli olarak izleniyor gibi hissederler ve bu nedenle her an cezalandırılabilecekleri korkusuyla hareket ederler. Bu modelde, her an gözetim yapılmasa bile mahkumlar her an disiplin altında tutulmaktadır. Dolayısıyla, panoptikon modeli, disiplin ve kontrolü içselleştiren bir toplum oluşturur.[212] Michel Foucault gözetimi, panoptikon gibi alanlarda otorite veya kontrol kurma süreci olarak ifade etmektedir[213].

Gözetimi disiplin bağlamında değerlendiren Foucault'a göre hapishane, fabrika ve askeriye gibi ortamlarda kullanılan gözetleme methotları toplumun her katmanına yayılmıştır. Modern toplumlarda insanlar daha fazla gözetlenmekte, sınıflandırılmakta ve belgelenmektedir. Panoptikon metaforunu "*disiplin toplumu*" kavramını açıklamada sembol olarak kullanan Foucault, toplumda herkesin yumuşak bir güçle disiplin altına alındığını belirtmektedir[214].

Gözetim toplumu araştırmacıları tarafından ortaya atılan kuramlar "*Panoptikon Merkezli Gözetim Teorileri*" ve "*Panoptikon Merkezli Olmayan Gözetim Teorileri*" olmak üzere ikiye ayrılmaktadır. Panoptikon merkezli gözetim kuramcıları, gözetimin şiddet ve baskı temelli, kontrol etme ve denetleme amaçlı, sosyal tabakalaşmada hiyerarşik ve iktidar merkezine yarayan bir faaliyet olduğunu ileri sürmektedirler[215]. Bu kuramcılara göre; Foucault'nun panoptikon kavramı, bir gözetim ve kontrol modelidir. Bu modelde, merkezi bir gözlem noktasıyla çevrelenen bireyler sürekli gözetim altındadır. Günümüz gözetim sistemlerinde kullanılan kameralar, sensörler ve diğer teknolojiler panoptikon tasarımına benzer bir

[212] Jeremy Bentham, Catherine Pease-Watkin, Simon Werret, Barış Çoban, Zeynep Özarslan, "*Panoptikon Gözün İktidarı*", 3. bs. Su Yayınları, İstanbul, 2019, s.9 vd.
[213] Küzeci, "*Kişisel Verilerin Korunması*", s. 29.
[214] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 30.
[215] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 14.

gözetim mekanizması uygulamaktadır. Bu nedenle, panoptikon kavramı, günümüzdeki gözetimi anlamak ve analiz etmek için kullanışlı bir kavramdır. Gözetim, genellikle baskı, disiplin, güç ve tahakküm kavramlarıyla ilişkilendirilir. Gözetim, bireylerin özgürlüklerini kısıtlayan ve toplumdaki güç dengesini etkileyen bir araç olarak algılanır. Bu nedenle olumsuz bir anlamı vardır. Genellikle devlet veya diğer otorite kurumları tarafından kontrol edilen gözetim mekanizmaları, bireyler üzerinde kontrol kurmak ve toplumun belirli kurallara uymasını sağlamak için kullanılır. Bu durum, güç ilişkilerini ve sosyal hiyerarşiyi pekiştirebilir ve bireylerin özgürlüklerini sınırlayabilir[216].

Panoptikon merkezli olmayan gözetim kuramcılarına göre ise, teknolojinin gelişimi, dijital izleme araçlarının yaygınlaşması ve farklı gözetim yöntemlerinin ortaya çıkması nedeniyle panoptikon kavramı günümüzdeki gözetimi tam olarak açıklamamaktadır. Günümüzdeki gözetim daha karmaşık ve çeşitlidir. Gözetimin hem olumlu hem de olumsuz etkileri olabilir. Bu nedenle, gözetim üzerine yapılan değerlendirmelerde tarafsız bir yaklaşım benimsemek önemlidir. Farklı perspektiflerden gözetimin avantajları, dezavantajları ve etik boyutları ele alınmalıdır. Gözetim sadece güvenlik veya kontrol amaçlı değil, aynı zamanda veri analizi, pazarlama, sağlık hizmetleri gibi diğer alanlarda kullanılmak üzere de yapılabilir. Veri toplama işlemi, bireylerin gizliliğine ve özgürlüklerine müdahale edebilirken aynı zamanda daha iyi hizmet sunumu, kişiselleştirme ve etkinlik artırma gibi avantajları da beraberinde getirebilir. Bu nedenle, gözetim üzerine yapılan analizlerin geniş bir perspektifi kapsaması önemlidir. Gözetim, sadece tek bir güç veya kurum tarafından uygulanan bir süreç değildir. Günümüzde gözetim, devlet, şirketler, kamu kurumları, medya ve diğer aktörlerin katılımıyla gerçekleşen ve teknoloji araçlarıyla desteklenen bir süreçtir. Bu nedenle, gözetim çoğulcu ve teknik bir süreç olarak kabul edilir[217].

Diana Gordon, devletlerin ve ticari şirketlerin sahip olduğu farklı kişisel veri tabanlarının birbirleriyle bağlantılı olduğunu ve bu durumun tüm toplumun elektronik panoptikon altında olduğunu vurgular[218]. Gordon, bireylerin kişisel

[216] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 23.
[217] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 24.
[218] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 35.

verilerinin çeşitli kurumlar ve şirketler arasında paylaşılması ve bu verilerin toplu bir şekilde izlenmesi ve analiz edilmesi durumunda, bireylerin hareketleri, tercihleri ve davranışları hakkında geniş bir bilgi birikimi oluşacağına ve bu bilgilerin kullanımıyla bireyler üzerinde etkili bir gözetim ve kontrol mekanizması oluşabileceğine dikkat çekmektedir. Elektronik panoptikon, bireylerin gözetim altında hissettiği bir ortamı tanımlar ve kişisel verilerin toplu olarak kullanılmasının potansiyel risklerine dikkat çeker.

Mark Poster bir adım daha ileri giderek süper-panoptikon kavramını ortaya atmıştır. Poster, bilgisayar veri tabanlarının insanları gözetlemesini ve profillemesini ele alarak süper-panoptikon kavramını geliştirmiştir. Poster'a göre, dünyamızı saran elektrik devreleri ve telefon kabloları, süper-panoptikon kavramının uç noktalarını temsil eder. Artık bilgisayar veri tabanları, panoptikonun sınırlarını hapishanelerden dışarı çıkarmıştır[219]. Poster bu yaklaşımında, bilgisayar veri tabanları sayesinde bireylerin çevrimiçi etkinlikleri, iletişimleri ve diğer dijital izlerinin toplanması ve analiz edilmesi yoluyla, insanların davranışları, tercihleri ve alışkanlıkları üzerinde geniş çaplı bir izleme ve kontrol mekanizması oluşturulabileceğine dikkat çekmektedir. Bu durum bilgi ve iletişim teknolojisi ve sensörlerle donatılmış akıllı şehirler için de geçerlidir. Akıllı şehirlerin her alanında veri toplayan akıllı cihazlar, tıpkı panoptikon modelindeki kuleden her an gözetlendiğini düşünen mahkumlar gibi, akıllı şehir sakinlerinin dijital gözetim ve kontrol altında her an denetleniyormuş gibi hayat yaşamalarına neden olabilir. Bu durum, bireylerin özgürlüklerini kısıtlayabilir ve toplumun güçlü otorite tarafından kontrol edildiği bir yapı oluşturabilir.

"*Gözetim Toplumu*" kavramını ilk ortaya atan Garry T. Marx, gözetim toplumunu açıklarken "*günümüz gözetim toplumu fiziksel, sosyal ve kişisel alanlarda daha derinlere inebilir; fısıltıları duyar ve duvarlara, pencerelere, bulutlara ve karanlığa nüfuz eder*" diyerek günümüz teknolojik gözetleme araçlarının her yerde olduğuna dikkat çekmektedir[220]. Marx'a göre günümüz gözetim anlayışı ile eski gözetim anlayışı arasında birkaç noktada farklılıklar bulunmaktadır. Eskiden gözetim zorlamaya dayanırken günümüzde kabul ve iknaya dayanmaktadır. Eskiden bilgiler

[219] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 36.
[220] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 22.

tek merkezden toplanıp saklanırken günümüzde veri toplama daha kolay ve veri paylaşımı da mümkün haldedir. Eskiden gözetleyen anlık gözetleme yaparken günümüzde geçmiş, o an ve hatta gelecek dahi gözetlenebilmektedir. Eskiden gözetleme küçük bir kesimin elindeyken günümüzde çok daha geniş bir kitle gözetleme imkanına sahiptir. Gözetlenen açısından da eskiden sınırlı bireyler gözetleniyorken günümüzde neredeyse herkes gözetlenebilmektedir. Eskiden gözetim teknikleri belli iken günümüzde gözetimi fark etmek çok da kolay olmamaktadır[221].

Gerçekten de akıllı şehirlerde verileri toplamak üzere yapılandırılan teknoloji altyapısı hayatın her alanında karşımıza çıkacaktır. Akıllı şehir teknolojilerinde sadece ses ve görüntü değil internet sitelerinde gezdiğimiz siteler, konumumuzun hareketleri, tükettiğimiz enerji verisinden attığımız çöpün verisine kadar çok geniş bir yelpazede veri toplanacağı için yeni gözetim tekniklerinin duyusu çok sayıdadır. Akıllı şehir insanları hayatın kolaylaşması ve refah seviyesinin yükselmesi için bu gözetlemeye de rıza göstermektedir. Akıllı şehirlerde veri toplama rutin bir şekilde her zaman ve fark ettirmeden yapılmaktadır. Veriler kaydedilebildiği için geçmiş hakkında, şu an için ve analizler yöntemiyle de gelecek için fikir verecek şekildedir. Akıllı şehir teknolojileri belirli bir kesim için değil tüm insanlar içindir. Sonuç olarak, akıllı şehirler Marx'ın post modern bilgisayar destekli gözetim modeline birebir uymaktadır. Marx'ın fikirleri doğrultusunda, akıllı şehirlerin bir gözetim toplumu yaratacağı çıkarımı yapılmaktadır.

Şüphesiz akıllı şehirlerde kullanılan gözetim araçlarının birçok faydası bulunmaktadır. Suçun önlemesi, işlenmiş suçun aydınlatılması, trafiğin düzenlenmesi, enerji kaynaklarını izlenmesi, doğal afetlerin meydana getirdiği hasarların en aza indirilmesi gibi daha önceki bölümlerde bahsettiğimiz birçok faydası bulunmaktadır. Zaten akıllı şehirler kavramını ortaya çıkaran ve bu kavrama önem verilmesini sağlayan da bu gözetim araçlarının refah seviyesini yükseltmek için kullanılıyor olmasıdır. Ancak bunun karşısında akıllı şehirlerde, kişinin özel hayatının korunmasının zorlaşması, bireyin, ekonomik değeri olan bir meta olarak görülmeye başlanması gibi tehditlerin de olduğu söylenebilecektir. Bu risklerin

[221] Aydın, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", s. 20 vd.

önünü alabilmek için akıllı şehirlerde kişisel verilerin korunması için hukuki düzenlemeler yapılmasına ihtiyaç bulunmaktadır.

Ayrıca burada şu soruların sorulması gerekir: Egemen güçler akıllı şehir kavramıyla insanlara daha yüksek standartlarda, rahat bir hayat yaşama şartlarını sunarken, acaba post-modern gözetim toplumunu inşa etmek için halkın onay ve rızasını almak mı istemektedir? Bir cennet gibi sunulan akıllı şehirler baskıcı, kontrol ve denetleyici bir süper-panoptikon modeline dönüşebilir mi? Akıllı şehirlerde teknolojik altyapıyı oluşturan akıllı sistemler, iktidarın kendi gücünü artırıp devamlılığını sağlamak ve bireylerin zihinlerini kontrol etmek için kullanılabilir mi? Bu konuda endişeleri olup bu endişeleri nedeniyle akıllı şehirler kavramına karşı çıkan insanlar bulunmaktadır. İşte bu noktada, iktidarın kendisi göstermeksizin sanal bir tahakküm kurmaması için kişisel verilerin toplanması, depolaması, analiz edilmesi, silinmesi, yok edilmesi ve başka yerlere aktarılması süreçlerinin insan onuruna, temel hak ve özgürlüklere, modern demokratik devletin gerekliliklerine ve hesap verebilirlik ilkesine uygun bir biçimde yapılması gerekmektedir.

C. Temel Hak ve Özgürlükler Yönüyle Değerlendirme

Geride kalan bölümlerde kişisel verilerin korunması hakkının hukuki niteliği konusunda ekonomik hak yaklaşımı ve insan hakkı yaklaşımı olmak üzere temelde iki yaklaşımın olduğunu belirtmiştik. Bu başlıkta, kişisel verilerin korunması hakkı diğer temel hak ve özgürlük yönüyle değerlendirilecek ve ardından bu bilgiler ışığında akıllı şehirlerde kişisel verilerin korunması hakkının neden önemli olduğu tartışılacaktır.

1. Kişilik Hakkı ve Veri Güvenliği

Kişilik hakkının ne demek olduğu net bir şekilde kanun koyucu tarafından tanımlanmamıştır. Mehaz İsviçre Hukuku, kişilik hakkı kavramının çerçevesini çizip, içeriğinin doldurulmasını doktrin ve içtihatlara bırakmıştır. Kişilik hakkı, kişiye sıkı sıkıya bağlı, herkese karşı ileri sürülebilen, sınırlandırılamaz ve vazgeçilemez haklardır. Kişilik haklarının, beden ve ruh sağlığı, kişinin hayatı, vücut tamlığı gibi maddi bütünlüğe ilişkin değerleri; şeref ve haysiyet, özgürlük, isim, sırlar, resim gibi manevi bütünlüğe ilişkin değerleri; mesleki kimlik, ekonomik durum, ticari sırlar gibi ekonomik bütünlüğe ilişkin değerleri kapsadığı kabul edilir. Kişilik hakkının

sınırları net olmadığı için gelişen teknoloji ile kişisel veriler de çok rahat bir şekilde bu kapsamda değerlendirilebilecektir. Çünkü kişisel veriler, kişinin adı, resmi, sesi, parmak izi gibi kişilik hakkı kapsamında ele alınan değerlere karşılık gelmektedir. Bu nedenle kişisel verilerin korunması için, kişilik hakkını koruyan hükümlere müracaat edilebilecektir[222].

2. İnsan Onuru ve Veri Güvenliği

İnsan onuru, insanı diğer canlılardan ayıran, insanın insan olmasından dolayı sahip olduğu en üstün ve vazgeçilmez bir özdeğerdir. İnsan haklarının temelini insan onuru oluşturmaktadır. Bu nedenle insan hakları belgelerinde önem verilen bir kavramdır. İnsan onuru, insanı iç dünyasında değerli hissettiren bir kavramdır. Alman Anayasa Mahkemesi insan onurunu *"İnsan onuru, insanın bizzat kendisinden sorumlu olması, tinsel-ahlâkî bir varlık olup kendini gerçekleştirme özgürlüğüne sahip olması demektir."* şeklinde tanımlamıştır. Yüksek Mahkeme insan onurunun ihlal edilip edilmediğini değerlendirirken "*obje formülü*" kullanmaktadır. Kişi, basit bir araç veya obje olarak görülmüşse, insan onurunun ihlal edildiği sonucuna varmaktadır[223].

Alman Federal Anayasa Mahkemesi'nin 15 Aralık 1983 tarihli, Nüfus Sayım Yasası hakkında verdiği karar kişisel verilerin korunması konusunda önemli bir karardır. Nüfus sayımında vatandaşlara yüz altmıştan fazla anket sorusu sorulmasını, ankete verilecek cevapların kişilerle eşleşme yapılabilecek şekilde işlenmesini, bu kayıtların uzun süre saklanmasını ve bu kayıtların ikamet bilgilerinin karşılaştırılması için kullanılacak olmasını düzenleyen yasa insanlardan tarafından endişeyle karşılanmıştır. Bu konu hakkında karar veren Alman Yüksek Mahkemesi, "*bireyin kişisel verilerinin geleceğini tayin hakkı*"nı tanımlayarak bu hakkın insan onuru ve kişiliği serbestçe geliştirme hakkının bir gereği olduğunu belirtmiştir[224].

"Kişisel verilerin korunması kişinin maddi ve manevi varlığını geliştirmesine imkân tanıyarak bireyin hayatını kendi özgür iradesiyle düzenlemesine katkı sağlamaktadır. Bireyin kişisel verileri üzerindeki hakkı yeteri kadar korunmazsa

---

[222] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 75 vd.
[223] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 173 vd.
[224] Ezgi Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", (Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2020), s. 51 vd.

kişiliğini serbestçe geliştirmesi zora gireceğinden özgür iradeleriyle yaşamlarını biçimlendiren bireylerden oluşan demokratik bir toplum düzeninin ortaya çıkması ve korunması da güçleşecektir. Kişinin maddi ve manevi varlığını geliştirmesi ancak ve ancak faaliyetlerini özgürce gerçekleştirmesi ile mümkündür. Kişisel verilerin korunmasıyla, kişisel veri toplanması, saklanması ve işlenmesi sırasında bireyin hak ve özgürlüklerinin korunarak demokratik toplum düzeninin oluşmasına katkı yapmak hedeflenmektedir. (Federal Almanya Anayasa Mahkemesi, Nüfus Sayımı Kanunu kararı, BVerfGE, 65, 1 - Volkszählung, 15/12/1983)[225].

Kural olarak bireyin özel hayatını kendi tercihleri ile nasıl şekillendirdiği, bir başka kişinin veya devletin ilgi alanına girmemelidir. Yaşam ilişkilerine ait tüm kişisel verilerinin kapsamlı bir kaydı tutulan ve özel yaşamının gizliliği adeta ortadan kalkan bireyin kişiliğini geliştirmesi mümkün değildir. Kişisel verilerin korunması hakkı ihlal edildiğinde bireyin diğer temel hak ve özgürlükleri kullanması zorlaşmaktadır. Kayıt altına alınan veya alındığını düşünen birey kendi özgür kişiliğinin gereği gibi değil kendisinden istenilen veya beklenilen davranış tarzıyla hareket edecektir. Bireyler çeşitli faaliyetlerinin devlet tarafından izleneceği endişesiyle bunları gerçekleştirmekten vazgeçebilirler. Aykırı hareket tarzlarının sürekli kayıt altına alındığını düşünen birey, örneğin örgütlenme, toplantı ve düşünce özgürlüklerini kullanmama eğilimine girecektir. Eğer insanlar seyahat etmek, iletişimde bulunmak gibi belli eylemlerin hükümet tarafından yakından izleneceğini düşünürlerse, bu eylemleri gerçekleştirmekten kaçınabilirler ve yasal faaliyetlerinde kendi kendilerini sınırlama eğilimine girebilirler. Bu durum kişinin özerkliğini etkileyerek yurttaşların özgür iradeleriyle kendi yaşamlarını belirleyebildikleri özgürlükçü demokratik esaslara dayanan bir toplum düzeninin oluşmasını engelleyecektir. (Federal Almanya Anayasa Mahkemesi, Nüfus Sayımı Kanunu kararı, BVerfGE, 65, 1 - Volkszählung, 15/12/1983)"[226].

