International Journal of Business, Economics and Management Perspectives
Uluslararası İşletme, Ekonomi ve Yönetim Perspektifleri Dergisi
Volume/Cilt: 10, Issue/Sayı: 1, pp/ss. 71-87
E-ISSN: 2458-8997
URL: https://ijbemp.com/
DOI: http://dx.doi.org/10.29228/ijbemp.94329
June/Haziran 2026

Article Type / Makale Türü: Araştırma Makalesi - Research Article
Application Date / Başvuru Tarihi: 04.08.2026 / 08.04.2026
Admission Date / Yayına Kabul Tarihi: 06.23.2025 / 23.06.2026

AKILLI KENT UYGULAMALARINDA VERİ GÜVENLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI: HUKUKİ RİSKLER VE DÜZENLEYİCİ ÇERÇEVENİN DEĞERLENDİRİLMESİ

DATA SECURITY AND PROTECTION OF PERSONAL DATA IN SMART CITY APPLICATIONS: EVALUATION OF LEGAL RISKS AND THE REGULATORY FRAMEWORK

Yasemin HAYTA[1], Sedat KIZILDAĞ[2]

ÖZ: Bilgi ve iletişim teknolojilerinin hızla geliştiği günümüz dünyasında, kentlerin yönetim biçimi de köklü bir dönüşüm sürecine girmiştir. Bu dönüşümün en somut yansımalarından biri olan akıllı kent uygulamaları, kentsel hizmetlerin daha etkin, verimli ve sürdürülebilir bir şekilde sunulmasını mümkün kılmaktadır. Ancak bu teknolojik ilerleme, beraberinde önemli sorumlulukları ve yeni risk alanlarını da getirmektedir. Araştırma sürecinde, hem ulusal hem de uluslararası çalışmalar incelenmiş; Türkiye'de yürürlükte bulunan Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) çerçevesinde mevcut düzenlemeler analiz edilmiştir. Bu kapsamda, teknolojik gelişmeler ile hukuki düzenlemeler arasındaki ilişki, ortaya çıkan riskler ve çözüm önerileri sistematik bir bakış açısıyla değerlendirilmiştir. Veri güvenliği meselesi, maalesef sadece teknik önlemler alınarak çözülebilecek kadar basit değildir. Süreçteki şeffaflık eksikliği, sorumluluk alanının tam olarak bilinememesi ve koruma ilkelerinin pratikte çoğu zaman somutlaşamaması gibi çok boyutlu sorunlar bulunmaktadır. Bu doğrultuda, teknik altyapı eksikliklerinin giderilmesi ile kurumların bu alandaki yetkinliklerinin artırılması eşgüdümlü olarak yürütülmelidir.

Anahtar Kelimeler : Akıllı Kentler, Kişisel Verilerin Korunması Kanunu (KVKK), Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), Veri Koruma Hukuku, Nesnelerin İnterneti (IoT).

ABSTRACT: In today's world, where information and communication technologies are rapidly developing, the way cities are managed has also undergone a radical transformation. Smart city applications, one of the most concrete reflections of this transformation, make it possible to provide urban services more effectively, efficiently, and sustainably. However, this technological progress also brings with it significant responsibilities and new areas of risk. In the research process, both national and international studies were examined; and the existing regulations within the framework of the Personal Data Protection Law (KVKK) in force in Turkey and the General Data Protection Regulation (GDPR) of the European Union were analyzed. In this context, the relationship between technological developments and legal regulations, the emerging risks, and proposed solutions were evaluated from a systematic perspective. The issue of data security is unfortunately not as simple as being solved by taking only technical measures. There are multi-dimensional problems such as the lack of transparency in the process, the inability to fully know the area of responsibility, and the fact that the protection principles are often not concretized in practice. Accordingly, addressing the deficiencies in technical infrastructure and increasing the competencies of institutions in this area should be carried out in coordination.

Keywords: **Smart Cities, Personal Data Protection Law (KVKK), General Data Protection Regulation (GDPR), Data Protection Law, Internet of Things (IoT).**

1. Doç. Dr. Balıkesir Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, yasemin.hayta@balikesir.edu.tr, https://orcid.or/0000-0003-4450-6444
2. Bağımsız Araştırmacı, avsedatkizildag@gmail.com, https://orcid.org/0009-0005-5224-9101

EXTENDED SUMMARY

Research Problem

The rapid expansion of smart city infrastructures has led to the continuous collection, processing, and storage of vast amounts of personal data. While these data-driven systems enhance the efficiency and quality of urban services, they simultaneously create significant risks concerning data security and individual privacy. One of the central challenges in this transformation process is the inability of existing legal frameworks to keep pace with technological advancements (Badii vd., 2020; Daoudagh vd., 2021). This gap increases the likelihood of large-scale surveillance practices and weakens the protection of fundamental rights. In the context of Türkiye, ambiguities in the implementation of personal data protection regulations and limitations in enforcement mechanisms further complicate this issue. Therefore, the primary research problem of this study is to examine the extent to which current legal frameworks are capable of addressing data security and privacy risks arising from smart city applications.

Research Questions

his study seeks to answer the following research questions:How do smart city technologies affect personal data security and individual privacy?What are the main legal risks associated with data collection and processing in smart city ecosystems?To what extent do the Turkish Personal Data Protection Law (KVKK) and the European Union's General Data Protection Regulation (GDPR) provide adequate protection against these risks?What are the similarities and differences between KVKK and GDPR in regulating data protection within smart city contexts?What kind of legal, technical, and institutional measures are required to ensure effective data protection in smart cities?

Literature Review

he existing literature demonstrates that smart city ecosystems are characterized by the integration of advanced technologies such as the Internet of Things (IoT), big data analytics, and artificial intelligence, which enable real-time data collection and analysis. While these technologies contribute to increased efficiency in urban governance, they also generate complex challenges related to data security and privacy. Previous studies emphasize that the extensive and continuous collection of personal data in smart cities raises concerns about surveillance, unauthorized access, and misuse of information.Scholars argue that current legal frameworks often struggle to keep up with the speed of technological innovation, leading to regulatory gaps. In this context, the GDPR is frequently highlighted as a comprehensive and robust model that establishes strict principles such as data minimization, transparency, and accountability. Similarly, Türkiye's KVKK provides a legal basis for personal data protection; however, studies indicate that its implementation may face certain limitations in practice.Moreover, the literature underlines that ensuring data protection in smart cities requires not only legal regulations but also strong technical infrastructure and institutional capacity. Interdisciplinary approaches that combine law, technology, and public administration are therefore essential for addressing the multidimensional nature of these challenges.