Türk Anayasa Mahkemesi kişisel verilerin korunmasındaki amacın, herhangi bir sınır olmaksızın kişisel veri toplayan ve kullanan teknoloji karşısında zayıf ve savunmasız hale gelen bireyin korunması olduğunu vurgulamaktadır. AYM'e göre de kişisel verilerin korunması hakkının temelinde insan onuru ve kişiliğin serbestçe

[225] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 84.
[226] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 85.

geliştirilmesi hakkı bulunmaktadır[227]. *"Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır"* (AYM, E.2014/122, K.2015/123, 30/12/2015, §§ 19, 20; Nurcan Belin, § 45)[228]. Bu açıdan bakıldığında kişisel verilerin korunması, Anayasa'nın 5. maddesinde belirtilen devletin temel amaç ve görevleri arasında sayılan *"insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak"* ile doğrudan ilişkilidir.

3. Özel Hayatın Gizliliği Hakkı ve Veri Güvenliği

Toplumsal bir varlık olan insan, evde, iş yerinde, okulda, sokakta, seyahatte, alışverişte, hastanede, sporda kısacası hayatı boyunca her ortamda ailesi, arkadaşları ve tanımadığı başka insanlarla iletişim halindedir. İnsanın kurduğu bu ilişkiler kişinin "*hayat alanı*"nı oluşturmaktadır. Hayat alanı üçe ayrılmaktadır:

1- Ortak Hayat Alanı: Belirli ve sınırlı olmayan insanlardan oluşan, toplumsal hayatın yaşandığı, kamusal alandır.
2- Özel Hayat Alanı: Belirli ve sınırlı olan insanlardan oluşan, aile, arkadaş ve güvenilen kişilerin oluşturduğu, herkese açık olmayan alanı ifade eder.
3- Sır Alan: Hayat alanı kapsamında en dar olan alan olup, kişinin kimseyle paylaşmadığı veya çok az sayıda güvendiği insanlarla paylaştığı, başka kişilerce bilinmesini istemediği alandır[229].

En geniş çapta olan ortak hayat alanında kişilik hakları neredeyse hiç korunmamaktadır. Kişinin özel hayat alanı ve sır alanında bulunan olguların, bu alanlarda olmayan kişilere ulaşması kişilik hakkını ihlal edecektir. Ancak bu alanların sınırlarını net bir şekilde çizmek mümkün değildir. Korunmak istenen değerin gizlilik düzeyine göre yorum yapılacaktır. Kişisel veriler ise bu üç alanın hepsinde bulunabilecek verilerdir.

Özel hayatın gizliliği hakkı, kişinin özel hayat alanını, devletin ve diğer bireylerin müdahalesine karşı korumayı sağlayan bir haktır[230]. İlk defa 1890 yılında

[227] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 83.
[228] AYM, Ümit Eyüpoğlu, B. No: 2018/6161, 28/6/2022, § 38.
[229] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", s. 48 vd.
[230] Mehmet Şükrü Gündüz, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği"*, 1. bs., Adalet Yayınevi, Ankara, 2022, s. 90.

Harvard Hukuk Fakültesi Dergisi'nde yayınlanan bir makalede Samuel Warren ve Louis Brandeis tarafından "*the right to be let* alone" (*yalnız bırakılma hakkı*) olarak nitelendirilerek ortaya atılmış bir haktır[231]. Günümüzde ise insan hakları belgelerinde ve anayasalarda bir insan hakkı olarak tanımlanmaktadır. Kişisel verilerin güvenliği hakkı ise, özel hayatın gizliliği hakkına birebir karşılık gelmese de özel hayatın gizliliği hakkı kapsamında doğan, henüz yeni yeni bu haktan bağımsız bir hak olarak tanımlanmaya başlanan bir haktır. İnsan Hakları Evrensel Bildirgesi'nde kişisel verilerin korunması hakkı ayrı bir hak olarak düzenlemese de 12. maddede düzenlenen "*Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır*." hükmü değerlendirilmiştir[232].

Avrupa İnsan Hakları Mahkemesi de özel hayat kavramının kişisel verileri de kapsayacak şekilde geniş yorumlanması gerektiğini ifade etmektedir[233]. 4 Aralık 2008 tarihli *S. ve Marper / Birleşik Krallık* kararında AİHM, *"Bir kimsenin özel hayatına dair verilerin saklanması, kendi başına, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin anlamı dâhilinde bir müdahale teşkil etmektedir. Söz konusu Sözleşme maddesi kişinin özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkını1 düzenlemektedir"* demektedir[234]. Avrupa Birliği Temel Haklar Şartı'nda özel hayatın gizliliği hakkı ile kişisel verilerin korunması hakkı ayrı ayrı düzenlenmiştir. ABD, Kanada, Avustralya, Yeni Zelanda gibi birçok ülkede yapılan iç düzenlemelerde kişisel verilerin korunması hakkı, özel hayatın gizliliği hakkının uyarlanmış hali olarak kabul edilmiştir[235].

Anayasa Mahkemesi'ne göre özel hayat kavramı, net bir şekilde tanımlanabilecek kadar dar bir kavram değildir. Bu kavram ile korunmak istenen hukuki değer kişisel bağımsızlıktır. Kişisel bağımsızlık kavramı ise sadece, dış alandan ayrı tutulan bir alanda özgürce yaşamak demek değildir. Kişiye özel bir sosyal hayat yaşamak da özel hayatın gizliliği kapsamında güvence altına

[231] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 80.
[232] Dülger, "*Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması*", s. 75.
[233] Gündüz, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*", s. 93.
[234] AİHM Büyük Daire- S. ve Marper/Birleşik Krallık, 30562/04, 04.12.2008, § 67.
[235] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 183.

alınmaktadır[236]. Özel hayata saygı hakkının unsurlarından biri olan mahremiyet hakkı, kişiye yalnız bırakılma hakkını tanımanın yanı sıra kişinin kendisiyle ilgili bilgilerin rızası olmaksızın kullanılmasını, erişilmesini, aktarılmasını ve ifşa edilmesini engellemektedir[237].

4. İfade Özgürlüğü ve Veri Güvenliği

Düşünce, insan beyninin bir fonksiyonu olan düşünme faaliyeti sonucu ortaya çıkan ürünlerdir. Çıktısı düşünce olan bu fonksiyonun girdisi ise bilgidir. Bir başka ifade ile, bilgi sahibi olmaksızın düşünce sahibi olmak imkansızdır. Bu nedenle düşüncenin oluşu için bilgi edinmek şarttır. Bilgi edinen insan, sahip olduğu bilgileri beyin süzgecinden geçirerek yani kendine göre bir değerlendirmeye tabi tutarak, bir kısmını eleyip kalan kısmıyla çıkarımlar yaparak bir kanaate sahip olur. Bu kanaatin dışa vurulmasına da ifade etmek denir. İfade özgürlüğü bu sürecin tamamını kapsamaktadır. Bu nedenle ifade özgürlüğü, bilgiyi elde etme kanalını korumak için "*haber alma ve öğrenme özgürlüğü*", edinilen bilgiler sonucu kişinin vardığı kanaatlerden kınanmamayı ifade eden "*kanaat özgürlüğü*" ve sahip olunan düşüncenin dışa vurulması süreci yani "*düşünceyi açıklama ve yayma özgürlüğü*" olmak üzere 3 temel unsurdan oluşur[238].

Düşünceyi açıklama ve yayma özgürlüğü, kişinin sahip olduğu bilgi ve düşüncelerin açıklamaya zorlanmamasını teminat altına almaktadır. Başkaları tarafından öğrenilmesi istenilmeyen bilgilerin müdahale ile elde edilmesinin önüne geçmektedir. Bu açıdan bakıldığında kişisel verilerin korunmasına da hizmet etmektedir. İnsanlar, kişisel verilerin açıklanmasına zorlanamamakta ve bu şekilde kişisel verilerin güvenliği sağlanmaktadır. Düşünceyi açıklama ve yayma özgürlüğü, kişisel verilerin ancak rıza ile elde edilme ilkesini destekler niteliktedir. Düşünceyi açıklama ve yayma özgürlüğü ile kişi, kişisel bilgisini açığa çıkartıp çıkarmama hususunda serbest olmaktadır ve kişisel verilerin hangi koşullarda ve kimlerle paylaşacağı konusunda seçim hakkına sahip olmaktadır[239].

İfade özgürlüğü ile kişisel verilerin korunması hakkı, basın özgürlüğü konusunda çatışma göstermektedir. Basın, toplumun göz önünde bulunan sanatçı,

---

[236] AYM, Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 31
[237] AYM, Serap Tortuk, B. No: 2013/9660, 21/1/2015, § 32
[238] M.Emin Artuk, Ahmet Gökçen, M.Emin Alşahin, Kerim Çakır, "*Ceza Hukuku Özel Hükümler*", 18. bs., Adalet Yayınevi, Ankara, 2019, s. 878.
[239] Gündüz, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*", s. 94 vd.

siyasetçi, sporcu, yönetici gibi kişiler hakkında bilgileri meraklı takipçilere ulaştırmak istemektedir. Söz konusu kişiler ise yalnız bırakılma hakkını kullanmak istediklerinde bir çekişme çıkmaktadır. Basın özgürlüğü kişisel verilerin korunmasını engellerken, kişisel verilerin korunması hakkı basın özgürlüğünü sınırlamaktadır. Bu durumda her iki hakkın da ayakta kalacağı bir denge noktası bulunmalıdır. Bu denge noktası, olaya özgü koşullar göz önünde tutularak orantılılık ilkesi gereğince tespit edilecektir[240].

5. Din-İnanç Özgürlüğü ve Veri Güvenliği

Din ve inanç özgürlüğü, bireylerin dini bir inanca sahip olma veya olmama, inancını değiştirebilme, inandığı dini inanç doğrultusunda yaşama özgürlüklerini içermektedir[241]. İnançlar kişinin iç evreni (forum internum) kapsamındadır. Bir başka ifadeyle, kişinin mahrem alanında bulunmaktadır ve açıklamaya zorlanamaz. Din ve inanç özgürlüğü kapsamında bulunan veriler, belirli veya belirlenebilir bir kişi ile bağlantı kurabildiği durumlarda kişisel veri niteliği taşıyacaktır. Üstelik bu kişisel veriler, hassas veri sınıfında olup daha özel korunmaktadır. Bu bakımdan din ve inanç özgürlüğü ile kişisel verilerin korunması hakkı birbirini destekleyici haklardır[242].

6. Haberleşme Özgürlüğü ve Veri Güvenliği

Haberleşme, kişiler arası yazılı veya sözlü olarak bilgi ve düşüncelerin aktarılmasıdır. Haberleşme özgürlüğü, iletişimin içeriğini korumakta ve haberleşmenin gizliliğini güvence altına almaktadır. Ayrıca haberleşmenin içeriği ile ilgili olmasa da görüşme trafiği, görüşme süresi, sayısı, görüşme olsun veya olmasın aranan ve arayan kişilerin bilgileri gibi verilerin korunması da bu hak kapsamındadır. Haberleşme esnasında kişiyi belirlenebilir kılan tüm veriler ve haberleşme kapsamı dışındaki iletişim trafiği verileri kişisel veri niteliğinde olup, haberleşme özgürlüğü de bu kişisel verileri korumaktadır[243].

Gelişen teknoloji ile iletişim kurma kanalları da çoğalmıştır. Klasik telefon görüşmelerine alternatif olarak birçok sayısal hale gelen yöntemler ortaya çıkmıştır. Belge paylaşma, ses ve yazı iletme, görüntülü iletişim kurma amacıyla birçok

[240] Küzeci, "*Kişisel Verilerin Korunması*", s. 96 vd.
[241] Tezcan, Erdem, Sancakdar, Önok, "*İnsan Hakları El Kitabı*", s. 484.
[242] Gündüz, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*", s. 102 vd.
[243] Gündüz, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*", s. 99.

uygulama geliştirilmiştir. Bu durum iletişime müdahale yollarını da artırmıştır. Yani günümüzde iletişime müdahale etmek eskisine göre çok daha kolay bir hal almıştır. Çünkü sadece görüşme esnasındaki ses değil, iletişim için kullanılan uygulamaya ilişkin kullanıcı adı, şifre, IP, ID ve diğer log kayıtları da kişiler hakkında bize bilgi vermektedir. Örneğin, kişinin irtibata geçtiği kişilerden yola çıkılarak sosyal çevresi hakkında bilgi elde edilebilir, görüşme sıklığı kullanılarak kişiler arası ilişki hakkında kanaate varılabilir, IP bilgilerinden konum verisi elde edilebilir. Görüldüğü sadece ses ve yazı elde edilmekle değil, dijital ortamda iz bırakan her verinin elde edilmesiyle gibi iletişime müdahale olabilir.

AİHM de, kamu otoritelerinin- her ne kadar görüşme içeriğine bakılmamış olsa da– iletişime dair veri trafiğinden yola çıkılarak sonuç çıkartılmasını özel yaşamın gizliliği hakkı ve haberleşme özgürlüğü kapsamında değerlendirmektedir. *Malone / Birleşik Krallık* (B. No:8691/79, K. T: 02/08/1984) kararında telefon hizmet sağlayıcısının abonelerin faturalandırılması için kullanılan sayaç denetim yazıcısının verilerinin polise verilmesini Sözleşme'nin 8.maddesine aykırı bulmuştur[244].

7. Bilgi Edinme Hakkı ve Veri Güvenliği

Bireyin devlet karşısında korunması ve idarenin şeffaflaşması açısından önemli bir yeri bulunan bilgi edinme hakkı, kişinin devletin elinde bulunan verilere erişmesini sağlayan haktır. Kişisel verilerin korunması hakkı ile bilgi edinme hakkı "*bilgi toplumu hukukunun iki sütunu*" ve "*bir madalyonun iki yüzü*" olarak nitelendirilmiştir. Çünkü her iki hak da kişilerin kendileri hakkında tutulan verilere erişmesini sağlamakta ve iki hak için de yapılan düzenlemeler bir arada görülmektedir. Kendisi hakkında devletin tuttuğu verilere erişen kişi, kayıt altına alınan kişisel verilerinin neler olduğunu, bu verilerin doğru ve güncel olup olmadığını görebilecektir. Bilgi edinme hakkı kişiye sadece kendi verilerine erişme imkânı tanımaktadır, kişinin üçüncü bir kişi ile ilgili verilere erişmesi mümkün değildir. Bu açıdan bakıldığında da kişisel verileri koruyan bir fonksiyonunun da olduğu görülmektedir. Sonuç olarak bilgi edinme hakkı ve kişisel verilerin korunması hakkı birbirini tamamlayan haklardır[245].

[244] Küzeci, "*Kişisel Verilerin Korunması*", s. 109.
[245] Küzeci, "*Kişisel Verilerin Korunması*", s. 102 vd.

D. Akıllı Şehirlerde Kişisel Verilerin Korunması Hakkının Önemi

Kaynakları verimli bir şekilde kullanmayı, insanların talep ettiği hizmet kalitesini artırmayı ve yaşam kalitesini yükseltmeyi hedefleyen akıllı şehirler, enerji üretimi ve dağıtımı, atık yönetimi ve geri dönüşüm, güvenlik sağlama ve suçun tespiti, ulaşım düzenlemesi, kamu sağlığı gibi amaçlar için sensörler veya diğer teknolojik araçlar aracılığıyla insanlardan, binalardan, çevreden veya altyapıdan veri toplayan şehirlerdir. Verilerin toplanması için kurulan altyapı o kadar geniştir ki, insanlar hayatın her alanında sensör ve diğer araçlarla yoğun bir şekilde kontrol altında tutulmaktadır.

Her daim izlenip, hayatına dair bilgileri kaydedilen ve bundan dolayı şeffaflaşan bir bireyin kendi kişiliğini serbestçe geliştirebilmesi mümkün değildir. Çünkü böyle bir ortamda kişi, kendisini belli bir davranış kalıbında hareket etmek zorunda hissedebilir. Çevresinde sensörler bulunan ve kendisi de sensörler içeren kıyafetler giyen birey, teknolojik altyapı açısından bir obje olarak görülecektir. Teknolojik altyapının bu bakış akısı zamanla devlet idaresinin de vatandaşa olan bakış açısını etkileyecek ve devlet de bireyleri birer obje gibi görmeye başlayabilecektir. Bireyin devlet tarafından her an ulaşılması mümkün bir veri nesnesi olarak alçaltılması, devletin kendisinde bireyi yoğun bir şekilde izlemeye yetkili görmesi durumunda insan, özdeğerini kaybedecek ve insan onuru sıfırlanacaktır[246].

2017 yılında, Facebook yöneticileri tarafından hazırlanan ve Avustralya'da yayımlanan "*The Australian*" adlı gazetenin ele geçirdiği rapora göre, Facebook Avustralyalı ve Yeni Zelandalı gençlerin kendilerini "*değersiz*" ve "*güvensiz*" hissettikleri, "*özgüvene ihtiyaç duydukları*" anları bilebilme kapasitesine sahiptir. Platform gönderileri, etkileşimleri ve fotoğrafları gerçek zamanlı olarak izleyerek, gençlerin ne zaman "*stresli*", "*yenik*", "*bunalmış*", "*endişeli*", "*gergin*", "*işe yaramaz*" ve "*başarısız*" hissettiklerini belirleyebilmektedir. Sızan bu belgeye göre Facebook, gençlerin mevcut ruh halleri ve ruhsal değişimleri hakkında ayrıntılı

[246] Duman, "*Anayasa Hukukunda Kişisel Verilerin Korunması*", s. 176.

veriler oluşturabilirken aynı zamanda onların ruh hallerini etkileyecek güce de sahiptir[247].

Akıllı şehirlerde kişisel verilerin toplanması, depolanması ve analiz edilerek sonuç çıkarılması süreci tek yönlü bir süreç değildir. Kişiden büyük veriye doğru olan veri akışı sonrasında büyük veriden de kişiye doğru da bir veri akışı olmaktadır. Büyük veriden kişiye olan veri akışının amacı kişinin kendisi için en uygun karara varmasını sağlamaktır. Örneğin akıllı ulaşım uygulamalarında kişilerin konum verileri ile şehir trafiğinin yoğunluk haritası çıkartılır. Kişi trafiğe çıktığında uygulama kişiye hedeflediği konuma gitmek için en uygun rotayı gösterir. Ancak yukarıda bahsedilen rapor bize göstermektedir ki, büyük veriden kişiye doğru olan veri akışı kişiyi manipüle etme amacı taşıyabilir. Bu kabiliyet günümüz bilgi ve iletişim teknolojilerinde bulunmaktadır. Kamu hizmetlerinin yerine getirilmesi için elde edilen büyük verinin idarenin elinde olduğu düşünüldüğünde, bu veriler siyasi otorite tarafından bireylerin fikir dünyasını manipüle etme, hayat tarzını belirleme ve itaati artırma amacıyla kullanılma riski bulunmaktadır. Bu durum, bir taraftan onuru incinmiş, mahremiyeti zedelenmiş ve özgür iradesini kaybetmiş bir birey, diğer taraftan ise bireyi kendi çıkarları uğruna yönlendiren bir otorite doğmasına sebep olacaktır.

Önceki bölümde insan onuru ile kişisel verilerin güvenliği arasındaki ilişki incelenirken, Alman Federal Anayasa Mahkemesi'nin insan onurunun ihlal edilip edilmediğini "*obje formülü*" kullanarak tespit ettiğini, kişinin, basit bir araç veya obje olarak görülmesi durumunda insan onurunun ihlal edildiği sonucuna vardığını belirtmiştik. Ayrıca Alman Yüksek Mahkemesi'nin bireyin kişisel verilerinin geleceğini tayin hakkını tanımlayarak bu hakkın insan onuru ve kişiliği serbestçe geliştirme hakkının bir gereği olduğunu belirttiğini vurgulamıştık.

Bu bilgiler açısından bakıldığında, akıllı şehirlerde kişisel verilerin korunması hukuku düzenlemeleri, başta kişiyi bir eşya veya obje olarak algılanmasının önüne geçerek, insan onurunu koruyan bir mekanizma olacaktır. Ayrıca kişisel verilerin hukuka aykırı olarak ve sınırsız bir şekilde toplanması, depolaması, işlenmesi, ifşa edilmesi karşısında, kişiye temel bir hak sağlayacaktır. Kişinin hiçbir baskı altında kalmaksızın kendi hayatını planlaması, toplumsal kalıplardan uzak bir şekilde kendi

[247] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 152.

tercihlerine göre bir hayat yaşayabilmesi ve kendi kişiliğini kendisinin geliştirmesi için bireylere kişisel verilerin korunması hakkı tanınması bir zorunluluktur. Çünkü kişisel verilerin korunması hakkının temelinde bireyin kişisel özerkliğini ve mahremiyetini koruma amacı bulunmaktadır.

Nesnelerin interneti kavramını akıllı şehirlerde kullanılan araçlardan olduğunu çalışmamızın daha önceki bölümlerinde belirtmiştik. Akıllı ev uygulamaları, evin sıcaklık, nem, hava kirliliği, ses düzeyi gibi değerleri ölçüp, ev sakinlerini ihtiyaçlarını belirleyebilen ev aletleri aracılığı ile çalışmaktadır. Evde bulunan cihazlar, ev sakinlerinin ne zaman eve gelip ne zaman evden çıktıklarını, hangi odada daha fazla vakit geçirdiklerini, evde vakit geçirmek için neler yaptıklarını, kaç saat uyuduklarını, evde kaç kişinin olduğunu belirleyebilir. Ses komutuyla çalışan akıllı ev aletlerinin sesleri alan bir sensörü olması sahip olduğu yetenek açısından bir zorunluluktur. Sesleri toplayan bu akıllı cihazların ev ortamında konuşulanları dinleme, elde ettiği verileri başka platforma aktarma yeteneklerine sahip olmadığı yönünde bir garanti bulunmamaktadır. Bu durumda kişinin özel hayat alanı ve sır alanı kapsamında kalan verilerin güvenliği tehdit altında olacak ve kişinin özel hayatın gizliliğinin ihlal edilip edilmediği gündeme gelecektir. Aynı şekilde ev ortamını dinleyen ses alma sensörüne sahip cihazlar, elde ettikleri sesleri depolayıp başka yerlere aktardığı durumda haberleşmenin gizliliği de ihlal edilmiş olacaktır. Bu ses verilerinde, kişinin sadece aynı evi paylaştığı kişilere ifade ettiği düşüncelerin bulunması durumunda ifade özgürlüğünün ihlali gündeme gelecektir.

Aynı endişe akıllı güvenlik uygulamaları için de geçerlidir. Hayat alanına yerleştirilen ses sensörleri vasıtasıyla "*İmdat*!" çığlıklarını duyup bir an önce olay yerine gitmek isteyen kolluk kuvvetlerinin, bu teknolojiyi kullanarak konuşulan tüm sesleri kaydedip, kişilerin fikirlerini öğrenmeye çalıştıkları durumda ifade özgürlüğü ve haberleşme özgürlüğünün ihlali gündeme gelecektir. Kent güvenliğini sağlamak amacıyla sokakta bulunan kameraların evin içini gözetlemesi durumunda özel hayatın gizliliğinin ihlali ortaya çıkacaktır.

Akıllı sağlık uygulamaları, giyilebilir teknoloji araçlarıyla insanın kalp ritmi, nabız, nefes, sıcaklık, kas hareketleri ve uyku düzeni gibi kişisel verilerine ulaşabilmektedir. Hatta bu araçların sayısı ve yetenekleri arttıkça vücutta meydana

gelen değişimlerden yola çıkarak insanın duygularını öğrenmek ve düşüncelerini tahmin etmek mümkün olacaktır[248]. Bu durumda kişinin düşünceyi açıklama ve yayma özgürlüğünün ihlal edilip edilmediği hususu gündeme gelecektir.

Kişisel verilerin hukuka aykırı bir şekilde elde edilmesinin insan onuru ve kişisel özerkliğine verdiği zarar ile ortaya çıkabilecek insan hakları ihlallerini inceledikten sonra, bir bu kadar daha önemli bir konu vardır ki göz ardı edilemez. Kişisel veriler hukuka uygun olarak elde edildikten sonra bu verilerin geleceğini öngörmek mümkün değildir. Kişisel veriler günümüzde ekonomik bir değere sahip olup gelir elde etmek amacıyla veri sahiplerinden habersiz olarak satılma riski bulunmaktadır.

Her şeyin dijitalleştiği bir zamanda gözetim, sadece görsel olarak izleme faaliyeti olarak tanımlanamaz. İnsanın gün içerisinde yaptığı rutin davranışları takip etmek, tercihlerini öğrenmek, fikir yapısını anlamaya çalışmak gibi faaliyetler de gözetim faaliyetidir. Akıllı cihazlar kullanılmadıkları durumlarda bile veri toplamaya devam etmekte, toplanan verilerle analizler yapmakta ve kişilerin hayat tarzı hakkında çıkarımlar yapmaktadır. Akıllı ev otomasyon şirketi Nest'i satın alan Google, 2018 yılında daha düşünceli bir ev yaratmak amacıyla Nest'in donanımı ile Google'ın yazılımını birleştirme kararı almıştır. Sosyal ağ projesi olan Facebook insansız hava araçları ve artırılmış gerçeklik teknolojisine yatırım yapmaktadır. Zuboff'a göre teknoloji firmalarının farklı alanda yaptıkları yatırımların sebebi, daha çok veri elde edip ellerindeki veri havuzunu büyütmek ve böylece insanların geleceği hakkında çıkarım yapma avantajını elde etmektir[249].

2027 yılında konum verilerinin dünya çapındaki pazarının 32 milyar dolar olması beklenmektedir. Güvenlik gerekçesiyle aile bireylerinin birbirlerinin konumlarını izleme imkânı veren bir uygulama olan "*Life360*" isimli uygulama, konum verilerinin satışından 2020 yılında 16 milyon dolar gelir elde etmiştir[250]. Bir başka örnek de Ford'un CEO'su Jim Hackett'in açıklamalarıdır. Hackett, 100 milyon Ford sürücüsünden toplayacakları verileri gelir kaynağı olarak değerlendireceklerini

[248] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 82.
[249] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 80 vd.
[250] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 151.

belirtmiştir[251]. Örnekler de göstermektedir ki kişisel veriler günümüzde maddi değeri olan bir kavramdır. Bu ekonomik değerin korunması muhakkak gereklidir.

Kişilerin onur ve mahremiyetini tehdit eden tüm bu risklerden dolayı kişisel verilerin hiç toplanmaması gibi bir çözüm yoluna gidilemez. Günümüzde bilgi ve iletişim teknolojilerinin sağlamış olduğu avantajlardan uzak duramayız. Akıllı şehirlerde sensörler veya diğer teknolojik araçlar aracılığıyla insanlardan, binalardan, çevreden veya altyapıdan veri toplamanın temel amacı yaşam kalitesini yükseltmektir. Bu amaç doğrultusunda hareket ederek, akıllı şehir sakinlerinin talep ettiği kamu hizmetlerinin kalitesini artırmak isteyen yönetim ile kişisel özerkliğini, onurunu kaybetmek istemeyen ve mahremiyetini korumak isteyen ilgili kişi arasında bir denge noktası bulunmalıdır. Bu denge noktası akıllı şehirlerde kişisel verilerin korunması hukuku ile sağlanacaktır.

V. AKILLI ŞEHİRLERDE VERİ İŞLEME FAALİYETİ

A. Veri İşlemenin Tanımı ve İlkeleri

1. Tanım

6698 sayılı KVKK'nın "*Tanımlar*" başlıklı 3. maddesinde "*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*" olarak tanımlanmıştır. Kanun gerekçesinde "*Kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır. Buna göre kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir*." denilmektedir.

[251] Uluk, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", s. 83.

Kanun koyucu madde metninde kişisel verilerin işlenmesini tanımlarken, veriler üzerinde yapılan işlemleri sayarak metni düzenlemeye başlamış olsa da metnin sonunu *"...gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde tanımı bitirerek, veri işleme faaliyetini sınırlı sayıda eylemlerle kısıtlamamış, kavramı geniş bir biçimde ele alarak yoruma müsait bir kavram ortaya koymuştur. Kavram o kadar geniş tutulmuştur ki veri ile ilgili olup da veri işleme olarak değerlendirilmeyecek bir eylem akla gelmemektedir.

Kanun koyucu veri işleme faaliyetini "*otomatik olan*" ve "*otomatik olmayan*" şeklinde ikiye ayırmıştır. Otomatik olan her türlü işlem kanun kapsamında veri işleme olarak nitelendirilecektir. Ancak otomatik olmayan yöntemlerle işlenen veriler, verinin bir veri kayıt sisteminin parçası olması şartıyla veri işleme olarak nitelendirilebilecektir. Veri kayıt sistemi ise kanunun aynı maddesinde "*Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini*" olarak tanımlanmıştır. Kanun gerekçesinde de "*Bu sistemler elektronik yahut fiziki ortamda oluşturulabilir. Buna göre, veri kayıt sisteminde kişisel veriler, ad, soyad veya kimlik numarası üzerinden sınıflandırılabileceği gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilecektir."* şeklinde açıklama getirilmiştir. Bu durumda belirli kriterlere göre yapılandırılmamış otomatik olmayan yollarla yapılan eylemler veri işleme olarak nitelendirilmeyecektir. GDPR'da yapılan veri işleme tanımı da KVKK ile benzerlik göstermektedir. Eylemler sınırlı sayıda olmayacak şekilde geniş ve yoruma açık düzenlenmiştir.

Akıllı şehirlerde sensör ve diğer teknolojik cihazlarla yapılan veri toplama, verilerin nesneler arası aktarımı, depolanması, analiz edilmesi ve sonuç alınması sürecinde yapılan her türlü işlemin hukuki niteliği "*kişisel verilerin işlenmesi*"dir. Akıllı şehirlerde veri işleme faaliyetinin neredeyse tamamı akıllı cihazlarla gerçekleştirdiği için "*otomatik veri işleme*" olarak nitelendirilecektir. Bu durum veri işlemede teknolojik cihazların kullanılmasından kaynaklanmakta olup tüm veri işleme faaliyetlerinin otomatik olması zorunluluğu doğurmamaktadır. Akıllı şehirlerde ihtiyaç duyulması halinde otomatik olmayan yollarla da yapılabilir ve bu verinin, bir veri kayıt sisteminin bir parçası olacağı muhakkaktır.

2. Kişisel Veri İşlemenin Genel İlkeleri

KVKK'nın 4. maddesinde veri işleme ilkeleri sayılmıştır. Kanun metnine göre veri işleme ilkeleri; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmektir.

Kanunda yapılan bu düzenleme uluslararası düzenlemelere de uygundur. Ortaya konulan ilkeler 95/46 EC sayılı Direktif, 108 sayılı Sözleşme ve GDPR ile paralellik göstermektedir. GDPR'da belirtilen sorumluluk ilkesinin bu kanun maddesinde düzenlenmemiş olması bir eksiklik değildir çünkü kanunun 11. maddesinde düzenlenmiştir[252]. Kişisel verilerin korunması hakkının anahtarı niteliğinde olan bu ilkeler, tüm veri işleme faaliyetleri için geçerli olmalıdır. Eşit öneme sahip olan bu ilkeler birbirleriyle bağlantılı ve iç içe geçmiş ilkelerdir[253].

a. Hukuka ve Dürüstlük Kurallarına Uygun İşleme

Kişisel verileri koruma hukukunda asıl olan verilerin işlenme yasağıdır. Kişisel veriler ancak hukukun izin verdiği durumlarda işlenebilir[254]. Hukuka uygunluk, veri işlemenin hem usul açısından hem esas açısından mevzuata, içtihada ve hukukun evrensel ilkelerine uygun olması anlamına gelmektedir[255]. Dürüstlük ilkesi, Türk Medeni Kanunu'nun 2. maddesinde belirtilen dürüstlük kuralı ve kişinin hakkını kötüye kullanması yasağının, veri koruma hukuku alanına yansımasıdır[256]. Dürüstlük ilkesi, veri sorumlusu ve veri işleyenin ahlaka uygun davranmasını emretmektedir[257].

GDPR'da düzenlenmiş ancak KVKKda açıkça düzenlememiş olan "*şeffaflık ilkesi*", veri işleme faaliyetinin ulaşılabilir, izlenebilir, anlaşılabilir olması, veri sahibinin haklarını bilmesi, kişisel verinin işlenmesinden dolayı ortaya çıkabilecek

---

[252] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 330.
[253] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması", 76.*
[254] *Yüksel Tolun, "Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması*", (Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale 2020), s. 41.
[255] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", s. 59.
[256] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", 333.
[257] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", s. 59.

riskleri öngörmesi, veri sorumlusu ve veri işleyenin veri sahibine karşı açık ve net olması anlamına gelmektedir[258]. Şeffaflık ilkesi her ne kadar açıkça kanunda düzenlenmemiş olsa da dürüstlük ilkesi kapsamında değerlendirilebilir.

Veri sahibinin haberi olmaksızın veri toplanması, verilerin veri sahibinin aleyhine kullanılması, veri sahibinin kişisel veri işlenmesine onay vermememi olması ve neye onay verdiğini bilmemesi hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılıklara örnek olarak verilebilir[259].

b. Doğru ve Gerektiğinde Güncel Olma

İşlenen kişisel verilerin doğru olması hem veri işleyen açısından hem veri sahibi açısından faydalı bir durumdur. İşlenen kişisel verilerin yanlış olması durumunda; veri sahibi, maddi ve manevi zarar uğrayabilir, veri işleyen de veri işlemedeki amacına doğru bir şekilde ulaşamaz. Verilerin doğru olması her iki tarafın da menfaatinedir[260].

Bu ilke, ilgiye kişinin "*kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme"* hakkını doğurmaktadır. Çünkü verinin doğru olup olmadığını en iyi bilebilecek kişi verinin sahibi olan kişidir. Aynı zamanda veri sorumlusuna da bir yükümlülük yüklemektedir. Veri sahibinin verilerinin doğruluğunu kontrol etmek ve gerektiğinde güncelleme yapmasını sağlamak için, veriye ulaşıp üzerinde değişiklik yapabilmesi gerekmektedir. Veri sorumlusuna düşen yükümlülük, veri sahibinin verilere ulaşabileceği bir kanal oluşturma yükümlülüğüdür[261]. Veri sahibinin verilerin doğru olması için bir çaba içerisinde olması gerekmektedir. Öncelikle verilerin doğruluğunu teyit etme, sonrasında da değişen bilgilerini güncelleme çabası göstermelidir. Kanun koyucu verilerin güncel olmasını her zaman değil gerektiğinde istemektedir. O halde ne zaman gerekip gerekmediği somut olayın yorumlanması ile anlaşılacaktır.

---

[258] Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", s. 41 vd.
[259] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 333.
[260] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", s. 78.
[261] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 334.

Doğru ve gerektiğinde güncel olma ilkesi, hem GDPR'da hem 95/46 EC sayılı Direktif'te düzenlenen bir ilkedir[262].

c. Belirli, Açık ve Meşru Amaçlar İçin İşleme

KVKK gerekçesinde *"Amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir."* demektedir. Örneğin, bir otopark işletmesinin, otoparka gelen araçlarla ilgili araç plakası ve otoparka giriş-çıkış saatlerini işlemesi meşru görülürken, aracın modeli, ruhsat numarası gibi bilgileri işlemesi meşru görülmemektedir.

Bu ilke veri sorumlusuna, ilgili kişiyi verinin toplanma amacını hakkında bilgi verme yani aydınlatma yükümlülüğü getirmektedir[263]. Veri işleme amacı en geç veriler toplanırken belli olmalıdır. "*Belki ilerde lazım olur*" düşüncesiyle hareket edilmemelidir[264]. Belirlenen amaç birden fazla olabilir ancak bu amaçların somut bir şekilde belirtilmesi gerekmektedir. Belirlenen amaçların, hizmet kalitesini artırma, güvenlik, reklam ve pazarlama gibi torba ifadeler değil daha detaylı ifadeler olması gerekmektedir[265].

d. İşlendikleri Amaç ile Sınırlı ve Ölçülü Olma

Kanun gerekçesinde bu ilke "*işlenen verilerin, belirlenen amaçların gerçekleştirilebilmesine elverişli olmasını, amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir*" şeklinde açıklanmıştır. Bu ilke işlenecek veri miktarını amaç ile sınırlamıştır. İlke gereğince mümkün oldukça az veri işlenmeli hatta hedeflenen amaca veri işlenmeden ulaşılabiliyorsa veri işlenmemelidir. Veri işlemek zorunlu ise işlenmelidir. Bu ilke "*veri ekonomisi*" veya "*veri minimizasyonu*" olarak da adlandırılmaktadır[266].

---

[262] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması", 79.*
[263] *Tolun, "Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması*", s. 43.
[264] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", s. 80.
[265] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 335.
[266] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", s. 81.

Kişisel verilerin işlenmesi gerekli ancak açıkça yani herkes tarafından görünebilir şekilde işlenmesi zorunluluk değil ise bu ilke gereğince, kişisel veriler işlenirken maskeleme veya anonimleştirme gibi metotlar kullanılması gerekmektedir[267].

Ölçülülük ilkesi, veri işleme faaliyeti ile faaliyetin amacı arasında makul bir denge bulunması gerektiğini ifade etmektedir. Verileri işlenen ilgili kişilerin açık rızalarının olması ölçülülük ilkesinin uygulanmamasına mazeret olamaz. Kişilerin rızası olsa bile gereğinden fazla veri işleme faaliyeti ölçülülük ilkesine aykırı olması gerekçesiyle hukuka aykırı olacaktır[268].

Örneğin, akıllı şehirlerde toplu taşıma kullanan kişiler otobüs, metro, vapur gibi toplu ulaşım araçlarını kullanırken adı, soyadı, kimlik numarası ve fotoğraf bilgilerinin bulunduğu bir kişiselleştirilmiş kart kullanabilirler. Bunun yerine kişilerden araçlara parmak izi okutarak binilmesi istenirse ölçülülük ilkesine aykırılık teşkil edecektir. Çünkü hedeflenen amaca mümkün olduğunca az veri ile ulaşılmaya çalışılmalıdır. Kişinin parmak izi biyometrik veri olup kişinin adı ve soyadına göre daha çok korunması gereken nitelikte bir kişisel veridir.