Methodology

This study is designed within the framework of qualitative research and adopts a descriptive and analytical approach. The research primarily relies on document analysis and literature review methods to examine data security and privacy issues in smart city applications.In the data collection process, primary sources include legal documents such as the Turkish Personal Data Protection Law (KVKK), the General Data Protection Regulation (GDPR), and relevant constitutional provisions. Secondary sources consist of academic studies, institutional reports, and international policy documents related to smart cities and data protection.The collected data were analyzed through thematic and content analysis techniques. Initially, key themes such as data security, privacy, legal frameworks, and technological risks were identified. Subsequently, these themes were systematically examined to reveal patterns, similarities, and differences between national and international practices. A comparative perspective was adopted to evaluate Türkiye's current legal framework in relation to global standards.This methodological approach allows for a comprehensive and multidimensional assessment of data protection challenges in smart city ecosystems. Metin girmek için buraya tıklayın veya dokunun.

1. GİRİŞ

Bilgi ve iletişim teknolojilerindeki hızlı ivmelenme, şehir yaşantısını köklü biçimde değiştiren "akıllı kent" modelini güçlü bir şekilde gündeme taşımıştır. Günümüzde bu şehirler; fiziksel ve dijital altyapıların otomasyonla harmanlandığı, yönetimin ise ağırlıklı olarak veriye dayalı işlediği çok katmanlı mekanizmalar olarak öne çıkmaktadır (Özdemir, 2025). Sistemin adeta omurgasını oluşturan Nesnelerin İnterneti (IoT) teknolojisi de hem kentsel hizmetlerin pratikliğini artırmakta hem de yaşam standartlarını doğrudan yukarı çekmektedir (Görgül, 2024). Ancak sürecin riskler barındıran başka bir boyutu daha ortaya çıkmıştır. Bu sistemlerin kentin her alanına yayılması, kesintisiz ve devasa bir kişisel veri toplama döngüsü meydana getirmektedir. Haliyle sistem genişledikçe; siber güvenlik zafiyetleri, sınırları tam çizilemeyen hukuki sorumluluklar ve yasal denetim boşlukları gibi karmaşık problemler de kaçınılmaz olarak su yüzüne çıkmaktadır (Kocabıyık, 2023; Özçağdavul & Sayan, 2023). Bu çalışma, akıllı kent uygulamalarında veri güvenliği ve mahremiyet meselesini yalnızca hukuki düzenlemelerin betimlenmesiyle sınırlı kalmayarak, Türkiye'deki mevcut veri koruma rejimini Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ile karşılaştırmalı bir çerçevede ele almaktadır. Çalışmanın özgün katkısı, akıllı kent ekosistemlerinde ortaya çıkan veri güvenliği risklerini; hukuki, teknik ve yönetsel boyutları birlikte değerlendiren bütüncül bir analiz sunmasında yatmaktadır. Ayrıca çalışma, literatürde sıklıkla ayrı ayrı ele alınan veri koruma hukuku ile akıllı kent teknolojileri arasındaki etkileşimi bütüncül bir perspektifle inceleyerek, kamu yararı ile bireysel mahremiyet arasındaki dengeye yönelik politika önerileri geliştirmektedir

2.Akıllı Kent Kavramı ve Tanımları

Akıllı kent kavramı, teknolojik yeniliklerin kentsel mekâna entegre edilmesiyle doğmuş ve zamanla sürekli evrilen dinamik bir yapıya bürünmüştür. Literatürde henüz üzerinde uzlaşılmış ortak bir tanımı bulunmayan bu kavram, doğası gereği disiplinler arası bir özellik sergilemektedir (Ünsal & Avcı, 2023). Kavramsal bir çerçeveden yaklaşıldığında akıllı kentler; bilgi ve iletişim teknolojilerini temel alarak kentsel hizmetlerin niteliğini, kentin genel güvenliğini ve buna bağlı olarak toplumsal refahı artırmayı hedefleyen bütüncül sistemler olarak değerlendirilmektedir (Görgül, 2024). Bu yaklaşımın özünde, mevcut altyapıyı dijital ağlar vasıtasıyla modernize etme düşüncesi yatar. Ulaşılmak istenen nihai hedef ise sağlanan bu dönüşüm sayesinde çok daha yaşanabilir ve sürdürülebilir kentsel mekânlar oluşturmaktır (Özçağdavul & Sayan, 2023). Uygulama pratiği açısından değerlendirildiğinde süreç; kentsel altyapının bilgi teknolojileri entegrasyonuyla yeniden şekillendirilmesini ve kent yönetiminin doğrudan veri temelli mekanizmalar üzerinden yürütülmesini

merkeze almaktadır. Bu yaklaşım, birbirinden bağımsız altyapı unsurlarının dijital ortamda bütünleşmesini sağlarken hizmet sunumunu da belirgin biçimde etkinleştirmektedir. Ayrıca bu entegrasyon süreci, sadece teknik cihazların kurulumundan ibaret olmadığı görülmektedir. Verinin toplanması, analiz edilmesi ve kurumlar arası paylaşımı, güçlü bir işbirliğini ve sağlam bir yönetişim mekanizmasını zorunlu kılmaktadır. Akıllı kent olgusu; coğrafi bilgi sistemleri ile kapsamlı dijitalleşme süreçlerinin sentezinden doğan, çok katmanlı ve dinamik bir yapıyı temsil etmektedir. Bu noktada dijital dönüşümü, yalnızca fiziksel verilerin dijital formata taşındığı teknik bir "sayısallaştırma" işlemi olarak görmek, meselenin kavramsal derinliğini ve operasyonel gücünü göz ardı etmek anlamına gelmektedir. Ünsal ve Avcı'nın (2023) da isabetle belirttiği üzere, bu süreç salt bir veri aktarımı değil; kentsel mekanın yeniden organizasyonu ve dönüşümünde belirleyici bir kaldıraçtır. Dolayısıyla dijitalleşme, teknik bir prosedür olmanın ötesine geçerek, modern kentsel dönüşüm stratejilerinin merkezinde yer alan, mekanı ve toplumsal yaşamı yeniden kurgulayan temel bir yapı taşı olarak kabul edilmektedir.