Toplanan kişisel veriler ancak toplama amacı doğrultusunda kullanılabilir. Ancak değişen şartlardan dolayı daha önce düşünülemeyen ancak sonradan ihtiyaç duyulan bir amaç ortaya çıkarsa, kanun gerekçesinde belirtildiği üzere "*işlemeye ilk kez başlıyor gibi, 5 inci maddede düzenlenmiş olan kişisel verilerin işlenme şartlarından birinin gerçekleşmesi gerekecektir*."

e. İşlendikleri Amaç ile Sınırlı Süre ile Muhafaza Edilme

Bu ilke "*veri minimizasyonu ilkesi*"nin zamansal versiyonudur[269]. Kanun gerekçesine göre "*veri sorumluları, ilgili mevzuatta verilerin saklanması için öngörülen bir süre varsa bu süreye uyacak; yoksa verileri, ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebilecektir. Bir verinin daha fazla saklanması için geçerli bir sebep olmaması durumunda, o veri silinecek veya anonim hale getirilecektir*". Anonim hale getirme kanun lafzıyla *"kişisel verilerin, başka*

[267] Kişisel Verileri Koruma Kurulu'nun 02/12/2021 tarihli ve 2021/1214 sayılı Kararı
[268] Kişisel Verileri Koruma Kurulu'nun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar
[269] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", s. 82.

verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini" ifade etmektedir.

Verilerin saklanacağı sürenin tespitinde öncelikle KVKK veya diğer kanunlara bakılmalıdır. Kanunda düzenleme bulunmaması durumunda Kişisel Verileri Koruma Kurulu'nun kararları incelenmelidir. Bu konuda karar olmaması durumunda ise veri sorumlusu süreyi kendisi karar verecektir. [270] Bu sürenin tespitinde dikkate alınacak hususlar Veri Sorumluları Sicili Hakkında Yönetmelik m.9'da sayılmıştır. Yönetmeliğe göre bu süre; verini işlenme amacı, aynı sektörde teamül olarak kabul edilmiş süre, veri sorumlusu ile veri sahibi arasındaki hukuki ilişkinin süresi, veri sorumlusunun elde edeceği menfaat için gerekli olan süre, ortaya çıkan risk, maliyet ve sorumlulukların hukuken devam edeceği süre, verinin güncel tutulabilme ihtimali, veri sorumlusunun saklamak zorunda kaldığı süre, kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi göz önünde bulundurularak tespit edilir.

VI. AKILLI ŞEHİRLERDE HUKUKA AYKIRI VERİ İŞLEME SEBEBİYLE SORUMLULUK

A. Akıllı Şehirlerde Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu KVKK'da "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*" olarak tanımlanmıştır. Belirtilen tüzel kişi hem kamu hem de özel hukuk tüzel kişisi olabilir. Kamu kurumları, şirketler, dernekler veya vakıflar gibi tüzel kişiler veri sorumlusu olabilecektir. Burada dikkat edilmesi gereken husus, tüzel kişinin veri sorumlusu olduğu durumda, sorumluluk tüzel kişilerin çalışanlarında veya belirlenen herhangi bir biriminde değil, tüzel kişiliğin bizatihi kendisindedir[271].

[270] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 337.
[271] Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", s. 55.

29'uncu Madde Çalışma Grubu'nun 1/2010 sayılı tavsiye kararı, Avrupa Veri Koruma Denetmeni tarafından 7 Kasım 2019 tarihli "*2018/1725 Numaralı Tüzük Kapsamında Veri Sorumlusu, Veri İşleyen ve Müşterek Veri Sorumlusu Kılavuzu*" ve Avrupa Birliği'ndeki düzenlemeler birlikte değerlendirildiğinde;

- Kişisel verilerin toplanmasına, toplama yöntemine, toplanacak kişisel veri türlerine, kimden ve hangi verilerin toplanacağına, toplanan verilerin hangi amaçlarla kullanılacağına,
- Kişisel verinin işlenmesine, kimin işleyeceğine, ne şekilde işleneceğine, verilerin saklama süresine, veri saklama politikasına, verilere kimlerin erişme yetkisi olacağına, alıcıların kim olacağına,
- Toplanan verilerin paylaşılıp paylaşılmayacağına, paylaşılacaksa kiminle paylaşılacağına,

herhangi bir emir ve talimat almadan özerk bir şekilde karar veren ve ilgili kişilerle doğrudan muhatap olan kişinin veri sorumlusu olduğu söylenebilecektir[272].

Veri işleyen ise KVKK'da *"Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* olarak tanımlanmıştır.

Veri işleyen; kişisel veri işlemek için başkasından talimat alan, aldığı talimatlar doğrultusunda görevini yerine getirmekle yükümlü olan kişidir. Kişisel verilerin toplanması ve saklanması sürecinde karar verme yetkisine sahip değildir. Verilerin ne şekilde ifşa olabileceğine, kimlerin bu verilere erişebileceğine, kişisel verilerin ne amaçla kullanılacağına karar veremez. Veri işlemenin sonuçlarından sorumlu değildir. Veri işleyenin verileri hukuka uygun olarak işlemesi veri sorumlusunun vermiş olduğu emir ve talimatlara uyduğu ölçüde gerçekleşecektir. Diğer bir deyişle veri işleyen, veri sorumlusunun çıkarlarını gözeterek, veri sorumlusunun verdiği yetki doğrultusunda, veri sorumlusunun belirlemiş olduğu temel amaç ve araçlarla, veri işlemenin daha çok teknik kısımları ile ilgili olarak veri işleme faaliyetini gerçekleştirmektedir[273].

Veri sorumlusu yetki verdiği takdirde, veri işleyen veri işleme faaliyetleri esnasında önemli ölçüde bir özerkliğe sahip olabilir. Veri sorumlusu ile veri işleyen arasında yapılacak kişisel veri işleme sözleşmesi ile; kişisel verilerin toplanması için

[272] Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Kararı
[273] Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Kararı

kullanılacak bilgi teknolojileri sistemleri veya diğer metotlar, verilerin saklama, aktarma silinme, yok edilme ve anonim hale getirilme yöntemi, verilerin korunması için alınacak güvenlik önlemleri gibi bazı teknik konularda, veri sorumlusunun çıkarlarını gözetmek ve talimatlarına uymak şartıyla, veri işleyen de bazı konularda karar verme yetkisine sahip olabilir[274]. Veri sorumlusunun başka bir kişiyi yetkilendirmesi durumunda, veri sorumlusu ve veri işleyen hukuka uygunluk açısından müştereken sorumlu olacaklardır[275].

GDPR'da veri sorumlusu "*data controller*" olarak, veri işleyen "*data processor"* olarak isimlendirilmiştir. GDPR'da yapılan tanımlar KVKK ile benzerlik göstermektedir. Ayrıca GDPR'da KVKK'dan farklı olarak, "*ortak veri sorumlusu*" düzenlenmiştir. Ortak veri sorumlusu, tek bir veri kayıt sisteminde, veri işleme faaliyeti araç ve amaçlarının birden fazla kişi tarafından belirlenmesi durumudur. Veri ihlali söz konusu olduğunda ortakların hepsi sorumlu olacaktır. KVKK'da ortak veri sorumlusu düzenlenmemiştir[276]. Ancak Kişisel Verileri Koruma Kurumu'nun rehber niteliğinde hazırlamış olduğu "*Veri Sorumlusu ve Veri İşleyen*" başlıklı dokümanda verilen bir örnekte, birden fazla kişinin veri sorumlusu olabileceği gösterilmiştir. Bir ilaç firmasının, bir araştırma şirketine memnuniyet anketi yaptırması örneğinde, anket yapılacak kişilerin ve anket metodunun seçilmesi, anket sonuçlarının sunumu anket şirketine bırakılmıştır. Anket şirketinin, hangi verilerin toplanacağına karar vermesi nedeniyle, ilaç firması ile birlikte veri sorumlusu olacağı belirtilmiştir. Ayrıca şunu da belirtmek gerekir ki bir tüzel gerçek ve tüzel kişi hem veri sorumlusu hem veri işleyen olabilir[277].

Bu bilgiler ışığında akıllı şehirlerde veri sorumlusu ve veri işleyenin kim olacağı tartışılmalıdır. Öncelikle şu husus belirtilmelidir ki, ülkemizde akıllı şehir uygulamaları yaygınlaşmaya başlasa da tek başına akıllı şehir olarak nitelendirilebilecek bir kentimiz bulunmamaktadır. Akıllı şehir kavramı ülkemizde halen erişilmesi gereken bir hedef konumundadır. Bu nedenle erişilmesi hedeflenen akıllı şehirlerdeki idari yapılanmada, akıllı şehir uygulamalarının yürütülmesine dair

[274] Kişisel Verileri Koruma Kurulunun 30/01/2020 tarihli ve 2020/71 sayılı Kararı
[275] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", s. 98.
[276] Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", s. 60.
[277] Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, Link: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf (Çevrimiçi Tarihi: 03.06.2023)

yetkilendirilmiş bir kamu kurumu, kurum içerisinde bir birim veya kurumlar arası görev paylaşımı net bir şekilde ortaya konulmuş değildir. Örneğin, akıllı ulaşım ve akıllı güvenlik uygulamaları kapsamında şehirlerde bulunan kameraların kurulumuna, yerleştirileceği konuma, sahip olması gereken teknolojik donanıma, elde edilen görüntülerin depolanacağı veri kayıt sistemine ve görüntülerin kullanım amaçlarına karar verecek kamu kurumunun tespiti her zaman kolay değildir. Belediyeler, valilikler, bakanlıklar ve bunlara bağlı olan kurumlar arasından farklı kamu kurumları hizmet sunmak isteyebilir. Halbuki akıllı şehirlerde farklı uygulamalardan toplanan verilerin bir araya getirilerek veri bütünlüğünün sağlanması ve verilerin koordineli bir şekilde toplanıp yekpare olarak analiz edilmesi çok önemli bir husustur.

"*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*", Çevre, Şehircilik ve İklim Değişikliği Bakanlığı tarafından hazırlanmış ve yürütülmektedir. Bakanlık bünyesinde Coğrafi Bilgi Sistemleri Genel Müdürlüğü'ne bağlı olarak "*Akıllı Şehirler Dairesi Başkanlığı*" kurulmuştur[278]. İstanbul Büyükşehir Belediyesi'nde "*Akıllı Şehir Stratejik Planı*" Bilgi İşlem Dairesi Başkanlığı Akıllı Şehir Şube Müdürlüğü tarafından yönetilmektedir[279]. Akıllı Şehirler Dairesi Başkanlığı tarafından hazırlanan Akıllı Şehir Portalı'nda (https://www.akillisehirler.gov.tr/) Ulusal Coğrafi Veri Platformu, Ulusal Akıllı Şehir Açık Veri Platformu, Ulusal Kent Rehberi, Ulusal Kent Bilgi Sistemi, Ulusal Trafik Güvenliği Analiz Platformu, Yerel Veri Platformu ve diğer platformlarda Türkiye'de yapılan tüm akıllı şehir çalışmaları ile ilgili verilere ulaşmak mümkündür. Merkezi yönetim, akıllı şehir çalışmalarının ülke genelinde planlanması ve tüm kamu kurumlarının, yerel yönetimlerin, üniversitelerin, özel sektör ve sivil toplum kuruluşlarının ortak bir eylem planı çerçevesinde hareket ederek akıllı şehir çalışmalarına yön vermesini önemsemektedir.

Akıllı şehirlerde veri sorumlusunu belirlerken, akıllı şehir uygulamasında kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişinin kim olduğuna bakılmalıdır. Kamu kurumlarında genelde bu süreci yönetecek bir makam tespit edilir. Yetki makamda oturan kişinin şahsında değil kurumdadır. Bir başka

[278] https://www.akillisehirler.gov.tr/ (Çevrimiçi Tarihi: 03.06.2023)
[279] https://akillisehir.istanbul/tr/ (Çevrimiçi Tarihi: 03.06.2023)

ifadeyle veri sorumlusu devlet memurunu kendisi değil kamu tüzel kişisi olacaktır. Akıllı şehirlerde veri sorumlusunun her zaman tek bir kamu tüzel kişisi olacağı kesinlikle söylenemez. Bu tamamen idarenin yapılanma şekline, kamu kurumları arasındaki görev ve yetki paylaşımına göre değişmektedir. Bu nedenle ülkeler arası farklı uygulamalar veya aynı ülkede şehirler arası farklılıklar bile olabilir. Örneğin bir şehirde veri sorumlusu sadece belediye olurken başka bir şehirde belediye ile beraber valilik de veri sorumlusu olarak karşımıza çıkabilir. Aynı şehirde farklı akıllı şehir uygulamalarında farklı kamu tüzel kişileri veri sorumlusu olabileceği gibi, aynı akıllı şehir uygulamasında farklı kamu tüzel kişileri ortak veri sorumlusu olabilecektir. Bu ihtimallerin tek bir ortak noktası vardır ki, her halükârda "*idare*" veri sorumlusu olarak karşımıza çıkacaktır.

Kamu hizmetleri doğrudan idare tarafından görüldüğü gibi, özel kişiler tarafından da gördürülebilmektedir. Akıllı şehirlerde idarenin, akıllı şehir uygulamalarının yürütülmesini bir özel hukuk kişisine yaptırması ihtimalinde, verilerin işleme amaçlarını ve vasıtalarını belirleyen özel hukuk kişi de veri sorumlusu kabul edilecek, idare ve özel hukuk kişisi birlikte veri sorumlusu olacaktır. Akıllı şehir uygulamalarında, uygulamanın sağlıklı çalışması ve cihazın işlevini yerine getirmesi sebeplerle kişisel veri toplayan işletim sistemi ve cihaz üreticileri, işlenen verileri ve amaçlarını belirleyen uygulama mağazaları[280] ve verinin işlenme amacını belirleyen uygulama geliştiriciler de veri sorumlusu olacaktır[281].

Kamu hizmetlerinin yürütülmesi açısından akıllı şehirlerde bir özel hukuk kişisinin tek başına veri sorumlusu olması beklenmemektedir. Çünkü bir özel hukuk kişinin tek başına akıllı şehir konsepti oluşturup kamu hizmeti sunması düşünülemez. Bu ifadeden, akıllı şehirlerde hiçbir zaman bir özel hukuk kişisinin veri sorumlusu olamayacağı sonucuna varılmamalıdır. Bizim tespitimiz akıllı şehir uygulamaları açısındandır. Tabi ki akıllı şehirlerde özel hukuk kişileri de kendi hizmetleri açısında veri sorumlusu olabilecektir. Ancak bu dar bir alan ile sınırlı kalacağı için akıllı şehir uygulamaları kapsamında değerlendirilemez.

[280] Apple Store ve Google Play Store örnek verilebilir.
[281] Habibe Esra Er, "*Mobil Uygulamalarda Kişisel Verilerin Korunması*", (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2020), s. 61 vd.

Akıllı şehirlerde veri işleyen, idarenin kendisi olabileceği gibi bir özel hukuk kişisi de olabilir. İdare veri işleme faaliyetini, bir araya getirdiği uzman personeller ile kendi bünyesinde veri işleme birimi oluşturarak yapabilir. Bir idare başka bir idareye veri işleme faaliyetini yaptırabilir. Örneğin, veri sorumlusu olan İstanbul Büyükşehir Belediyesi veri işleme faaliyeti yapmak üzere kendi bünyesinde bir birim kurabilir. Bu durumda hem veri sorumlusu hem de veri işleyen İstanbul Büyükşehir Belediyesi olacaktır. Ayrıca veri işleme faaliyetini İstanbul Valiliği'ne bağlı olan bir kamu kurumuna da yaptırabilir. Bu durumda veri işleyen Valilik olacaktır. Üçüncü ihtimalde de veri işleme faaliyeti bir özel hukuk kişine yaptırılabilir. Bu durumda da veri işleyen özel hukuk kişisi olacaktır. Örneğin, akıllı şehirlerde toplanan kişisel veriler bir bulut bilişim sisteminde saklanmak istendiğinde, anlaşma yapılan bulut hizmeti sağlayıcısı veri işleyen statüsünde olacaktır[282].

Sonuç olarak, kamu hizmetlerinin sunulması açısından akıllı şehirlerde idare, kesinlikle veri sorumlusu olacaktır. İdare tek başına veri sorumlusu olabileceği gibi bir özel hukuk kişisiyle beraber de veri sorumlusu olabilir. Akıllı şehirlerde veri işleyen ise, idarenin kendisi olabileceği gibi özel hukuk kişisi de olabilir.

B. Akıllı Şehirlerde Veri Sorumlusunun Yükümlülükleri

Veri sorumlusu, KVKK ile kendisine getirilen sorumlulukları ve kişisel verilerin işlenmesi ilkelerine uymakla yükümlüdür. Aksi takdirde ortaya çıkacak zararların tazmininden ve Kişisel Verileri Koruma Kurumu tarafından kendisine verilecek kararları uygulamakla sorumlu olacaktır[283]. KVKK'da belirtilen veri sorumlusunun yükümlülükleri başlıca "*aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükler, ilgili kişiler tarafından yapılan başvuruların cevaplanması ve Kişisel Verileri Koruma Kurulu'*nun *kararlarının yerine getirilmesi yükümlülüğü, veri sorumluları siciline kaydolma yükümlülüğü*" olarak sayılabilir.

[282] Kişisel Verileri Koruma Kurumu, Veri Sorumlusu ve Veri İşleyen, Link: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf (Çevrimiçi Tarihi: 03.06.2023)
[283] Tolun, "*Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması*", s. 27.

GDPR'a göre veri sorumlusu, işleme faaliyetine dair yazılı bir kayıt tutma, ilgili kişiyi aydınlatma, işlem güvenliğini sağlama ve veri koruma görevlisi atama yükümlülüğü altındadır[284].

Veri sorumlusunun yükümlülükleri aşağıda açıklanmıştır.

1. Aydınlatma Yükümlülüğü

KVKK'nın 10. maddesinde *"Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;*

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,

d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür." denilmektedir.

Aydınlatma yükümlülüğü, veri sorumluları açısından bakıldığında bir yükümlülüktür. Bunun yanında, kişisel verisi işlenen gerçek kişiler için ise kişisel verilerle ilgili bilgilendirmeyi ifade etmekte olup kişilerin verileri üzerinde kontrol ve denetim sağlama ve verilerinin geleceğini belirleyebilme yetkisini sağlama hakkı tanımaktadır. Veri sorumluları ile veri sahipleri arasındaki güven ilişkisinin kurulması, şeffaflık ve hesap verebilirlik ilkeleri açısından önem arz eden bir yükümlülüktür[285].

Aydınlatma yükümlülüğünün yerine getirilmesi için ilgili kişinin talebi olmasına gerek yoktur. Kişinin rızası ve diğer veri işleme şartları yerine getirilmiş olsa da aydınlatma yükümlülüğü yerine getirilmelidir. Aydınlatma yükümlülüğünün yerine getirilmesi için, ilgili kişinin onay vermesine gerek yoktur. Yükümlülük tek taraflı bir beyanla yerine getirilebilir. Aydınlatma yükümlülüğünün yerine getirildiğine dair ispat yükü veri sorumlusundadır[286]. Kişisel verinin işleme amacının

---

[284] Yılmaz, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", s. 53 vd.
[285] Kişisel Verileri Koruma Kurumu, "Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi". Link:https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Çevrimiçi Tarihi: 03.06.2023)
[286] Kişisel Verileri Koruma Kurumu, "*Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*".

değişmesi veya aktarılması düşünülmeyen verilerin sonradan aktarıma konu olması durumunda ayrıca aydınlatma yükümlülüğü ortaya çıkmaktadır[287].

Veri Sorumluları Siciline kaydolmuş bir veri sorumlusunun, ilgili kişiyi aydınlatırken vereceği bilgiler, Sicil'e açıklanan bilgilerle uyumlu olmalıdır. Kanunun 10. Maddesi aydınlatma yükümlülüğünün kimin yapacağına dair veri sorumlusuna seçim hakkı tanımıştır. Aydınlatma yükümlülüğünü veri sorumlusu bizzat kendisi de yerine getirebileceği gibi veri sorumlusu tarafından yetkilendirilen veri işleyen de yerine getirebilir[288].

Aydınlatma yükümlülüğü veri sorumlusu ya da yetkilendirdiği kişi tarafından yüz yüze yapılan şifahi görüşmede sözlü, web sayfasında yer alan metin, duvara asılmış bir pano gibi yazılı, ses kaydı dinletilerek, çağrı merkezi yoluyla ses dosyası dinletilerek, açılan pencere ve mobil uygulamalar gibi elektronik ortamda farklı yöntemlerle yerine getirilebilir[289]. Kişisel verilerin elde edildiği an, aydınlatma yükümlülüğü kapsamında ilgili kişiye iletilecek hususların tamamı iletilemiyorsa katmanlı bilgilendirme yöntemi kullanılabilir[290].

10 Mart 2018 tarihli ve 30356 sayılı Resmi Gazete'de yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in 6. maddesi, kişisel verilerin veri sahibi dışında başka bir kişiden elde edilmesinde durumunda aydınlatma yükümlülüğünün nasıl yerine getirileceğini düzenlemiştir.

Buna göre; fiili imkânsızlık veya ilgili kişiye ulaşılamaması nedeniyle kişisel veriler doğrudan ilgili kişiden elde edilemiyorsa;

- Kişisel verinin elde edildiği tarihten itibaren makul bir süre içerisinde,
- Kişisel veri ilgili kişiyle iletişim amacıyla kullanılacak ise, ilk iletişim kurulduğu anda,
- Kişisel veri aktarılacak ise, en geç kişisel verilerin ilk aktarılacağı anda, ilgili kişiye aydınlatma yükümlülüğünün yerine getirilmesi gerekir.

[287] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", 99.
[288] Kişisel Verileri Koruma Kurulu'nun 30/01/2020 tarihli ve 2020/71 sayılı Kararı
[289] Kişisel Verileri Koruma Kurumu, "*Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*".
[290] Öztürk, Altınok Çalışkan, Seyhan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*", s. 101.

Bununla birlikte, Tebliğ'in 5. maddesine göre, ilgili kişinin açık rızası alınması gerekiyorsa, aydınlatma yükümlülüğü ile açık rıza alınması işlemleri ayrı ayrı yerine getirilmelidir.

2. Veri Güvenliğine İlişkin Yükümlülükler

KVKK'nın 12. maddesi gereğince, veri sorumlusu, hukuka aykırı şekilde kişisel verilerin işlenmesini ve verilere erişimi engellemek, kişisel verilerin korunmasını sağlamak için gerekli teknik ve idari önlemleri almakla sorumludur. Bu önlemler, uygun güvenlik düzeyinin sağlanması amacıyla alınmalıdır. Bu kapsamda akıllı şehirlerde veri sorumlusu olan idare, bireylerin temel hak ve özgürlüklerinin korunmasının temini için, alacağı bir takım idari ve teknik tedbirlerle, kişisel verilerin hukuka aykırı olarak işlenmesi ile kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilmeli, kişisel verilerin muhafazasını sağlamalıdır. Veri işleyenin veri sorumlusundan farklı bir kişi olması durumunda alınması gereken tedbirlerden müştereken sorumlu olacakları ilgili kanun maddesini 2. fıkrasında belirtilmiştir.

Akıllı şehirlerde veri sorumlusu olan idarenin, kamu hizmetlerini yerine getirirken alması gereken idari ve teknik tedbirleri ve veri güvenliğine ilişkin yükümlülüğünü daha iyi anlamak için, belediyelerin ödeme ve borç sorgulama hizmetleri hakkında Kişisel Verileri Koruma Kurulu'nun 21/04/2022 tarihli ve 2022/388 sayılı ilke kararı incelenebilir. Söz konusu kararda, *"Bu çerçevede belediyeler tarafından emlak vergisi ödeme/hızlı ödeme veya borç sorgulama vb sayfalar aracılığıyla çevrimiçi olarak sunmuş oldukları hizmetler kapsamında Kanunun 12 nci maddesinde yer alan yükümlülüklerin yerine getirilmesi ve herhangi bir veri ihlalinin önlenmesi amacıyla; çift faktörlü doğrulama için ilk doğrulamanın TC kimlik no, ad soyad, vergi no, sicil no gibi verilerle yapılırken ikincil düzeydeki doğrulamanın kişiye özel oluşturulmuş SMS ya da e-postaya iletilen şifre gibi bir sistemle gerçekleştirilmesi, ikincil düzeyde kişiye ait başkalarının da erişebileceği telefon no, doğum tarihi, anne baba adı, sicil no gibi bilgiler yerine sadece kişiye özel olarak belirlenecek ve sadece ilgili kişinin erişebileceği verilerin istendiği sistemler ya da üyelik sistemi ile söz konusu hizmetlerin sunulmasının uygun olacağı değerlendirilmektedir"* denilerek belediyelerin emlak vergisi ödeme/hızlı ödeme ve borç sorgulama hizmetlerinde üyelik ve şifre ya da çift faktörlü doğrulama kullanmak sureti ile KVKK'nın 12 nci maddesi kapsamında gerekli teknik ve idari

tedbirleri alması gerektiğine karar verilmiştir. Kararda söz konusu önlemleri almayan belediyeler hakkında iletilecek şikâyet/ihbarlar doğrultusunda ilgili belediye hakkında KVKK'nın Kabahatler başlıklı 18. maddesi hükümleri çerçevesinde işlem tesis edileceği hususu vurgulanmıştır.

Verileri Koruma Kurulunun 21/12/2017 tarihli ve 2017/62 Sayılı İlke Kararı ile *"Bankacılık ve sağlık sektörleri başta olmak üzere birden fazla çalışan ile birlikte bitişik düzende hizmet veren posta ve kargo hizmetleri, turizm acenteleri, zincir mağazaların müşteri hizmetleri bölümleri, çeşitli abonelik işlemlerinin yapıldığı kuruluşlar ile belediye, vergi ve nüfus ile ilgili işlemler gibi hizmetlerin verildiği kamu ve özel sektör kurum ve kuruluşlarının, KVKK'nın 12. maddesi uyarınca kişisel verilerin korunması ile ilgili olarak; banko/gişe/masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda birbirlerine yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymasını, görmesini, öğrenmesini veya ele geçirmesini engelleyecek nitelikte gerekli teknik ve idari tedbirleri almasına"* karar verilmiştir.

KVKK m. 12/3'te yapılan düzenlemeye göre, veri sorumlusu, kendi kurum veya kuruluşunda, yasaların uygulanmasını sağlama ve kişisel verilerin yasalara uygun bir şekilde işlenmesi için gerekli denetimleri yapma veya yaptırma yükümlülüğü altındadır.

KVKK m. 12/4'te, veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğü düzenlenmiştir. Bu hükme göre veri sorumluları ile veri işleyenler görevden ayrılsalar bile öğrendikleri kişisel verileri, hukuka aykırı olarak ifşa edemez veya kişisel menfaatleri için kullanamazlar.

KVKK m. 12/5'te, veri güvenliğinin ihlal edilmesi halinde, veri sorumlusunun işlenen verilerin hukuka aykırı olarak üçüncü şahıslarca elde edildiğini kısa sürede ilgilisine ve Kişisel Verileri Koruma Kurulu'na bildireceği düzenlenmiştir.

3. İlgili Kişiye Başvuru İmkânı Tanıma ve Başvurulara Cevap Verme Yükümlülüğü

KVKK'nın 13. maddesi ile, ilgili kişi tarafından kullanılmak üzere, veri sorumlusuna bir başvuru yolu düzenlenme yükümlülüğü getirilmiştir. İlgili kişilerin, KVKK ile alakalı taleplerini, öncelikle veri sorumlusuna iletmeleri zorunludur. Bu

zorunluluğun yerine getirilmesi için ilgili kişilere başvuru yapmaları için bir yol oluşturulmalıdır.

Başvuru ücretsiz olarak yapılabileceği gibi işlemin ayrıca bir maliyeti gerektirmesi halinde, Kişisel Verileri Koruma Kurulu tarafından belirlenen tarifeye göre alacağı ücret alınabilir. İlgili kişiden bir talep alan veri sorumlusu, en kısa sürede ve en geç otuz gün içinde talebi inceler; kabul veya gerekçesini açıklayarak reddeder. Ayrıca veri sorumlusu cevabını, başvuru yapan gerçek veya tüzel kişiye 7201 sayılı Tebligat Kanunu'nu dikkate alarak bildirir. Talep kabul edildiği takdirde veri sorumlusu talebin gereğini yerine getirir. Başvuru talebine konu hususta veri sorumlusu hatalıysa ve ilgili kişiden ücret alınmışsa, alınan ücretin ilgiliye iade edilmesi gerekmektedir.

İlgili kişiye başvuru imkânı tanıma ve başvurulara cevap verme yükümlülüğü, ilgili kişinin kendileri ile ilgili bilgilere erişme ve bu bilgileri kontrol etme hakkı nedeniyle veri sorumlusuna yüklenmiştir. Kişinin kendisi ile ilgili bilgilere erişme hakkı, KVKK'nın uygulanmayacağı istisnai hallerde bile kullandırılması gereken bir haktır. AİHM'in yaklaşımına göre bu hak ancak yasal bir dayanağının bulunması şartıyla, meşru amaçlar doğrultusunda ve demokratik toplum düzeninin gerektiği ölçüde sınırlanabilir. Örneğin, Mahkeme *Haralambie – Romanya* (B. No: 21737/03, K. T: 27.01.2010) Davası'nda komünist rejim tarafından tutulan istihbarat arşivinde bulunan bilgilere başvurucu kişinin erişmesinin engellenmesini Sözleşme'nin 8. maddesine aykırı bulmuştur[291].

4. Kurul Kararlarını Yerine Getirme Yükümlülüğü

KVKK m. 15/5'te yapılan düzenlemeye göre, Kişisel Verileri Koruma Kurulu'nun şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlalin varlığının anlaşılması hâlinde, tespit edilen hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar verilerek ilgililere tebliğ edilir. Veri sorumlusu tebliğ tarihinden itibaren en geç otuz gün içinde kararı yerine getirmelidir.

5. Sicile Kayıt Olma Yükümlülüğü

KVKK m. 16'da Kişisel Verileri Koruma Kurulu'nun gözetiminde Kişisel Verileri Koruma Kurumu Başkanlığı tarafından kamuya açık olarak veri

[291] Eren Solmaz, "A*vrupa İnsan Hakları Mahkemesi Kararları'nın 'Kişisel Verilerin Korunması'na Katkısı*", İdare Hukuku ve İlimleri Dergisi, 18/1, 2019, s. 70. https://doi.org/10.26650/ihid.644402.

sorumlularının kaydedileceği Veri Sorumluları Sicili tutulması gerektiği düzenlenmiştir. İstisna getirilenler hariç olmak üzer kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmalarını zorunlu kılınmıştır. Kişisel verilerin korunması hakkının daha etkin şekilde kullanılması için veri sorumlularının kimler olduğunun kamuya açıklanması amaçlanmıştır. Bu nedenle sicil kamuya açık tutulur.

Kişisel Verileri Koruma Kurulu, işlenen verinin özelliği, miktarı, veri işleme işleminin yasal dayanağa sahip olup olmaması ve üçüncü taraflara aktarılması gibi objektif kriterler doğrultusunda Sicile kayıt zorunluluğundan istisna tanıyabilir.

6. Verileri İmha Etme Yükümlülüğü

KVKK m. 7'e göre, işlenme sebebi ortadan kalkan veriler resen veya ilgili kişinin talebi üzerine silinecek, yok edilecek veya anonim hale getirilecektir.

Kişisel verilerin silinmesi, kişisel verilerin erişebilir ve kullanılabilir olma özelliklerinin tamamen imkânsız hale getirilme işlemidir. Verilerin yok edilmesi ise, bilgilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin ortadan kaldırılmasını ifade etmektedir.

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir şekilde kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek duruma getirilmesidir. Anonim hale getirme işleminde, ilgili kişinin kimliğinin tespit edilmesini engellemek amacıyla, bir veri kümesindeki tüm tanımlayıcıların çıkartılmakta ya da değiştirilmektedir. Bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiler yapılan işlem sonucunda belli bir kişiye işaret etmeyen veri haline gelmiş olur yani anonim hale getirilmiş veri sayılır[292].

Kişisel verilerin yok edilmemesi, AİHM'in davalarına da konu olmuştur. AİHM, bilgilerin ne kadar bir süre tutulacağının hukuk kuralları ile düzenlenerek devletin sahip olduğu takdir yetkisinin açıkça ortaya konulması gerektiğini ortaya koymuştur. Ayrıca, artık geçerliliği kalmamış, doğruluğunu kaybetmiş ve ilgili

[292] Kişisel Verileri Koruma Kurumu, "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi*".

kişinin hayatını olumsuz etkiler hale gelen verilerin silinmesi gerektiğini belirtmiştir[293].

C. İstisnai Haller

6698 sayılı KVKK'nın 2. maddesiyle kanunun kapsamı belirlenmiştir. Kişisel verileri işlenenler açısından sadece gerçek kişiler kapsam dahilinde olup, verileri işleyenler açısından ise hem gerçek ve hem tüzel kişiler kapsam dahilindedir. Veri işleyen kişiler açısından özel sektör ile kamu sektörü ayrımı yapılmamıştır. Yapılan düzenlemeler her iki sektörde de uygulanmaktadır. İşleme yöntemi açısından, kişisel verilerin otomatik olan yollarla işlenmesi durumunda ve bir dosyalama sistemi olarak nitelendirilmiş, belirli kriterlere göre yapılandırılmış herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi durumunda KVKK uygulama alanı bulacaktır. Otomatik olmayan yollarla işlenen kişisel veriler bir veri kayıt sisteminin parçası değilse kanun kapsamında değerlendirilmeyecektir. Ancak, veri kayıt sisteminin parçası olmayan veriler, kişisel veri niteliğini kaybetmez, KVKK hükümleri uygulanmasa da diğer kanunların da uygulanmayacağı anlaşılmamalıdır. Örneğin, kişisel verilerle ilgili hukuka aykırı eylemler 5237 sayılı Türk Ceza Kanunu'nda tanımlanan suç tiplerine uygun olduğunda, TCK uyarınca suç teşkil edecek ve cezalandırılacaktır.

Otomatik kayıt sistemleri, insan müdahalesi olmaksızın veya çok az olarak, teknolojik cihazlarla kayıt yapan kayıt sistemleridir.[294] Akıllı şehirlerde veri işleme faaliyetinin neredeyse tamamı akıllı cihazlarla gerçekleştirdiği için "*otomatik veri işleme*" olarak nitelendirilecektir. Akıllı şehirlerde işlenen her veri kişisel veri değildir. Örneğin, havanın sıcaklık, nem, kirlilik verileri kişisel veri değildir ancak akıllı şehir uygulamaları için önemli verilerdir. Bu tip veriler için kişisel verilerin korunması hukuku düzenlemelerinin uygulanmasına gerek yoktur. Zaten bu veriler, toplanan verilere nazaran cüzi oranda olacaktır. Otomatik veri işleme neticesinde toplanan verilerin çok büyük bir kısmı kişisel veridir. Ancak her kişisel veri işleme faaliyetinde KVKK hükümleri uygulanmamaktadır. Kanunun 28. maddesi tam ve kısmi istisna hallerini düzenleyerek kanunun kapsamını daraltmıştır.

---

[293] Solmaz, "*Avrupa İnsan Hakları Mahkemesi Kararları'nın 'Kişisel Verilerin Korunması'na Katkısı*", s. 76.

[294] Yüzbaşı Tobaz, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", s. 314.

“Madde 28- Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.”

Tam istisna halleri olarak sayılan bu hallerden; kanun maddesinin b, ç ve d fıkralarında belirtilen durumlar akıllı şehirlerde yerine getirilen kamu hizmetleri kapsamına giren hususlar olup çalışmamız açısından büyük önem arz etmektedir.

Kanun maddesinin devamında ise kısmi istisna halleri düzenlenmiştir.

(2) Bu Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16ncı maddeleri aşağıdaki hâllerde uygulanmaz:

a) Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.

b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.

c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması.

Örneğin suç işlenmesinin önlenmesi veya suç soruşturması kapsamında emniyet birimleri tarafından, Elektronik Denetleme Sistemi ve Mobil Elektronik Sistem Entegrasyonu gibi kent güvenliğinin sağlanması amacıyla kurulan güvenlik sistemlerinde kayıtlarının işlenmesi durumunda, ilgili kişilere aydınlatma yapılması bir zorunluluk değildir.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nin 9. maddesinde de devlet güvenliği, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadele edilmesi, ilgilinin veya üçüncü kişilerin hak ve özgürlüklerinin korunması ile verilerin istatistiki veya bilimsel amaçlarla kullanılması gibi durumlarda kişisel verilerin korunmasına sınırlamalar getirilebileceği öngörülmüştür.

İstisna halleri KVKK hükümlerinin uygulanmayacağı anlamına gelmektedir ancak bu istisna hallerinde toplanan verilerin kişisel veri niteliğinde olmadığı anlamına gelmemektedir. Bu nedenle istisna hallerinde işlenen kişisel veriler KVKK kapsamında korunmasa da Anayasa'nın 90. maddesi gereğince uluslararası sözleşmeler ve kişisel verilerin korunması hakkını düzenleyen 20. maddesi kapsamında korunmaya devam etmektedir. Bir başka ifade ile, istisna halleri kişisel verilerin işlenmesinde veri sorumlusu ve veri işleyenlere tam bir özgürlük sunmamaktadır.

D. İstisnai Durumlarda Uygulanacak Hukuki Rejim

Akıllı şehir kavramı günümüzde yeni gelişen ve tam olarak ulaşılamamış bir kavram olması nedeniyle Avrupa İnsan Hakları Mahkemesi'nin önüne, doğrudan akıllı şehir uygulamaları kapsamında işlenen verilerle ilgili bir dava konusu gelmemiştir. Ancak günümüz şehirlerinin akıllı şehir olma sürecinde yapılan faaliyetler kapsamında toplanan verilerle ilgili davalara AİHM içtihatlarında görmek

mümkündür. Bir başka ifadeyle, doğrudan akıllı şehir uygulamalarını konu alan bir içtihat olmasa da devletin kamu hizmetlerini yerine getirmek amacıyla ve kamusal alanda toplamış olduğu kişisel verilerin dava konusu olduğu içtihatlar ışığında konu ele alınacaktır.