Akıllı kent projelerinin başarısını tartarken, konuyu sadece teknolojik donanımın yeterliliğine veya gelişmişlik düzeyine hapsetmek oldukça sığ bir yaklaşım olmaktadır. Kurulan bu sistemlerin gerçek anlamda işlevsellik kazanması, dijital kapasiteden ziyade, söz konusu kentin kendine has sosyal dokusu ve mevcut idari işleyişiyle ne ölçüde bütünleşebildiğine bağlıdır. Bundan ötürü teknoloji, yerel dinamiklerle ve yönetim mekanizmalarıyla uyum sağladığı oranda kalıcı bir karşılık bulabilmektedir. Dolayısıyla bu süreci sadece teknik bir ilerleme olarak değil; sosyolojik ve yönetsel katmanları da içine alan kapsamlı bir dönüşüm olarak okumak gerekmektedir (Ünsal & Avcı, 2023). Bu noktada, geliştirilen inovatif çözümlerin kentin yerel ihtiyaçlarıyla doğrudan örtüşmesi kritik bir öneme sahip olduğu görülmektedir. Yerel dinamiklerle uyumlu bir tasarım süreci, hem vatandaşın bu dijital dönüşüm süreçlerine aktif katılımını kolaylaştırmakta hem de projelerin toplumsal tabanda meşruiyet kazanarak benimsenmesini sağlamaktadır (Ünsal & Avcı, 2023). Sonuç itibarıyla teknoloji, kentin toplumsal ve idari yapısıyla bütünleşebildiği ölçüde sürdürülebilir bir verimlilik sunabileceği görülmektedir.

2.1.Akıllı Kent Teknolojileri

Akıllı kent ekosistemi, kentsel dinamikleri dijital bir dönüşüme uğratırken, veri odaklı karar mekanizmalarını besleyen geniş bir teknolojik yelpazeden güç almaktadır. Bu yapı içerisinde Nesnelerin İnterneti (IoT), kentsel verilerin anlık olarak derlenmesi ve işlenmesi safhalarında kritik bir işlev üstlenerek akıllı şehir mimarisinin temel omurgasını teşkil etmektedir (Görgül, 2024). IoT ile eşgüdümlü çalışan internet tabanlı teknolojiler ise veri merkezli planlamayı kolaylaştırmakta, hızlı müdahale kapasitesini geliştirerek yerel yönetimlerin operasyonel verimliliğini üst seviyeye taşımaktadır. Akıllı kent ekosistemleri, özünde veri odaklı mekanizmalar üzerine temellenmekte; bu doğrultuda büyük veri ve açık veri stratejileri sürecin belirleyici unsurları olarak öne çıkmaktadır.

Büyük veri teknolojileri, kentsel ağlardan süzülen yoğun veri trafiğinin analiz edilerek stratejik bilgiye dönüştürülmesine imkân tanımaktadır. Açık veri politikaları ise şeffaflık ve katılımcılık zemininde, bireylerin yerel yönetim süreçlerine dahil olmasını kolaylaştıran demokratik bir işlev üstlenmektedir. Öte yandan bu dijital altyapı, kamu hizmetlerinde verimlilik artışı vaat etse de veri güvenliği ve bireysel mahremiyetin korunması gibi kritik risk başlıklarını da beraberinde getirmektedir (Hayta, 2021; Özçağdavul & Sayan, 2023).

Yapay zekâ, büyük veri analitiği ve otomasyon sistemlerinin IoT ile eklemlenmesi, kaynak kullanımını optimize ederek kentsel hizmetlerin daha rasyonel sunulmasını sağlamaktadır (Ünsal & Avcı, 2023). Buna karşın, özellikle IoT tabanlı ağların genişlemesi, siber güvenlik açıklarını ve mahremiyet ihlallerini beraberinde getiren temel bir paradoks olarak güncelliğini korumaktadır (Görgül, 2024).

2.2.Veri Güvenliği Kavramı

Akıllı kent ekosistemlerinde teknolojik altyapılar aracılığıyla yürütülen yoğun veri toplama faaliyetleri, kamu hizmetlerinin optimizasyonu açısından kilit bir rol oynasa da bu süreç veri güvenliğini en kritik bileşenlerden biri haline getirmektedir (Özçağdavul & Sayan, 2023). Sistematik veri akışıyla şekillenen bu dijital mimari, doğası gereği siber saldırılar ve yapısal sistem zafiyetleri gibi ciddi riskleri bünyesinde barındırmaktadır (Chen, 2021). Bu noktada veri güvenliği; toplanan bilginin yetkisiz erişim, manipülasyon veya kalıcı imha riskine karşı bütüncül bir yaklaşımla korunmasını temsil etmektedir. Söz konusu güvenliğin tesis edilmesi, teknik ve idari mekanizmaların eş güdümlü bir şekilde kurgulanmasına bağlıdır. Bu bağlamda şifreleme protokolleri, yetkilendirilmiş erişim kontrolü ve güvenli depolama birimleri gibi teknik önlemler savunmanın temel hattını oluştururken; veri koruma otoriteleri de teknolojik dönüşüm sürecinde rehberlik, danışmanlık ve kurumsal iş birliği rolleriyle bu süreci desteklemektedir (Çubukcu, 2024).

Büyük veri, Nesnelerin İnterneti (IoT) ve yapay zeka teknolojilerinin birbiriyle eklemlenmesi, veri mahremiyeti düzleminde geleneksel yaklaşımlarla açıklanamayacak kadar karmaşık ve özgün risk alanları inşa etmektedir. Bu doğrultuda, düzenleyici otoritelerin bilgi teknolojileri ekseninde uzmanlaşmış insan kaynağı ve ihtisas birimleri kurarak kurumsal kapasitelerini tahkim etmeleri elzem hale gelmektedir. Esasen; akademi, girişim ekosistemleri ve kamu sektörü arasında kurulacak stratejik iş birlikleri, hızla evrilen teknolojilerin mahremiyete yönelik tehditlerine karşı proaktif bir savunma mekanizması geliştirilmesi bakımından kritik bir öneme sahiptir (Çubukcu, 2024).

2.3.Kişisel Veri ve Mahremiyet Kavramları

Akıllı kent ekosistemlerinde etik ve hukuki tartışmaların odak noktasını, kişisel veri ve mahremiyet kavramları oluşturmaktadır. Bireyin insan onurunu muhafaza etmedeki kritik rolü nedeniyle kişisel verilerin korunması, temel bir hak olarak özel hayatın gizliliği çatısı altında ele

alınmaktadır (Özçağdavul & Sayan, 2023). Modern şehircilik uygulamalarının gündelik yaşamın her anından veri süzebilme kapasitesi, teknolojik kazanımlar ile bireyse mahremiyetin dokunulmazlığı arasında hassas bir dengenin kurulmasını zorunlu kılmaktadır. Dolayısıyla, veri toplama süreçlerinin meşruiyeti, bu iki uç arasındaki dengenin ne denli korunduğuna bağlıdır.

Türkiye'deki mevcut hukuki zeminde 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), verilerin işlenmesi ve saklanmasına dair temel parametreleri belirlemektedir (KVKK, 2016). Mevzuat; verilerin dürüstlük kuralına uygun, şeffaf, belirli amaçlar doğrultusunda ve rıza esasına dayalı olarak işlenmesini gerektirmektedir. Ancak uygulamada, akıllı kent bileşenlerinin zaman zaman KVKK'nın çizdiği sınırları aşarak geniş kapsamlı veri toplama eğilimi göstermesi, doktrinde ciddi hukuki ihtilafları tetiklemektedir (Özçağdavul & Sayan, 2023).

Özünde mahremiyet, bireyin kendisine ait bilgi akışını denetleyebilme yetisidir. Akıllı kentlerin sunduğu teknolojik konforun bütünüyle veri odaklı sistemlere dayanması, veri güvenliğine dair yapısal endişeleri de beraberinde getirmektedir (Çubukçu, 2024). Dolayısıyla, bu süreçlerin başarısı, teknolojik verimlilik ile temel hakların korunması arasındaki o ince çizginin ne denli titizlikle muhafaza edileceğine bağlıdır. Hukuki düzenlemelerin ve güvenlik protokollerinin etkin tesisi, dijitalleşen kentsel mekânda birey mahremiyetinin sürdürülebilirliği açısından kilit rol oynamaktadır.

2.4. İlgili Araştırmalar

Akıllı şehir ekosisteminde veri koruma ve kişisel mahremiyetin tesisi üzerine yapılan araştırmalar, meselenin teknik boyutunun ötesinde, çok katmanlı ve disiplinler arası bir derinliğe sahip olduğunu kanıtlamaktadır. Özdemir (2025), teknoloji ile hukuk arasındaki etkileşimi odağına aldığı çalışmasında, mevcut mevzuatın dijital dönüşüm hızına yetişmekte zaman zaman güçlük çektiğini savunsa da bu uygulamaların meşruiyeti için gereken temel hukuki zeminin mevcut olduğunu vurgulamaktadır. Bu durum, akıllı şehir yönetişiminde yasal çerçevenin statik bir yapıdan ziyade, teknolojik inovasyonlarla eş zamanlı olarak güncellenen dinamik bir perspektifle ele alınması zorunluluğunu ortaya koymaktadır. Özçağdavul ve Sayan (2023), akıllı kent ekosistemlerinde kişisel verilerin toplama safhasından işleme ve depolama süreçlerine kadar her adımın, veri koruma ilkeleriyle sıkı bir uyum içinde olması gerektiğini vurgulamaktadır. Bilim uzmanları, bu sistemlerdeki veri trafiğinin hukuki normlara uygun yönetilmesini, kullanıcı tarafından sarsılmaz bir güven temeli oluşturmanın koşulu olarak değerlendirmektedir. Bu bakış açısı, teknolojik dönüşümlerin toplumsal düzlemde karşılık bulabilmesi için bireyi merkeze alan ve güvenliği baştan itibaren esas alan bir yaklaşımın zorunluluğuna işaret etmektedir.

Akıllı kent ekosistemlerinde veri toplama ve işleme faaliyetleri, bireysel mahremiyet üzerinde yadsınamaz bir etki alanı oluşturmaktadır. Özçağdavul ve Sayan (2023), bu süreçlerin yönetilmesinde veri koruma ile özel hayatın gizliliği arasında hassas bir dengenin gözetilmesi gerektiğini

savunmaktadır. Yazarlar, bahsedilen dengenin tesisi ve sürekliliği noktasında hukuki düzenlemelerin belirleyici bir işlev üstlendiğini ifade etmektedir. Öte yandan, bu sistemlerin teknolojik altyapısından kaynaklanan siber saldırı riskleri ve muhtemel güvenlik açıkları, veri güvenliğini doğrudan tehdit eden sebepler olarak öne çıkmaktadır (Chen, 2021). Mevcut literatür, akıllı kent uygulamalarının başarısı için etik değerler ile güvenlik protokollerinin bütüncül bakış açısıyla ele alınmasının zorundalığına işaret etmektedir.