Özel hayat kavramını bir kişinin ismi, fotoğrafı veya fiziksel ve ahlaki bütünlüğü gibi kişisel kimliğe ilişkin konulara kadar genişleten AİHM, Sözleşme'nin 8. maddesi tarafından sağlanan teminatın esas olarak her bir bireyin kişiliğinin, dışarının müdahalesi olmaksızın, diğer insanlarla olan ilişkilerinde gelişmesine yönelik olduğunu belirtmektedir. Bu nedenle, kamusal bağlamda dahi bir insanın diğer insanlarla bir etkileşim alanını, özel hayatın kapsamı içerisinde olduğunu kabul eder.[295] Devlet görevlileri tarafından yapılan izleme ve özel verilerin toplanması faaliyetleri, bu faaliyetler kapsamında sistematik olarak toplanan bilgilerin kamu görevlilerince tutulan bir dosyada saklanması konuları Sözleşme Madde 8 bakımından "*özel hayat*" kapsamı içerisine girmektedir[296].

Bu ilkeyi uygularken Mahkeme, bir insanın özel hayatının, o insanın konutu ya da özel mülkü dışında yani kamusal alanda gündeme gelen tedbirlerden etkilenip etkilenmediğinin incelenmesiyle ilgili birtakım unsurlar olduğunu açıklamıştır. İnsanların bilerek ya da isteyerek kendilerini kamusal alanda, kişisel verilerin kaydedildiği ya da rapor edildiği faaliyetlere dahil edebilecekleri durumlar bulunduğundan, bir kişinin özel hayata yönelik makul beklentileri tek başına belirleyici olmasa da önemli bir faktör arz edebilir.[297] Örneğin, sokakta yürüyen bir kişi, kaçınılmaz olarak, sokakta hazır bulunan herhangi bir toplumun üyesine görünebilir olacaktır. Kamusal alanın teknolojik araçlarla izlenmesi (örneğin, güvenlik görevlisinin kapalı-devre televizyon ile izlemesi) de bu duruma benzer niteliktedir. Ancak, kamusal alandan böylesi bir materyalin herhangi bir sistematik ya da kalıcı kaydı söz konusu olduğunda özel hayat gereklilikleri gündeme gelebilir. Bu nedenledir ki güvenlik hizmetlerince belli bir kişiye ilişkin olarak toplanan

[295] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 21; Von Hannover – Almanya (No. 2), B. No: 40660/08 ve 60641/08, 07/02//2012, § 95.
[296] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 35.; Rotaru – Romanya, B. No: 28341/95, 04/05/2000, § 44
[297] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 35.; Benedik - Slovenya, B. No: 62357/14, 24/04/2018, § 101.

dosyalar ve bilgiler, müdahaleci veya gizli bir yöntemle elde edilmese de Madde 8 kapsamına girmektedir[298].

AİHM'in yaklaşımı aslında tam olarak akıllı şehir uygulamaları konusuna ışık tutmaktadır. Akıllı şehir uygulamaları kapsamında verilerin toplanması genel olarak kamusal alanda ve gizlenmeksizin yapılmaktadır. Kişi kendi isteğiyle yani verilerinin toplanacağını bile bile kamusal alana çıkmaktadır. Kamusal alanda toplanan veriler büyük veri havuzuna aktarılarak analiz yapılmaktadır. Bu durumda, AİHM içtihatlarına göre, akıllı şehirlerde veriler kamusal alanda toplanmış ve kişinin rıza olmuş olsa bile, veriler sistematik olarak toplandığı ve kaydedildiği için Madde 8 kapsamına girecektir. AİHM'nin tavrına bütüncül olarak baktığımızda akıllı şehir uygulamaları kapsamında toplanan kişisel veriler konusunda Madde 8'in uygulanacağı görülmektedir.

AİHS m. 8 ve Anayasa'ya göre hakka getirilen sınırlamalar kanunla öngörülmüş olmalıdır. Ancak Anayasa ile AİHS'de belirtilen kanunilik ilkeleri birebir aynı anlama gelmemektedir. AİHM, yargı kararları ile ortaya konulmuş ilkeleri de hukukilik prensibi kapsamında değerlendirirken, Anayasa sadece kanun ile hakkın sınırlanabileceğini belirtmektedir. Bu durumda idare tarafından yapılan düzenleyici işlemlerle kişisel verilerin korunması hakkına müdahale etmek Anayasa'ya aykırı olacaktır[299].

Temel hak ve özgürlükleri sınırlayan kanunlar sadece şekli açıdan değil maddi açıdan da kanunilik şartını sağlamalıdır. Yani düzenleme; keyfi müdahaleleri engelleyici, kişilere hukuku öğreten, hukuk güvenliği teminatı sağlayan, erişilebilir, öngörülebilir ve kesin olma niteliklerini haiz olmalıdır[300]. Hukuk, keyfiliğin önüne geçmek için, meşru amaç doğrultusunda hakka müdahale eden kamu makamlarının takdir yetkisini net bir şekilde ortaya koymalıdır. Hukuk, kamu makamlarına verdiği yetkinin kullanılma şartlarını ve ölçüsünü açık bir şekilde ortaya koymalı ki, hakkı sınırlanan kişiler müdahalenin sebebini ve sonucu bilebilmelidir[301]. Kamu makamlarına tanınan yetki hakkında yapılan düzenleme, kamu makamlarının takdir

[298] AİHM, P.G. ve J.H. – Birleşik Krallık, B. No: 44787/98, 25/09/2001, § 57.
[299] AYM, Ümit Karaduman, B. No: 2020/20874, 2/2/2022, § 55.
[300] AYM, Ümit Karaduman, B. No: 2020/20874, 2/2/2022, § 57.
[301] AYM, Ümit Karaduman, B. No: 2020/20874, 2/2/2022, § 59.

edebilme kabiliyeti kaldıracak düzeyde net olması gerekmez ancak asgari düzeyde bir kesinlik içermelidir[302].

Akıllı şehirlerde kamu makamlarının veya idare tarafından yetkilendirilmiş özel hukuk kişilerinin veri işleme faaliyetini düzenleyen kurallar; kişisel verilerin toplanması, saklanması ve kullanılması açısından süre, erişim, gizlilik, bütünlük, yok edilme ve analiz edilme gibi hususları içermeli, keyfiliğin ve yetki aşımının önüne geçecek, açık ve detaylı olmalıdır. Veriler açısından, kaydedilecek ve başka yerlere iletilecek bilgilerin hangi veriler olduğu belirlenmelidir. Veri işlemenin hangi şartlarda yapılacağı ve veri işleyen ve veri sorumlularının hangi usulle hareket edecekleri düzenlenmiş olmalıdır. Böylece akıllı şehir sakinleri, kişisel verilerinin kullanıldığı alan hakkında yeterli bilgiye sahip olmalıdır.

AYM kararlarına göre ölçülülük ilkesi; elverişlilik, gereklilik ve oranlılık unsurlarını içermelidir. Elverişlilik, müdahale teşkil eden eylemin, sınırlama amacını gerçekleştirmeye uygun olmasını ifade eder. Gereklilik, müdahale teşkil eden eylemin, sınırlama amacını gerçekleştirmek için bir zorunluluk olmasını ifade eder. Oranlılık ise, amaç ile araç arasında bir aşırılığın olmamasını ifade etmektedir. Ölçülülük ilkesinin amacı temel hak ve hürriyetlere getirilen sınırlamaların olması gerektiği seviyede kalmasını sağlamak yani aşırılığa kaçmasını engellemektir. Aksi takdirde, müdahaleler hakkın özüne dokunarak, hakkın kullanılmasını zorlaştırır, imkânsız kılar veya hakkı yok eder boyuta ulaşmaktadır. Müdahalenin ölçülü olup olmadığını tespit ederken, sınırlama amacı ile kişinin yapmış olduğu fedakârlık boyutu düşünülerek, toplum yararı ile kişinin temel hakkının korunması arasında adil bir denge noktası bulunmalıdır[303].

Akıllı şehirlerde kişilerin özel hayatına saygı hakkına müdahale ederek veri işleyen idare, veri işleme eyleminin "*demokratik bir toplumda gerekli*" ve "*ölçülülük ilkesine uygun*" olduğunu ortaya koymalıdır. Veri işleme faaliyeti, veri işlemedeki amaç ile orantılı bir biçimde yapılmalıdır. İdare, veri işleme faaliyetinin haklılığını tatmin edici bir boyutta inandırıcı bir biçimde ve konuyla ilgili olarak açıklamalıdır.

Aşağıda bazı akıllı şehir uygulamalarına benzer durumlar hakkında AİHM ve AYM'nin yaklaşımı ele alınacaktır.

---

[302] AYM, Ümit Karaduman, B. No: 2020/20874, 2/2/2022, § 60.
[303] AYM, Marcus Frank Cerny, E.2012/100, K.2013/84, 04/07/2013, §§ 72 ve 73.

1. Akıllı Güvenlik Uygulamaları Açısından Değerlendirme

Akıllı güvenlik uygulamaları, şehirlerdeki güvenliğine yönelik oluşabilecek tehditleri tespit etmek, bu tehditlere karşı önlemler almak ve kriz yönetimini sağlamak için kullanılan, güvenlikle ilgili verileri sürekli olarak toplayarak, analiz ederek ve raporlayarak şehir yöneticilerine ve güvenlik güçlerine anlık bilgi sağlayan, şehirdeki suç oranlarının izlenmesi, trafik kazalarının önlenmesi, doğal afetler veya terör saldırıları gibi olaylara hızlı ve etkili müdahale edilmesi gibi hedefler gerçekleştirilebilen uygulamalardır. Bu uygulamalar kapsamında şehrin görüntülenmesi, ses verilerinin toplanması, konum bilgilerinin elde edilmesi gibi metotlar uygulanır.

Yukarıda belirttiğimiz istisnai hallerden *"kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi"* ile *"kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi"* durumları, akıllı güvenlik uygulamaları ile doğrudan ilişkilidir.

AİHM, kişisel ya da kamusal nitelikli verilerin güvenlik güçlerince ya da Devlet makamlarınca toplandığı ve arşivlendiği hallerde Madde 8'in gündeme gelebileceğini kararlaştırmıştır[304]. AİHM'e göre kamu makamlarının veri işleme faaliyetleri özel hayata saygı hakkına müdahaledir. Müdahalenin oluşması için verinin kullanılmasına gerek yoktur, kişisel verinin elde edilmiş olması yeterlidir. Elde edilen verilerin kullanılıp kullanılmaması önemli değildir. Mahkeme, kamu makamları tarafından işlenen kişisel verilerin özel yaşam unsurlarından birini devreye sokup sokmadığını tespit etmek için bu işlenen verilerin hangi çerçevede alındığını ve muhafaza edildiğini, verilerin türünü, kullanıldığı ve işlendiği şekli, bunlardan çıkarılabilecek sonuçları dikkate alarak sonuca varmaktadır[305].

Örneğin Mahkeme, terörist olduğundan şüphelenilen bir kişinin GPS ile izlenmesinin ve bu yolla elde edilen verinin işlenerek kullanılmasının Madde 8'i ihlal

[304] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 41.; Rotaru - Romanya, B. No: 28341/95, 04/05/2000, §§ 43-44.
[305] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 41.; Büyük Daire - S. ve Marper/Birleşik Krallık, 30562/04, 04.12.2008, § 67.

etmediğine karar vermiş[306] iken, polisin bir insan hakları örgütüne üyeliği nedeniyle bir kişinin ismini "*gizli izleme güvenlik veri tabanı*"na kaydetmesini ve hareketlerini izlemesini Madde 8 ihlali olarak görmüştür[307]. Aynı şekilde, ceza kovuşturması kapsamında tutuklanan kişiler bakımından, kolluk faaliyetleri bağlamında bir videonun kaydedilmesinin ya da başvurucunun fotoğraflarının polis yetkililerince medyaya verilmesinin özel hayat hakkına bir müdahale teşkil ettiğine karar veren Mahkeme, terörist olduğundan şüphelenilen bir kişinin izni olmaksızın bir fotoğrafının çekilmesinin ve tutulmasının demokratik bir toplumda teröristlerin önlenmesi meşru amacıyla orantısız olmadığına karar vermiştir[308].

Mahkeme, görsel verinin kaydedildiği, arşivlendiği ve halka ifşa edildiği durumda kamusal yerlerin video ile izlenmesini Madde 8 kapsamında görmüştür. Örneğin, intihar teşebbüsü televizyon kameralarına yakalanan bir başvurucunun video kayıtlarının yayın amacıyla kullanımı için medyaya servis edilmesi, başvurucunun söz konusu zamanda kamusal bir yerde olmasından bağımsız olarak onun özel hayatına ciddi bir müdahale olarak görülmüştür[309]. AİHM'e göre, bir kişinin görüntüsü, kişinin özgün karakteristiklerini ortaya koyduğu ve kişiyi diğer kişilerden ayırdığı için, kişiliğin başlıca niteleyicilerinden biridir. Bundan ötürü bir kişinin görüntüsünün korunması hakkı kişisel gelişimin temel bileşenlerindendir. Fotoğrafların bir kişi ya da aile hakkında çok kişisel ve hatta mahrem bilgileri içerebileceğini düşünerek Mahkeme, hakların ve başkalarının itibarının korunmasının bu alanda ayrı bir önem arz ettiğini tespit etmiştir[310].

AİHM, millî güvenliğin korunması amacını gerçekleştirmede devletlerin geniş bir takdir yetkisinin olduğunu kabul etmektedir. Bu kapsamda, ilk olarak kişiler hakkında bilgi toplama ve halka açık olmayan siciller tutma, ikinci olarak millî güvenlik bakımından önemli pozisyonlarda çalışmak isteyen adayların bu işe

[306] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 47.; Uzun – Almanya, B. No: 35623/05, 02/09/2010, § 81.
[307] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 47.; Shimovolos – Rusya, B. No: 30194/09, 21/06/2011, § 66.
[308] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 37.; Murray – Birleşik Krallık, B. No: 14310/88, 28/10/1994, § 93.
[309] AİHM, Peck – Birleşik Kralık, B. No: 44647/98, 28/02/2003, § 87
[310] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 36.; Von Hannover – Almanya (No. 2), B. No: 40660/08 ve 60641/08, 07/02/2012, § 103.

uygunluğunu takdir ederken bu bilgiyi kullanma yetkisi veren kuralların olması gerektiğinde kuşku bulunmadığını belirtmektedir[311].

Bilginin elde edildiği ve arşivlendiği bağlamı ve bilginin niteliğini de dikkate alan AİHM, terörist olduğundan şüphelenilenlerle ilgili davalarda Devletlerin, özellikle geçmişte terörist faaliyetlerle ilişiği olan kişilerin bilgilerinin arşivlenmesinde geniş bir takdir yetkisine sahip olduğuna karar vermiştir. Mahkeme yetkili makamlarca tutuklanan kişiler veya hatta tutuklama anında ve yerinde hazır bulunan diğer kişiler ile ilgili temel kişisel detayların kaydedilmesinin ve tutulmasının terörizm suçlarının soruşturulması sürecinin meşru sınırları içerisinde kaldığına hükmetmiştir[312].

Devletin ulusal güvenliğini gizli izleme tedbirleriyle korumadaki menfaati, bir başvurucunun özel hayata saygı hakkına müdahalenin ciddiyeti karşısında dengelenirken, ulusal makamlar ulusal güvenliği koruma meşru amacına erişmenin araçlarını seçmekte belli bir takdir yetkisine sahiptir. Ancak, kötüye kullanıma karşı yeterli ve etkili güvenceler bulunmalıdır. Dolayısıyla Mahkeme, olası tedbirlerin mahiyeti, kapsamı ve süresi, bunlara izin vermeye, bunları yerine getirmeye ve denetlemeye yetkili makamlar ve ulusal hukukun tanıdığı başvuru yolunun türü gibi dava koşullarını dikkate alınmaktadır[313].

Telefon konuşmalarının dinlenmesi ya da başka şekillerde denetlenmesi özel hayata ve haberleşmeye ciddi bir müdahaledir ve bundan ötürü kesin bir yasaya dayanmalıdır. Özellikle de kullanılabilen teknoloji sürekli daha da karmaşık hale geldiğinden, konuya ilişkin açık, detaylı kuralların bulunması elzemdir[314]. Akıllı şehir uygulamalarında kullanılan ses toplama sensörleri veya uygulamalar kapsamında iletişim kurulan kişilerle yapılan görüşmeler, haberleşmeye müdahale olarak nitelendirilmektedir ve AİHM'in bu yaklaşımı dikkate alınmalıdır.

AİHM, ceza adaleti sisteminde modern bilimsel tekniklerin kullanılmasına ilişkin olarak Mahkeme, söz konusu tekniklerin geniş kapsamda kullanılmasının

[311] AİHM, Leander - İsveç, B. No: 9248/81, 26/03/1987, § 59; AYM, Ümit Eyüpoğlu, B. No: 2018/6161, 28/6/2022, § 35.
[312] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 37.; Murray – Birleşik Krallık, B. No: 14310/88, 28/10/1994, § 93.
[313] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 48.; Roman Zakharov - Rusya, B. No: 47143/06, 04/12/2015, § 232.
[314] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 48.; Kruslin - Fransa, B. No: 11801/85, 24/04/1990, § 33.

potansiyel faydaları ile özel hayat menfaatleri arasında dengenin dikkatlice sağlanması gerektiği, aksi takdirde Sözleşme Madde 8 tarafından sağlanan korumanın kabul edilemez ölçüde zayıflayacağına karar vermiştir[315]. Ceza kayıtlarının tasnif edilmeksizin ve sınırsız bir şekilde toplanması, güvenceleri net bir şekilde ortaya koyan, diğer hususların yanı sıra verinin toplanabileceği şartları, saklanma süresini, kullanılabileceği amaçları ve ortadan kaldırılabileceği durumları düzenleyen kuralların açık ve detaylı yasal düzenlemelerin yokluğunda Madde 8 gerekliliklerine aykırı olarak kabul edilecektir[316].

Ulusal kanun koyucu ve makamlar hangi izleme sisteminin gerekli olduğunu belirlemekte belli bir takdir yetkisine sahip olsa da bu hak sınırsız değildir[317]. AİHM Devletlerin, casusluk ve terörizmle mücadele kapsamında, uygun gördükleri her türlü tedbiri alamayacağını, aksine hangi izleme sistemi benimsenirse benimsensin kötüye kullanıma karşı yeterli ve etkili teminatların olması gerektiğini belirtmektedir[318].