Görgül (2024), akıllı kent ekosistemlerinde Nesnelerin İnterneti (IoT) teknolojisinin üstlendiği kritik rolü, Türkiye ve dünya genelindeki örnekler üzerinden karşılaştırmalı bir yaklaşımla analiz etmektedir. Çalışma, IoT'nin salt bir teknik altyapı olmanın ötesinde, veri üretimi ve yönetimi süreçlerini yapılandıran temel yapıtaşı olduğunu vurgulamaktadır. Böylece araştırmanın üzerinde durduğu en hassas mesele, bu teknolojik yayılımın doğurduğu güvenlik açıkları ve mahremiyet ihlali riskleridir. Bu bağlamda, akıllı şehirleşme hamlelerinde teknolojik kapasite artırılırken, veri güvenliğini tesis edecek hukuki ve teknik mekanizmaların sürece eş zamanlı olarak dahil edilmesi stratejik bir zorunluluk teşkil etmektedir. Özetle mevcut literatür, ilgili alanyazın akıllı kentlerin sunduğu teknolojik imkânların yanı sıra veri güvenliği ve mahremiyet hususunda ciddi riskleri barındırdığını kanıtlamaktadır. Dolayısıyla bu uygulamaların sürdürülebilir bir zeminde başarıya ulaşması; teknik inovasyonun hukuki normlar, etik değerler ve toplumsal dinamiklerle eşgüdümlü yürütüldüğü bütüncül bir stratejiyi zorunlu kılmaktadır.

3.YÖNTEM

3.1. Araştırmanın Modeli

Bu çalışma, nitel araştırma yöntemine uygun olarak betimsel ve analitik bir perspektifle kurgulanmıştır. Akıllı kent uygulamalarındaki veri güvenliği ve kişisel verilerin korunması meselelerini çevreleyen hukuki riskleri analiz etmek amacıyla, literatür taraması ve doküman incelemesi yöntemlerine başvurulmuştur. Hukuki normlar ile teknolojik süreçlerin iç içe geçtiği bu karmaşık ekosistemi derinlemesine anlayabilmek için nitel metodolojinin sağladığı esnek yaklaşım benimsenmiştir. Böylelikle, akıllı kent olgusunun disiplinler arası doğası ve verilerin korunmasına ilişkin yasal boyutlar bütüncül bir bakış açısıyla ele alınmaktadır. Araştırmanın temel omurgasını ise güncel mevzuatın, akademik çalışmaların ve uygulama örneklerinin sistematik bir biçimde değerlendirilmesi oluşturmaktadır.

3.2. Evren ve Araştırma Grubu

Araştırmanın evrenini; akıllı kent ekosisteminde kişisel veri güvenliğini ve hukuki standartları konu alan ulusal ve uluslararası akademik literatür, güncel yasal mevzuat, düzenleyici kurumların yayımladığı raporlar ve somut uygulama örnekleri oluşturmaktadır. Bu geniş çerçeve içerisinden,

çalışmanın temel amacıyla doğrudan örtüşen ve belirlenen unsurlara uyum sağlayan veri kaynakları seçilerek kapsam dâhilinde incelenmiştir. Araştırma grubunun oluşturulmasında amaçlı örnekleme yöntemi tercih edilmiştir. Bu bağlamda çalışma; Türkiye'deki akıllı kent projelerini, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) perspektifinden analiz etmeye odaklanmaktadır. İnceleme birimleri seçilirken, uygulamaların veri güvenliği ve mahremiyet standartlarını yansıtma potansiyeli göz önünde bulundurulmuş; böylece farklı hizmet alanlarından temsil gücü yüksek örneklere yer verilmiştir.

Ayrıca, akıllı kent altyapılarının omurgasını oluşturan Nesnelerin İnterneti (IoT) teknolojilerinin rolü ile bu teknolojilerin veri güvenliği düzleminde doğurduğu riskler, araştırmanın kapsamını derinleştiren temel unsurlar arasında ele alınmıştır. Araştırma kapsamında incelenen dokümanlar belirlenirken, akıllı kent uygulamaları ile veri güvenliği ve mahremiyet ilişkisini doğrudan ele alan çalışmalar önceliklendirilmiştir. Bu doğrultuda; Türkiye'de yürütülen akıllı kent projelerine ilişkin raporlar, veri koruma otoritelerinin yayımladığı rehber dokümanlar ve Avrupa Birliği'nin veri koruma çerçevesini ortaya koyan düzenleyici metinler analiz kapsamına dahil edilmiştir. Ayrıca, IoT tabanlı sistemlerin veri işleme süreçlerine etkisini inceleyen uluslararası akademik çalışmalar da araştırma grubuna dahil edilerek, farklı bağlamların karşılaştırmalı olarak değerlendirilmesi sağlanmıştır.

3.3. Veri Toplama Araç ve Teknikleri

Bu araştırmanın temel veri toplama stratejisini doküman incelemesi yöntemi oluşturmaktadır. Çalışma sürecinde birincil veri kaynağı olarak Türkiye Cumhuriyeti Anayasası ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gibi temel yasal düzenlemeler merkeze alınmaktadır. Söz konusu çalışmalar, kişisel verilerin korunmasına yönelik mevcut hukuki zeminin sınırlarını belirlemek amacıyla temel dayanak noktaları olarak kullanılmaktadır. İkincil kaynaklar sürecinde ise akıllı kentler, veri güvenliği ve mahremiyet konularında literatüre giren akademik makale ve kitaplardan yararlanılmıştır. Bu kapsamı genişletmek ve küresel standartları izlemek adına; Birleşmiş Milletler, OECD ve Avrupa Birliği gibi uluslararası mekanizmaların raporları ile veri koruma otoritelerinin yayımladığı güncel belgeler de veri setine dâhil edilmektedir. Toplanan tüm veriler, belirli temalar altında sınıflandırılarak içerik analizine tabi tutulmuş; böylece yasal mevzuat ile pratik uygulamalar arasında mukayeseli bir değerlendirme imkânı doğmaktadır. Doküman incelemesi sayesinde, akıllı şehir ekosistemindeki veri güvenliğinin hem hukuki hem de teknik boyutları disiplinler arası bir derinlikle ele alınabilmektedir.

3.4. Verilerin Toplanma Süreci

Çalışmanın veri toplama aşaması, sistematik literatür taraması ve doküman analizi yöntemlerine dayalı olarak kademeli bir yapıda yürütülmektedir. İlk aşamada; "akıllı kent", "kişisel

veri güvenliği", "KVKK", "GDPR", "veri koruma otoriteleri" ve "IoT teknolojileri" gibi kavramlar temel alınarak ulusal ve uluslararası akademik veri tabanlarında geniş kapsamlı bir tarama yapılmıştır. Bu süreçte, araştırmanın odağıyla doğrudan örtüşen, bilimsel niteliği yüksek ve güncel çalışmalar belirlenerek kapsamlı bir veri havuzu oluşturulmuştur.