Daha önce de ifade ettiğimiz gibi "*Hukuka uygun*" ifadesi sadece ulusal hukuka uyulmasını gerektirmez, aynı zamanda bu hukukun kalitesine de ilişkindir ve bunun hukukun üstünlüğüne uygun olmasını gerektirir. Kamu makamlarınca gerçekleştirilen gizli izleme bağlamında, ulusal hukukun, bir bireyin Madde 8 altındaki hakkına keyfi müdahaleye karşı koruma sağlaması gerekir. Dahası hukuk, lafzı bakımından bireylere kamu makamlarının böyle gizli tedbirlere hangi hallerde ve koşullarda başvurabileceği ile ilgili yeterli bir emare sağlayacak ölçüde açık olmalıdır[319]. Vatandaşların gizli izlenmesine ilişkin yetkiler ancak demokratik kurumları korumak için gerekli olduğu ölçüde hoş görülmektedir[320]. Böyle bir müdahale, ilgili ve yeterli gerekçelerle desteklenmeli ve güdülen meşru amaç ya da amaçlarla orantılı olmalıdır[321]. Ulusal makamlara tanınan kişisel bilgileri toplama ve

---

[315] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 48.; Büyük Daire- S. ve Marper - Birleşik Krallık, 30562/04, 04.12.2008, § 112.
[316] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 42.; M.M. – Birleşik Krallık, B. No: 24029/07, 13/11/2012, § 199.
[317] Takdir yetkisinin mutlak ve sınırsız olmaması konusu, hukuk devleti ilkesinin bir gereğidir. Takdir yetkisinin sınırı konusunda ayrıntılı bilgi için bkz. Nilay ARAT ÖZKAYA, "*Türk İdare Hukukunda İdarenin Hukuk Sınırları İçinde Hareket Serbestisi 'Takdir Yetkisi' ve Bunun Sınırları Üzerine Bir İnceleme*", 1. Baskı, Beta, Ekim 2015.
[318] AİHM, Gabriele Weber ve Cesar Richard Saravia - Almanya, B. No: 54934/00, 29/06/2006, § 106
[319] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 48.; Khan – Birleşik Krallık, B. No: 35394/97, 12/05/2000, §§ 26-28.
[320] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 46.; AİHM, Klass ve Diğerleri- Almanya, B. No: 5029/71, 06/09/1978, § 42.
[321] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 46.; Segerstedt-Wiberg ve Diğerleri- İsveç, B. No: 62332/00, 06/06/2006, § 88.

arşivleme yetkisinin kullanılma kapsamı ve biçimi, yerel hukukta yeterli açıklıkla gösterilmediği durumda özel hayata müdahalenin gerçekleştiği sonucuna varılmaktadır. Yerel düzenleme özellikle, yetkinin kötüye kullanıma karşı asgari güvence belirtisini kamuya erişilebilir şekilde öngörmelidir[322].

Ulusal mevzuat, izleme tedbirlerine başvurulmasına karar verme, icra etme ve oluşabilecek durumlarda tazminata ilişkin yeterli ölçüde kesin, etkili ve kapsamlı güvenceler öngörmelidir. Müdahalenin "*demokratik bir toplumda gerekli olması*" ihtiyacı hem genel açıdan hem özel açıdan gerekliliği ifade etmektedir. Yani kişisel verilerin korunması hakkına müdahale edilerek alınan her türlü tedbirin, hem demokratik kurumları korumak için genel bir gerekliliği barındırması hem de özel bir durumda konuya özgü önemli istihbarat elde etmek için kesinlikle gerekli olması şeklinde yorumlanmalıdır. Gereklilik ölçütünün katı uygulanmaması durumunda herhangi bir gizli izleme tedbiri yetkililerce kötüye kullanıma açık hale gelmektedir[323].

Örneğin, *Rotaru/Romanya* (B.No: 28341/195, K.T.: 04.05.2000) Davası'nda Mahkeme, Romanya İstihbarat Örgütü'nün kişilerin özel hayatına ilişkin bilgi toplama ve arşivleme yetkisinin dayanağı olan ulusal düzenlemeyi; yetkiye herhangi bir sınır getirilmemiş olması, bilgileri toplama usulünün gösterilmemiş olması ve bilgilerin kullanılma yöntemini açıklamamış olması gerekçeleriyle, yasal dayanağın bulunmadığı kanaatine varmıştır[324].

Sonuç olarak; AİHM'e göre kişisel verilerin korunması, Sözleşme'nin 8. maddesinde düzenlenen özel hayata saygı hakkından kişinin yararlanması konusunda büyük öneme sahiptir. İç hukuk kişisel verilerin bu maddede düzenlenen güvencelere aykırı bir şekilde kullanımını engellemek için gerekli güvenceleri sağlamalıdır. Otomatik işleme tabi tutulan kişisel verilerin korunması söz konusu olduğunda, özellikle de bu verilerin polis tarafından kullanılması hâlinde, güvencelerin bulunmasının gerekliliği daha fazla hissedilmektedir. İç hukuk, bu verilerin işlenme amaçlarına uygun olarak işlenmesini düzenlemeli, gerektiğinden fazla veri işlenmemesini sağlamalı, verilerin kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edilmesini temin etmelidir. İç

[322] AİHM, Szabó ve Vissy - Macaristan, B. No: 37138/14, 12/01/2016, §§ 72-73.
[323] AİHM, Szabó ve Vissy - Macaristan, B. No: 37138/14, 12/01/2016, §§ 72-73.
[324] Çalışkan, "*Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*", 5.

hukuk, aynı zamanda kişisel verilerin uygun olmayan şekillerde, keyfî ve yetki aşımı yapılarak kullanılmalarına karşı uygun güvenceler de içermelidir[325]. AİHM tarafından ortaya konulan bu ilkeler akıllı güvenlik uygulamaları kapsamında dikkate alınmalıdır.

2. Akıllı Sağlık Uygulamaları Açısından Değerlendirme

Akıllı sağlık uygulamaları, bilgi ve iletişim teknolojileri yardımıyla sağlık verilerinin analiz edilmesini sağlayan, sağlık hizmetlerinin etkili ve hızlı bir şekilde yerine getirilmesini amaçlayan uygulamalardır. Konumuz açısından akıllı sağlık uygulamalarını ikiye ayırmak gerekmektedir. Birincisi, bakıma muhtaç kişilerin sağlık durumunu kontrol etmek amacıyla geliştirilen uygulamalar, ikincisi ise, toplumun genel sağlığını ilgilendiren, salgın gibi durumları önleyici ve kontrol altına alan uygulamalardır. Kişisel sağlık durumunu takip etmek amacıyla yapılan akıllı sağlık uygulamaları KVKK kapsamında olacaktır. Ancak toplumun genel sağlığı ile ilgili geliştirilen uygulamalar kamu düzenini sağlamaya yönelik olarak yürütülen önleyici ve koruyucu faaliyet kapsamında olması nedeni ile bu uygulamlarda KVKK uygulanmayacaktır. Tıpkı akıllı güvenlik uygulamalarında olduğu gibi AİHM ve AYM içtihatları ışığında AİHS ve Anayasa'da belirtilen düzenlemeler uygulanacaktır.

Sağlık verilerinin gizliliğine saygı, Avrupa İnsan Hakları Sözleşmesi'ne taraf devletlerin hepsinin hukuk sistemlerinde temel bir ilkedir. Bir hastanın özel hayatına saygı göstermenin yanı sıra, onun tıp mesleğine ve genel olarak da sağlık hizmetlerine güvenini korumak çok önemlidir. Böyle bir koruma olmadan, tıbbi yardıma ihtiyaç duyanlar, uygun tedaviyi görmek için gerekli olabilecek kişisel ve mahrem nitelikli böyle bir bilgiyi vermekten ve hatta böyle bir yardımı aramaktan dahi cayabilirler. Dolayısıyla da kendi sağlıklarını ve bulaşıcı hastalıklar söz konusu olduğunda toplumun sağlığını tehlikeye atabilirler. Bu nedenle ulusal hukuk, kişisel sağlık verilerinin Sözleşme Madde 8 teminatlarına aykırı olabilecek bir şekilde yayılmasını veya ifşasını önleyecek uygun güvenceleri sağlamalıdır[326].

[325] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 43.; Büyük Daire- S. ve Marper - Birleşik Krallık, 30562/04, 04.12.2008, § 103.
[326] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 43.; Z - Finlandiya, B. No: 22009/93, 25/02/1997, § 95.

Kişinin sağlık durumu kendisi dışında başka insanları da ilgilendiriyorsa, kişisel verilere müdahale haklı görülebilmektedir. Ancak bu durumda bile kişinin özel hayatı, aile ilişkileri, mesleki itibarı, sosyal statüsü gibi durumlar göz önünde bulundurulmalıdır. Örneğin bir kararda AİHM, özel hayat hakkı ve diğer gereklilikler özellikle HIV ile alakalı bilginin gizliliğinin korunması söz konusu olduğunda uygulanacağını, zira bu bilginin ifşası kişinin özel ve aile hayatı ile onun sosyal ve mesleki durumu üzerinde, damgalanmaya ve olası bir dışlanmaya maruz kalma dahil yıkıcı sonuçlar doğurabileceğini vurgulamıştır[327]. Dolayısıyla böyle bir bilginin gizliliğinin korunmasındaki menfaat, müdahalenin güdülen meşru amaçla orantılı olup olmadığının belirlenmesindeki dengede oldukça ağır basacaktır. Böylesi bir müdahale ağır basan kamu yararı menfaati, başvurucunun menfaati ya da hastane çalışanlarının güvenlik menfaati ile meşru kılınmadıkça Madde 8'e uygun olmayacaktır.

Mahkeme bir kişinin sağlığa ilişkin verilerinin çok uzun bir zaman boyunca toplanmasının ve arşivlenmesinin, bunların ifşası ve ilk başta toplanma nedenleriyle alakasız amaçlar için kullanılması ile özel hayata saygı hakkına orantısız bir müdahale teşkil ettiğine karar vermiştir[328]. Bir başka davada AİHM, toplanan kişisel verilerin kapsamı konusunda herhangi bir sınırlama getirilmemesi ve ilgili kurumun olayla doğrudan ilgisi olmayan verileri de ayrım gözetmeksizin elde edebilmesi, yasada keyfiliğin önlenmesine yönelik yeterli korumanın bulunmaması gerekçeleri ile başvuranın özel hayatına yapılan müdahalenin Sözleşme'nin 8/2. maddesi anlamında hukuka uygun olmadığı sonucuna varmıştır[329].

3. İstatistik Uygulamaları Açısından Değerlendirme

Akıllı şehir uygulamalarında elde edilen verilerin kullanım alanlarından biri de kamu politikası belirlemek için analiz yapmaktır. Toplanan veriler istatistiki bilgilere dönüştürülerek bir çıktı alınır. KVKK m. 28'te sayılan istisnai hallerden biri de "*Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi*" olarak belirtilmiştir. KVKK'nın

[327] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 45.; Z - Finlandiya, B. No: 22009/93, 25/02/1997, § 96.
[328] AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", s. 45.; AİHM, Surikov - Ukrayna, B. No: 42788/06, 26/01/2017, §§ 70 ve 89.
[329] T.C. Adalet Bakanlığı, "*Tematik Bilgi Notu – Sağlık*", 2015, s. 6.; AİHM, L.H. – Letonya, B. No: 52019/07, 29/04/2014, §§ 47-60.

uygulanmayacak olması nedeniyle bu durumda da yine AİHM ve AYM içtihatları açısından bir değerlendirme yapılmalıdır.

AYM, resmi istatistik üretmek amacıyla gereksinim duyulan alanlarda kişilerden veri ve bilgi toplanıp analiz edilmesini, kamu düzeni ve ülkenin ekonomik refahı amaçlarına yönelik olduğunu, bu nedenle bu faaliyetlerin AY m. 20 ve AİHS m. 8 açısından meşru amaç olarak kabul edilmesi gerektiğini kabul etmiştir[330]. Modern devletler, objektif ve rasyonel sonuçlar ortaya koyabilmek için istatistik biliminden faydalanmaktadır. Güncel ve gerçek bilgilerin toplanması, ekonomik ve sosyal büyümenin devamlılığını sağlamak için sosyal devlet olmanın da bir gereği olarak görülmüştür[331].

AYM, devletin kamu güvenliği ve planlı kalkınma konularında gerekli önlemleri alabilmesi için toplumun ekonomik durumunu belirlemek amacıyla hane halklarına yönelik anket yapılmasının demokratik bir toplumda gerekli olduğu kanaatindedir[332]. Bu anketler, toplumun tüketim harcamalarını ve ekonomik düzeyini belirlemek amacıyla gerçekleştirilen veri toplama yöntemleridir. Bu veriler, devletin ihtiyaç duyduğu bilgileri sağlayarak, kamu politikalarının oluşturulmasında ve uygulanmasında önemli bir rol oynamaktadır. Anket çalışmalarının yapılabilmesi için belli bir düzeyde kamu gücünün kullanılması gerekmektedir. Bu nedenle AYM, ankete katılımın zorunlu olmasını demokratik toplumda gerekli olarak görmüştür[333].

Örneğin akıllı enerji uygulamaları kapsamında kullanılan akıllı sayaçlar ile kişinin günün hangi saati ne kadar elektrik, su ve doğalgaz gibi enerji kaynaklarını kullandığı tespit edilebilmektedir. Enerji politikasının belirlenmesinde bu sayaçlardan elde edilen veriler istatistiki verileri dönüştürülecektir. Bu işlem için kişilerin rızası olmasa bile zorunlu olarak verileri kullanmak AYM görüşüne göre hukuka uygundur.

E. Sorumluluk

Akıllı şehirlerde veri sorumlusunun mutlaka idare olacağı, idarenin yanında özel hukuk kişisinin de veri sorumlusu olabileceği ancak özel hukuk kişisinin tek

[330] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, §§ 81 ve 82.
[331] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 86.
[332] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 96.
[333] AYM, Güzide Defne Samyeli, B. No: 2014/4399, 21/9/2016, § 97.

başına veri sorumlusu olamayacağını belirtmiştik. Veri işleyen ise idarenin kendisi olabileceği gibi özel hukuk kişisi de olabilir. Veri sorumlusu ve veri işleyenin yapmış oldukları işlemler neticesinde ortaya çıkacak hukuka aykırı durumlardan dolayı idari, cezai ve hukuki sorumluluklar gündeme gelecektir. Hukuka aykırı veri işleme faaliyeti ile karşılaşan bir ilgili kişinin yargı dışı denetim yollarına veya yargısal yola başvurma imkanına sahiptir. Yargı dışı yollar veri sorumlusuna başvuru ile Kişisel Verileri Koruma Kurumu'na başvuru yollarıdır. Yargı yollarında ise duruma göre idari yargı, hukuk yargısı ve ceza yargısına konu durumlar ortaya çıkabilmektedir.

Veri sorumlusuna başvuru yolu KVKK'nın 13. maddesinde düzenlenmiştir. Veri sorumlusu ilgili kişilerden başvuru almak için gerekli altyapıyı hazırlamakla mükelleftir. Gerek yazılı gerek elektronik ortamda müracaat alınabilmelidir. Başvuru ücretsiz olabileceği gibi bir masraf gerektirmesi halinde ücretli de olabilir. Başvuruyu alan veri sorumlusu en geç 30 gün içerisinde ilgili kişiye sonuç hakkında bilgi vermek zorundadır. Başvuru talebinin kabul edilmesi durumunda veri sorumlusu talebin gereğini yerine getirir ve kusur veri sorumlusunda ise aldığı başvuru ücretini de iade eder.

KVKK'nın 14. maddesinde Kurul'a şikâyet yolu düzenlenmiştir. Kanun koyucu doğrudan Kurul'a müracaat etme yolu öngörmemiştir. İlgili kişiler veri ihlalleri ile ilgili hususlarda Kişisel Verileri Koruma Kurulu'na başvurmadan önce veri sorumlusuna başvurmak zorundadır. Veri sorumlusuna başvuran ilgili kişi, gelen cevapla tatmin olmaz yani talebi kabul olmaz veya kabul olmakla beraber soruna çözüm olmazsa veya hiç cevap verilmezse Kurul'a şikâyet yolunu kullanabilir.

1. İdari Sorumluluk

3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'a göre yetkili makamlara yapıla başvurularda, dilekçe ile idareye müracaat eden kişiye en geç 30 gün içerisinde cevap verilmelidir. 2577 sayılı İdari Yargılama Usulü Kanunu'nda idareye başvuru yapılması durumunda idarenin 30 gün içerisinde cevap vermemesi durumunda başvuranın talebinin reddedilmiş sayılacağı düzenlenmiştir. Bu bakımdan veri sorumlusunun idare olduğu durumlarda KVKK'nın hükümleri ile diğer mevzuatın uyumlu olduğu görülmektedir. İlgili kişi, veri sorumlusu idare tarafından veri güvenliğinin ihlal edildiği durumlarda, gerekli düzeltmelerin yapılması için

idareye müracaat edebilir. İdare cevabını 7201 sayılı Tebligat Kanunu'na uygun bir şekilde müracaat edene tebliğ eder.

Veri sorumlusu olan idarenin ilgili kişiye verdiği cevap, müracaat eden kişiyi memnun etmezse kişi Kişisel Verileri Koruma Kurulu'na şikâyet yoluna başvurabileceği gibi doğrudan idari yargıya da başvurabilir. Kurul şikâyet üzerine veya resen veri sorumlunu gerektiğinde inceler. Kurul'un bu yetkisi veri sorumlusunun özel hukuk kişisi veya kamu kurumu olması açısından bir fark yaratmamaktadır. Kurul, veri sorumlusu idarenin işlemlerini inceleyebilir. Ancak ortay çıkacak sonuç açısından farklılık bulunmaktadır. KVKK'da düzenlenen kabahatleri işleyen veri sorumlusu idare hakkında para cezasına karar veremez, veri sorumlusu olan kurum çalışanları hakkında disiplin soruşturması açılması sonucu ortaya çıkar.

İlgili kişi, veri sorumlusu idare tarafından kişisel verileri korunması hakkının ihlal ettiğini düşündüğünde, Kurul'a şikâyet yoluna başvurmak zorunda değildir. Doğrudan 2577 sayılı İYUK'a göre iptal davası ve uğramış olduğu zararların tazmini için tam yargı davası açma yoluna başvurabilir.

Veri sorumlusunun özel hukuk kişisi olduğu durumda da ilgili kişi veri sorumlusuna müracaat edebilir. Özel hukuk kişisi de müracaat almak için gerekli altyapıyı hazırlamakla mükelleftir. Kurul'a şikâyet yolu açısından, başvuru öncesi işlemlerde bir fark olmamakla beraber, Kurul'un incelemesi sonucu ortaya çıkacak sonuçta bir fark bulunmaktadır. Veri sorumlusu özel hukuk kişisi olduğunda Kurul, KVKK'da belirtilen kabahatlerin işlendiği kanaatine varırsa idari para cezasına karar verecektir.

2. Cezai Sorumluluk

KVKK'nın 17. maddesinde suçlar ve cezai yaptırımlar açısından 5237 sayılı Türk Ceza Kanunu'nun ilgili maddelerine atıf yapılmıştır.

TCK'nın 135. ve 136. maddelerinde, kişisel verileri hukuka aykırı olarak kaydeden, ele geçiren, başkasına veren ve yayan kişilerin, TCK'nın 138. maddesinde de, kişisel verileri silmeyen veya anonim hale getirmeyenlerin cezalandırılacağı düzenlenmiştir. Kamu görevlileri açısından, görevinin verdiği yetki kötüye kullanılmak suretiyle 135. ve 136. maddelerde belirtilen suçlar işlendiğinde cezanın yarı oranında artırılacağı düzenlenmiştir.

3. Hukuki Sorumluluk

Kişisel verilerin korunması hakkı, kişilik hakkının önemli bir parçasıdır. KVKK yürürlüğe girmeden önce de kişilik hakları hukukumuzda korunmaktaydı. 4721 sayılı Türk Medeni Kanunu'nun 23.,24., ve 25. maddelerinde kişiliğin korunmasına ilişkin düzenlemeler yapılmıştır. Özel hukuk kapsamında;

- Kişilik hakkına yönelik ciddi ve yakın bir saldırı tehlikesi bulunması durumunda önleme davası,
- Kişilik hakkına yönelik devam eden bir saldırı bulunması durumunda durdurma davası,
- Kişilik hakkına yönelik yapılan saldırının ortaya konulması için tespit davası,
- Kişilik hakkına yönelik yapılan saldırı neticesinde zarara uğranması durumunda tazminat davası açılabilecektir[334].