İkinci aşamada, Türkiye'deki akıllı kent uygulamalarının yasal zemini mercek altına alınmıştır. Bu doğrultuda, başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) olmak üzere ilgili mevzuat; veri koruma ilkeleri, işleme süreçleri ve hukuki sorumluluklar ekseninde sistematik bir analize tabi tutulmuştur. Sürecin üçüncü halkasını ise veri koruma otoritelerinin pratikleri ile yeni nesil teknolojilerin içerdiği risklere karşı geliştirilen teknik ve idari tedbirlerin incelenmesi oluşturmaktadır. Bu noktada, özellikle akıllı kent ekosisteminin ayrılmaz bir parçası olan IoT tabanlı sistemlerin veri güvenliği üzerindeki somut etkileri irdelenmiştir. Elde edilen tüm dokümanlar, araştırmanın temel hedefleri doğrultusunda tematik ve kronolojik bir tasnife tabi tutulmuştur. Akıllı kentlerin çok disiplinli doğası gereği; hukuk, bilişim teknolojileri ve kamu yönetimi gibi farklı disiplinlere ait kaynaklar incelenmiştir. Toplanan veriler, karşılaştırmalı bir yaklaşımla yorumlanarak bütüncül bir bakış açısıyla sonuçlandırılmıştır.

3.5. Verilerin Analizi

Araştırma kapsamında derlenen veriler, içerik ve tematik analiz yöntemleriyle birlikte çözümlenmiştir. İçerik analizi aşamasında, incelenen dokümanlar sistematik olarak incelenmiştir. Araştırma temelde, Türkiye'de yürürlükte bulunan Kişisel Verilerin Korunması Kanunu (KVKK) ile Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) çerçevesinde mevcut düzenlemeleri analiz etmeye odaklıdır. Fakat konu ile ilgili olan kavramların açıklanabilmesi için; çalışma ile doğrudan ilişkili temel kavramlar, temalar ve bulgular titizlikle ayıklanmıştır. Tematik analiz sürecinde ise akıllı kent uygulamalarından elde edilen veriler, belirli kavramsal çerçeveler altında sınıflandırılarak anlamlandırılmıştır. Veri güvenliği, mahremiyet, hukuki düzenlemeler ve teknolojik riskler gibi ana temalar belirlenmiştir. Bu temalar altında toplanan veriler karşılaştırmalı olarak analiz edilerek, Türkiye'deki mevcut uygulamalar ile uluslararası standartlar arasındaki benzerlikler ve farklılıklar ortaya konulmuştur. Bu sayede, akıllı kent uygulamalarında veri güvenliğine ilişkin çok boyutlu bir değerlendirme yapılması mümkün olmuştur. Konu bütünlüğünü belirtmek amacıyla üç temel boyutta yapılandırılmıştır:

Akıllı kent uygulamalarının içerdiği teknik özellikler,

Kişisel veri güvenliğinin hukuki dayanağı ve mevcut düzenlemeler,

Uygulama sahasında beliren potansiyel riskler.

Bu boyutlar üzerinden şekillenen veriler karşılaştırmalı bir bakış açısıyla ele alınmış; böylece Türkiye'deki mevcut durum ile uluslararası standartlar arasındaki benzerlikler ve farklı noktalar netleştirilmiştir. Değerlendirme kriteri olarak kişisel verilerin korunmasında kritik öneme sahip olan; hukuka uygunluk, veri minimizasyonu ve açık rıza ilkeleri baz alınmıştır. Bu kriterler ışığında, veri işleme süreçleri hem teknik gereklilikler hem de hukuki normlar açısından irdelenmiştir.

4.1. Akıllı Kentlerin Kavramsal Temelleri

Akıllı kentler; bilgi ve iletişim teknolojilerinin kentsel altyapı ile birleştiği, temelde yaşam kalitesini artırmayı ve kaynak yönetimini optimize etmeyi hedefleyen çok katmanlı yapılar olarak tanımlanmaktadır. Bu yaklaşımın odağında, kamu hizmetlerini aktif kılmak amacıyla Nesnelerin İnterneti (IoT), büyük veri ve yapay zekâ gibi dijital unsurların kent ekosistemine entegrasyonu yer almaktadır (Görgül, 2024; Özdemir, 2025). Dolayısıyla akıllı şehir pratikleri, yönetimsel süreçlerde verimliliği odağa alırken toplumsal refahı da üst seviyeye taşımayı amaçlar. Öte yandan bu teknolojik evrim, beraberinde getirdiği dijital izlerle kişisel verilerin korunması, mahremiyetin muhafazası ve veri güvenliği gibi alanlarda kritik hukuki ve etik tartışmaları tetiklemektedir. Bu bağlamda, akıllı kent teknolojilerinin sürdürülebilir bir zemine oturması, bireysel hakların korunması ile toplumsal fayda arasındaki hassas dengenin kurulmasına bağlanmaktadır (Hayta, 2021; Kocabıyık, 2023). Bu bölümde sunulan bulgular, yalnızca literatürde yer alan bilgilerin aktarımından ibaret olmayıp, farklı kaynaklardan elde edilen verilerin tematik analiz yoluyla yorumlanması sonucunda oluşturulmuştur. Bulgular, akıllı kent uygulamalarında veri güvenliği ve mahremiyetin üç temel boyut etrafında şekillendiğini göstermektedir: (i) teknolojik altyapıdan kaynaklanan riskler, (ii) hukuki düzenlemelerin uygulamadaki sınırlılıkları ve (iii) kurumsal kapasite eksiklikleri. Bu çerçevede, mevcut durum yalnızca betimlenmemiş, aynı zamanda söz konusu risk alanları arasındaki ilişkiler analiz edilerek bütüncül bir değerlendirme yapılmıştır

4.2. Akıllı Kentlerde Veri Toplama ve Dijital Gözetim Teknolojileri

Akıllı kent ekosistemleri, kentsel yaşamın her alanına nüfuz eden çok katmanlı ve entegre bir teknolojik altyapı üzerinden veri toplamaktadır. Bu süreçte Nesnelerin İnterneti (IoT) sensörlerinden akıllı cihazlara ve dijital izleme ağlarına kadar uzanan geniş bir donanım yelpazesi, kent dinamiklerine dair kapsamlı verileri kesintisiz bir biçimde sisteme aktarmaktadır (Görgül, 2024; Makhdoom vd., 2019). Bahse konu teknolojilerle elde edilen veri seti; bireylerin anlık konumlarından hareket rotalarına, kamu hizmeti kullanım alışkanlıklarından spesifik kişisel tercihlere kadar uzanan oldukça heterojen bir yapı sunmaktadır. Toplanan bu veriler, akıllı kent paydaşları ve farklı yönetim platformları arasında eş zamanlı olarak işlenip paylaşıma sunulmaktadır (Daoudagh vd., 2021; Özçağdavul ve Sayan, 2023).

Temelde kamu hizmetlerinin optimizasyonunu ve idari verimliliği hedefleyen bu izleme sistemleri, beraberinde kişilerin günlük yaşantısında takip edildiği "dijital gözetim" olgusunu da getirmektedir. Özellikle IoT tabanlı ağlarda verilerin aralıksız kaydedilip analiz edilmesi, kişisel verilerin gizliliği ve bilgi güvenliği noktasında yapısal riskleri barındırmaktadır (Makhdoom vd., 2019; Hayta, 2021). Dolayısıyla, akıllı kentlerdeki veri toplama süreçlerini yalnızca teknik bir operasyon olarak görmek eksik bir yaklaşım olacaktır. Bu süreçlerin hukuki ve etik bir bakış açısıyla; hukuka uygunluk, ölçülülük ve şeffaflık ilkeleri ışığında kurgulanması, temel hak ve özgürlüklerin korunması adına kritik bir gereklilik olduğu görülmektedir (Kocabıyık, 2023; Özdemir, 2025).

4.3. Akıllı Kent Uygulamaları Kapsamında Gizlilik ve Mahremiyet Tehditleri

Literatürdeki güncel çalışmalar, akıllı kent ekosistemlerinin sunduğu teknolojik imkanların yanı sıra gizlilik ve mahremiyet konusunda birçok riskleri de beraberinde getirdiğini ispatlamaktadır. Özellikle Nesnelerin İnterneti (IoT) tabanlı ağların şehir geneline yayılması, devasa boyutlardaki kişisel verinin kesintisiz bir biçimde toplanmasına, analiz edilmesine ve farklı paydaşlarla paylaşılmasına zemin hazırlamaktadır. Bu durum, veri güvenliği ve bireysel mahremiyet üzerinde ciddi bir baskı oluşturmaktadır (Makhdoom vd., 2019; Daoudagh vd., 2021).

Akıllı şehir mimarilerinde sıklıkla tercih edilen merkezi veri yönetim modelleri, "tek hata noktası" (single point of failure) riski taşıdıkları için siber saldırıların odak noktası haline gelebilmektedir. Bu yapısal kırılganlığın ötesinde, kullanıcı verilerinin şeffaf olmayan süreçlerle platformlar arası aktarımı, kişilerin şahsi verileri üstündeki denetimini azaltmaktadır (Makhdoom vd., 2019). Dolayısıyla bu teknolojiler, yalnızca teknik birer sistem değil, aynı zamanda karmaşık toplumsal ve hukuki sorunların kaynağı olarak karşımıza çıkmaktadır.

Dijital gözetim olgusu, şehir sakinlerinin hareketlerinden hizmet kullanım alışkanlıklarına kadar her türlü verinin sürekli kayıt altına alınmasıyla yeni bir boyuta evrilmektedir. Bireylerin rutin davranışlarının bu denli detaylı analiz edilebilmesi, özel hayatın gizliliğine yönelik ihlal riskini doğrudan tetiklemektedir (Daoudagh vd., 2021). Türkiye'deki mevcut durum göz önüne alındığında verilerin işleme sürecindeki şeffaflık düzeyi ile veri toplama faaliyetlerinin hukuki zeminindeki belirsizlikler dikkat çekmektedir. Uygulamaların çoğunlukla geniş kapsamlı veri toplama eğiliminde olması ve açık rıza mekanizmalarının işlevsel bir şekilde yürütülememesi, kişisel verilerin korunması noktasında temel sorunlar teşkil etmektedir (Hayta, 2021; Özçağdavul ve Sayan, 2023). Sonuç itibariyle akıllı kentlerde mahremiyetin tesisi, sadece teknik donanımlarla değil; veri minimizasyonu, amaçla sınırlılık ve açık rıza gibi temel prensipleri esas alan güçlü bir hukuki denetim mekanizmasıyla mümkündür (Kocabıyık, 2023; Özdemir, 2025).

4.4. Veri Koruma Hukuku ve Hukuki Düzenlemeler

4.4.1. Türkiye'de KVKK ve İlgili Mevzuat

Türkiye'de kişisel verilerin korunmasına yönelik hukuki zemin, 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile inşa edilmiştir. Bu kanun, verilerin işlenme süreçlerine dair temel prensipleri ve tarafların yükümlülüklerini belirten esas kaynak durumundadır (KVKK, 2016). Özünde kişilerin temel hak ve özgürlüklerini, özellikle de özel hayatın gizliliğini güvence altına almayı hedefleyen bu düzenleme, dayanağını doğrudan Anayasa'nın ilgili hükümlerinden almaktadır (Türkiye Cumhuriyeti Anayasası, 1982). Bundan hareketle veri koruma, Türkiye'de sadece idari bir prosedür değil, anayasal bir hak olarak konumlandırılmaktadır.

Kanun; hukuka uygunluk, dürüstlük, güncellik, belirli amaçlar doğrultusunda işleme ve veri minimizasyonu gibi kritik ilkeleri veri sorumluları için zorunlu kılmaktadır (KVKK, 2016). Bu ilkeler, özellikle verinin merkezde olduğu akıllı kent projelerinde hayati bir önem taşımaktadır. Zira literatürdeki çalışmalar, akıllı şehir uygulamalarının doğası gereği devasa boyutlarda veri toplama eğiliminde olduğunu ve bu durumun zaman zaman veri koruma sınırlarını zorladığını göstermektedir (Özçağdavul & Sayan, 2023).