Akıllı şehirlerde veri sorumlusu idarenin yapmış olduğu işlemler nedeniyle idari yargıya başvurulması gerektiğini belirtmiştik. Şayet idare, bir özel hukuk kişisi ile ortak veri sorumlusu olduğunda, özel hukuk kişisinin ihlallerinden dolayı özel yargıya gidilmesi gerekecektir.

[334] Çabuk, "*Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması*", 123.

SONUÇ

Akıllı şehirler, iletişim teknolojileri, akıllı güvenlik, coğrafi bilgi sistemleri, akıllı altyapı, bilgi teknolojileri, akıllı sağlık, bilgi güvenliği, akıllı yapılar, afet ve acil durum yönetimi, akıllı ekonomi, akıllı insan, akıllı enerji, akıllı çevre, akıllı ulaşım, akıllı yönetişim ve akıllı mekân yönetimi bileşenlerinden oluşur. Akıllı şehirler, atık yönetimi, evler, binalar, trafik sistemleri, ulaşım sistemleri, su şebekeleri, suç tespit sistemleri, hastaneler, okullar ve kütüphaneler gibi şehrin tamamını kapsayan kamu hizmetleri izlemek ve yönetmek için, elektronik nesnelerin sensör denilen algılayıcıları yardımıyla verileri toplayan ve toplanan verilerden çıkarmış olduğu bilgileri kullanan şehirlerdir. Veri, akıllı şehir kavramının olmazsa olmazıdır.

Kamu hizmetlerinin kalitesinin yükseltilmesi için yapılan veri toplama faaliyetleri ise insanların mahremiyetini tehdit etmektedir. Kişilerin resim, görüntü, tahlil sonuçları, yargılama bilgileri, günlük hareket bilgileri, alışkanlıkları, yapılan alışverişler gibi daha birçok mahrem bilgisi kayıt altına alınıp bir veri bankasında toplanmakta, bu veri bankasında elde edilen büyük verilerden yola çıkılarak kişi hakkında analiz yapılabilmektedir. Dolayısıyla kişinin en mahrem bilgileri kamu kuruluşlarının ve özel kuruluşların eline geçmektedir.

Kamu hizmetlerinin yerine getirilmesi, şehirde hayat kalitesinin artırılması, şehir sakinlerinin daha rahat bir yaşam tarzı edinmesi için toplanan verilerin başka amaçlar için kullanılıp kullanılmayacağı belirsizdir. Toplanan verilerin nerede tutulduğu, kimlere verildiği, ne zaman yok edildiği gibi hususları vatandaş bilmemektedir. Günümüzde veri, "*çağın petrolü*" olarak nitelendirilmekte olup veri tüccarları tarafından başka kişilere yüksek meblağlar ile satılmaktadır. Çünkü veri, insan profilleri hakkında bilgiler vermekte olup üretim planlaması, ürün pazarlaması ve manipüle etme yöntemleri için kullanabilen bir metadır. Akıllı şehirlerde kişisel verilerin toplanmasıyla veri bankası oluşturan idarenin, bütçeye kaynak sağlamak amacıyla verileri veri tüccarlarına satma ihtimali her zaman vardır. Bunun yanında siyasi iktidar, verilerle kişi profili oluşturma ve kişileri manipüle etme gibi yöntemlerle propaganda yaparak, iktidarının devamını sağlamak isteyebilir. Bu nedenle, verileri toplanan akıllı kent sakinlerinin, verilerinin akıbetini öğrenmeleri, veri bankasını yöneten kişileri denetlemesi, verilerin amacına uygun

davranıldığından emin olması gerekmektedir. Bunun için gerekli teknik, idari ve hukuki altyapının sağlanması elzemdir.

Kamu hizmetlerinin büyük bir çoğunluğu KVKK kapsamında değildir. Resmi istatistik tutmak, millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamak, soruşturma, kovuşturma, yargılama veya infaz işlemleri kanunda istisna olarak sayılarak, kanun hükümlerinin uygulanmayacağı belirtilmiştir. Bu durumlarda Anayasa ve uluslararası düzenlemeler, kişisel verilerin korunması hakkını koruyan düzenlemeler olarak kalmaktadır.

Ayrıca günümüzde akıllı şehir konseptinin kurucuları, bütünleşik sorunlara kolay çözümler bulmak amacıyla mümkün olduğunca çok veri toplamak istemektedir. Bir şehrin akıllı şehre dönüşebilmesi için teknolojilerini ve dijital gelişmelerini bir bütün haline dönüştürmesi gerektiği, bu nedenle farklı amaçlarla farklı veri tabanına toplanan verilerin bir bütün haline getirilmesi gerektiğin savunulmaktadır. Halbuki kişisel verilerin korunması hukukunda "*amaçla sınırlı olma*" ilkesi çok önemlidir. Veriler işlenme amaçları haricinde başka amaçla işlenmemelidir. Veriler "*belki ilerde lazım olur*" düşüncesiyle toplanmamalıdır. Diğer yandan, tam olarak neden gerekli olduğu izah edilmeksizin olabildiğince çok veri toplamak ölçülülük ilkesini de ihlal edecektir.

Anlatılan bu sorunlar akıllı şehirlerde veri toplama, kayıt altına alma, depolama, analiz etme, saklama, silme, yok etme ve anonim hale getirme süreçlerinde bir belirsizlik yaratmaktadır. Bu belirsizliğin giderilmesi için, akıllı şehirler henüz yeni doğarken, kanuni bir düzenleme ile akıllı şehirlerin hukuki altyapısı da inşa edilmelidir. Akıllı şehirlerin bir panoptikon modeline dönüşmemesi, kişilerin bir obje gibi değerlendirilmemesi, insanların her daim izlendiklerini düşünerek insan onuruna aykırı bir hayat yaşamaması için, kişisel verilere saygılı bir akıllı şehir yönetimi şarttır. Bu nedenle akıllı şehirlerde kişisel verilerin korunması hakkı büyük önem arz etmektedir.

Devlet politikası olarak belirlenen toplumsal refahı artırmanın bir yöntemi olan teknolojik olanakların kullanılması ile temel hukuk devleti ilkesi gereğince asıl olan temel hak ve özgürlüklerin korunması arasında makul dengenin oluşturulması için, mahremiyetin korunmasına yönelik uygulamaların iç hukuka aktarılması

gerekmektedir. Bu aktarım sadece mevzuat düzeyinde değil aynı zamanda devletin tüm organları tarafından uygulanabilir düzeyde olmalıdır.

KAYNAKÇA

ADALET BAKANLIĞI, "*Tematik Bilgi Notu – Sağlık*", 2015.

AIHEMAITI, Aınıwaer, "*Türkiye'deki Akıllı Şehirlerin Sıralama Modeli*", Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2018.

AİHM, "*Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi*", 2019, https://www.echr.coe.int/documents/d/echr/Guide_Art_8_TUR (Çevrimiçi Tarihi: 19.07.2023).

ALTINOK ÇALIŞKAN, Elif, "*Dijital Dönüşümün Getirdiği Yeniliklerin Kamu Hizmetine Uyarlanmasında Yeni Bir Kavram Olarak 'Ortak Hizmet Sunumu' Üzerine Değerlendirmeler*", UYSAD 6th International Management and Social Research Conference, Proceeding Book, C. I, 2021.

ARAT ÖZKAYA, Nilay, "*Türk İdare Hukukunda İdarenin Hukuk Sınırları İçinde Hareket Serbestisi 'Takdir Yetkisi' ve Bunun Sınırları Üzerine Bir İnceleme*", 1. Baskı, Beta, Ekim 2015.

ATEŞ, Mücella, "*Akıllı Şehir Olgusunu Değerlendirme Yaklaşımında Yerel Boyut*". Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2018.

AVCIOĞLU, Abdurrahman, "*Akıllı Şehirlerden Akıllı Ülkelere: Akıllı Ülke Sıralama Modeli ve Türkiye Analizi*", Doktara Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara 2020.

AYDIN, Yavuz Selim, "*Gözetim Toplumu Bağlamında Kişisel Verilerin Korunmasında Karşılaşılan Sorunlar ve Riskler*", Yüksek Lisans Tezi, Muğla Sıtkı Koçman Üniversitesi Sosyal Bilimler Enstitüsü, Muğla 2022.

AYGÜN, Merve, "*Akıllı Şehir Yönetişiminde Toplumun Karar Alma Mekanizmalarına Katılımı: İstanbul Beyaz Masa Örneği*", Yüksek Lisans Tezi, İstanbul Medeniyet Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul 2020.

BAL, Hüseyin, "*Kent Sosyolojisi*", 9. Bs., Bursa: Sentez Yayıncılık, 2020.

BARUTÇU, Burcu, "*Akıllı Şehirler Üzerine Sistemik Bir Literatür Taraması ve Akıllı Şehirlerde Endüstri Mühendisliği Uygulama Alanları*", Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara 2021.

BAŞARAN, İsmail, "*Sağlıklı Kentler Kavramının Gelişiminde Sağlıklı Kentler Projesi*", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 9/3 (2007).

BENTHAM Jeremy/PEASE-WATKIN Catherine/WERRET Simon/ÇOBAN Barış/ ÖZARSLAN Zeynep, "*Panoptikon Gözün İktidarı*", 3. bs. Su Yayınları, İstanbul, 2019.

CUI, Lei/XIE, Gang/QU, Youyang/GAO, Longxiang/YANG, Yunyun, "*Security and Privacy in Smart Cities:Challenges and Opportunities*". IEEE Access, C:6, 2018, s. 46134 - 46145.

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

ÇALIŞKAN, Ayla, "*Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*", (https://www.jurix.com.tr/article/20726).

ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI, "*2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı"*.

DOĞRU, Osman/NALBANT, Atilla, "*İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar*", C. 2, 1. bs., Pozitif Matbaa, Ankara, 2013.

DORUK, Büşra, "*Teknoloji ile Bütünleşen Şehirlerde Akıllı Şehir Yönetiminin Analizi*", Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir 2022.

DUMAN, Berat, "*Anayasa Hukukunda Kişisel Verilerin Korunması*" Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya 2020.

DÜLGER, M.Volkan, "*Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması*", Yaşar Hukuk Dergisi C.1 S.2 Temmuz 2019, syf.71-174.

EMİKÖNEL, Melek, "*Göç ve Akıllı Şehir Türkiye Uygulaması*", Yüksek Lisans Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2021.

ER, Habibe Esra, "*Mobil Uygulamalarda Kişisel Verilerin Korunması*", Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2020.

ERSOY, Melih, "*Kentsel Planlama – Ansiklopedik Sözlük*", 2. bs., Ninova Yayıncılık, İstanbul, 2016.

GÜLAN, Aydın. "*Kamu Hizmeti ve Görülüş Usulleri*", Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 1987.

GÜLMEZ, Savaş Muharrem, "*Yerel Yönetimlerde Akıllı Şehir Uygulamalarının Yansımaları ve Süreç Yönetimi: İstanbul Büyükşehir Belediyesi Örneği*", Yüksek Lisans Tezi, İbni Haldun Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul 2022.

GÜNDÜZ, Mehmet Şükrü, "*Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği*", 1. bs., Adalet Yayınevi, Ankara, 2022.

GÖRMEZ, Kemal. "*Şehir ve İnsan*", Milli Eğitim Basımevi, İstanbul, 1991.

HUOT, Jean Louis/THALMANN, Jean Paul/VALBELLE, Dominique, "*Kentlerin Doğuşu",* Çev. Ali Bektaş Girgin, İmge Kitabevi, Ankara, 2000.

ILGAZ, Elif, "*Akıllı Şehirler ve Akıllı Şehirlerin Kurulmasında Rüzgar Enerjisinin Yönetimi ve Organizasyonu*", Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018.

ISMAGILOVA, Elvira/HUGHES, Laurie/RANA, Nripendra/DWIVEDI, Yogesh K, "*Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework*", Information Systems Frontiers, 2022, s. 393-414.

KESKİN, Züleyha, "*Kamu Hizmetlerinde Eşitlik İlkesi*", Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2014.

KILINÇ SUCU, Büşra Merve. "*Temel Hak Boyutuyla Kişisel Verilerin Korunması*", Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir, 2022.

KİŞİSEL VERİLERİ KORUMA KURUMU, "*Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi*".

KİŞİSEL VERİLERİ KORUMA KURUMU, "*Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)*".

KİŞİSEL VERİLERİ KORUMA KURUMU, "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi*".

KİŞİSEL VERİLERİ KORUMA KURUMU, "*Veri Sorumlusu ve Veri İşleyen Rehberi".*

KÜZECİ, Elif, "*Kişisel Verilerin Korunması*", Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2010.

ONAR, **Sıddık Sami**, "*İdare Hukukunun Umumi Esasları*", Marifet Basımevi, İstanbul, 1952.

OKUR, Ulvi, "*Kamu Hizmeti Sunan Aktörlerin Anlatılarında Kentsel Politik Mekanlar: Gazi Mahallesi Örneği*", Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2022.

OVALIOĞLU, Senem. "*Avrupa Birliği Hukukunda Kişisel Verilerin Korunması*", Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2021.

ÖZSÜER, Özgür, "*Akıllı Şehir Uygulamaları ve İstanbul Büyükşehir Belediyesi Örneği*", Bitirme Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2017.

ÖZTÜRK, Bahri/ALTINOK ÇALIŞKAN, Elif/SEYHAN, Serkan, "*Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı",* Seçkin Yayıncılık, Ankara, 2022.

POLAT, Erkan, "*Ağır Ağır Çıkacaksın Bu Merdivenlerden: Yavaş Kent Hareketi (Cittaslow)*" Mimarlık Dergisi, S: 359, Mayıs-Haziran 2011.

SANCAKDAR, Oğuz, ÖNÜT, Lale Burcu, US DOĞAN, Eser, KASAPOĞLU TURHAN, Mine, SEYHAN, Serkan, "*İdare Hukuku Teorik Çalışma Kitabı*", 11 bs., Ankara, Seçkin Yayıncılık, 2022.

SARIGÜL, Merve Melek, "*Yapay Zeka Teknolojilerinin Akıllı Şehirlerdeki Uygulamalarına Yönelik Bir Araştırma: Konya İli Örneği*", Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2022.

SINMAZ, Serkan, "*Yeni Gelişen Planlama Yaklaşımları Çerçevesinde Akıllı Yerleşme Kavramı ve Temel İlkeleri*", Megaron, C. 8, S. 2, 2013, s. 76-86.

SOLMAZ, Eren, "*Avrupa İnsan Hakları Mahkemesi Kararları'nın 'Kişisel Verilerin Korunması'na Katkısı*", İdare Hukuku ve İlimleri Dergisi, C. 18, S. 1, 2019, s. 61-78. (https://doi.org/10.26650/ihid.644402).

ŞENAY ÖZKAN, Nefise Ayşe, "*Belediye Hizmetlerinin Sunumu Bağlamında Akıllı Şehirler: Çanakkale Belediyesi Örneği*". Yüksek Lisans Tezi, Çanakkale OMÜ Lisansüstü Eğitim Enstitüsü, Çanakkale, 2022.

ŞENER, Raziye Betül, "*Kamu Hizmeti Anlayışındaki Değişim ve Akıllı Kentler*", Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2019.

ŞENTEK, Arif, "*Sorumlu Bir Mimarlık İçin Manifesto*", Mimarlık Dergisi, S:387, Ocak- Şubat 2016.

TAŞÇI, Burak, "*Akıllı Şehir Teknolojileri Kapsamında Türkiye Uygulamaları Örneği*", Yüksek Lisans Tezi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara, 2021.

TEZCAN, Durmuş/ERDEM, M.Ruhan/SANCAKDAR, Oğuz/ÖNOK, R.Murat, "*İnsan Hakları El Kitabı"*, Seçkin Yayıncılık, Ankara, 2021.

TOLUN, Yüksel, "*Kişisel Verilerin KVKK ve GDPR Kapsamında Korunması*", Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale, 2020.

TOPAL, A.Kadir, "*Kavramsal Olarak Kent Nedir ve Türkiye'de Kent Neresidir*?". Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, C. 6, S.1, 2004, s. 276-294.

ULUK, Murat, "*Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*", Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2022.

WIRTH, Louis, "*Bir Yaşam Biçimi Olarak Kentlileşme*", Ayten Alkan, Bülent Duru (Der. ve Çev.), 20. Yüzyıl Kenti, İmge Yayınevi, Ankara, 2002.

YALÇINER ERCOŞKUN, Özge, "*Sürdürülebilir Kent İçin Ekolojik-Teknolojik (Eko-tek) Tasarım: Ankara-Güdül Örneği*", Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2007.

YILMAZ, Tüze, "*Avrupa Birliğinde Kişisel Verilerin Korunması*", Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2022.

YÜZBAŞI TOBAZ, Firdevs, "*Uluslararası İnsan Hakları Hukukunda ve Türk Hukukunda Kişisel Verilerin Korunması*", Doktora Tezi, Trabzon Üniversitesi Lisansüstü Eğitim Enstitüsü, Trabzon, 2021.

ZHUANG, Rongxia/FANG, Haiguang/ZHANG, Yan/LU, Aofan/HUANG, Ronghuai, "*Smart Learning Environments For A Smart City: From The Perspective Of Lifelong And Lifewide Learning*", Open Access, C. 4, S. 6, 2017.

İNTERNET KAYNAKLARI

https://www.academia.edu/14408770/Dijital_Kentler_ve_Kent_Y%C3%B6neti (Çevrimiçi Tarihi: 14.07.2023)

https://akillisehir.istanbul/tr/ (Çevrimiçi Tarihi:03.06.2023)

https://insanhaklarimerkezi.bilgi.edu.tr/tr/content/117-medeni-ve-siyasi-haklara-iliskin-uluslararas-sozlesme/ (Çevrimiçi Tarihi:20.05.2023)

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Çevrimiçi Tarihi: 07.05.2023)

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487 (Çevrimiçi Tarihi: 10.05.2023)

https://www.akillisehirler.gov.tr/ (Çevrimiçi Tarihi:03.06.2023)

https://www.kvkk.gov.tr/Icerik/2030/Rehberler?&page=3 (Çevrimiçi Tarihi: 11.05.2023)

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf (Çevrimiçi Tarihi: 03.06.2023)

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/31d9c444-27a5-4a75-95b1-1ca9bdb81ea5.pdf (Çevrimiçi Tarihi: 03.06.2023)

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/a569a068-c079-4189-b134-f57bc727af7d.pdf (Çevrimiçi Tarihi: 03.06.2023)

https://www.oecd.org/60-years/ (Çevrimiçi Tarihi: 07.05.2023)

https://www.oecd.org/60-years/timeline/#selectorBlock (Çevrimiçi Tarihi: 07.05.2023)

https://www.oecd.org/digital/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm (Çevrimiçi Tarihi: 10.05.2023)

https://akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf (Çevrimiçi Tarihi: 05.04.2023)

http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET(2014)507480_EN.pdf (Çevrimiçi Tarihi: 14/07/2023)

https://www.centreforcities.org/reader/smart-cities/what-is-a-smart-city/ (Çevrimiçi Tarihi:14/07/2023)

https://population.un.org/wup/Publications/Files/WUP2014-PressRelease.pdf (Çevrimiçi Tarihi: 21.07.2023)