Türkiye'deki veri koruma rejimi, sadece KVKK ile sınırlı kalmayan, Anayasa'dan alt yönetmeliklere kadar uzayan çok katmanlı bir yapıya sahip olmaktadır. Bu amaçla hazırlanan 2020–2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı, veri yönetimi ve güvenliği hususunda somut politika amaçlarını belirleyerek sürece stratejik bir boyut kazandırmıştır (T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2019). Kişisel Verilerin Korunması Kurumu (KVKK Kurumu) ise bu ekosistemde denetleyici ve rehberlik edici rolüyle uygulamanın güvenliğini sağlamaktadır (Çubukcu, 2024). Özetle, Türkiye'nin akıllı kent vizyonu güçlü bir hukuki altyapıyla desteklense de teknolojinin hızı karşısında bu rejimin sürekli güncellenen dinamik bir yapıda kalması kaçınılmazdır.

4.4.2. Avrupa Birliği'nde GDPR

Avrupa Birliği bünyesinde yürürlüğe giren 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR), akıllı kent uygulamalarındaki veri işleme süreçlerine dair kapsamlı ve bağlayıcı bir hukuki temel teşkil etmektedir. Tüzük; yapılan işlemlerin hukuka uygunluk, şeffaflık, amaçla sınırlılık, veri minimizasyonu ve hesap verebilirlik prensipleri doğrultusunda yürütülmesini şart koşmaktadır. Böylece açık rıza mekanizması, "unutulma hakkı", veri taşınabilirliği ve ihlallerin bildirilmesi gibi kritik düzenlemelerle kişilerin dijital haklarını güvence altına almaktadır (Avrupa Parlamentosu ve Konseyi, 2016).

Önceki 95/46/EC sayılı Direktife kıyasla çok daha geniş bir etki alanına sahip olan GDPR, otomatik ve manuel olarak yürütülen veri işleme çalışmalarını gözlem altına almakta ve veri sorumlularına "Veri Koruma Görevlisi" (DPO) atama yükümlülüğü getirmektedir. Tüzüğün belirlediği

bu katı ilkeler, veri sorumlularının süreçlerini sıkı bir özdenetim ve dış denetim sarmalında yönetmesini zorunlu kılmaktadır. Akıllı kentlerin temelini oluşturan IoT tabanlı platformlar açısından bakıldığında ise devasa veri yoğunluğu ve kesintisiz akış, bu hukuki prensiplerin sahadaki uygulamasını karmaşık hale getirmektedir. Verilerin farklı ekosistemler içinde kontrolsüz paylaşımı ve kullanıcı davranışlarının sürekli izlenmesi, mahremiyet ihlali riskini kayda değer ölçüde artırmaktadır (Daoudagh vd., 2021; Makhdoom vd., 2019). Sonuç olarak GDPR, yalnızca teknik bir güvenlik protokolü değil, bireyi merkeze alan bir hak arama mekanizmasıdır. Bu niteliğiyle, akıllı kent projelerinde verinin sınırlandırılması ve denetlenmesi noktasında vazgeçilmez bir referans kaynağı olmaktadır (Avrupa Parlamentosu ve Konseyi, 2016).

4.4.3. Uluslararası Standartlar ve Karşılaştırmalı Analiz

Kişisel verilerin korunmasına yönelik uluslararası standartlar, ulusal düzeydeki yasal rejimlerin temel mimarisini belirleyen en önemli unsurlardır. Bundan hareketle, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ile Türkiye'deki 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), veri hukuku disiplininin temel sütunlarını oluştururken; aynı zamanda karşılaştırmalı analizler için kapsamlı zemin oluşturmaktadır. Normatif bir bakış açısıyla incelendiğinde, KVKK ve GDPR'ın birbirine çok benzer özellikler taşıdığı söylenebilmektedir. Her iki düzenleme de verinin işlenme sürecinde hukuka ve dürüstlük kurallarına uygunluk, belirli amaçlar çerçevesinde hareket etme, veri minimizasyonu ve güvenlik gibi köklü ilkeleri merkeze almaktadır. Bu ortak yaklaşımın temel gayesi, bireylerin kendi verileri üzerindeki kontrol mekanizmalarını güçlendirmektir (KVKK, 2016; Avrupa Parlamentosu ve Konseyi, 2016). Buna karşın GDPR, KVKK ile kıyaslandığında çok daha ayrıntılı ve katı bir sistematik yapıya sahiptir. Özellikle veri sorumlularının yükümlülüklerinin net sınırlarla çizilmesi, yüksek idari para cezalarına dayalı ağır yaptırım rejimi ve "veri koruma etki değerlendirmesi" gibi proaktif mekanizmalar, GDPR'ı daha ileri bir koruma rejimi olarak konumlandırmaktadır (Avrupa Parlamentosu ve Konseyi, 2016).

Akıllı kent ekosistemleri özelinde ise her iki mevzuat; şeffaflık, hesap verebilirlik ve verinin işlenme sınırlarının tayini noktasında kritik bir rehber olmaktadır. Ancak akıllı kentlerdeki durmaksızın veri akışı, IoT tabanlı sistemlerin karmaşıklığı ve çok paydaşlı yapılar, bu hukuki normların pratikte uygulanmasını zorlaştırarak birçok riskleri tetiklemektedir (Daoudagh vd., 2021; Makhdoom vd., 2019). Bu literatürlere göre, KVKK ile GDPR arasında temel prensipler düzeyinde yapısal bir uyum bulunsa da GDPR'ın sunduğu detaylı düzenleme seti ve güçlü denetim araçları dikkat çekmektedir. Bu durum, Türkiye'deki veri koruma prosedürünün geliştirilmesi ve özellikle akıllı kentlerdeki veri güvenliği açıklarının en aza indirgenmesi hususunda, GDPR'ın öncelikli bir referans modeli olarak kabul edilmesini gerekli kılmaktadır.

4.5. Genel Değerlendirme

Akıllı kent ekosistemlerinin genişlemesi, verimlilik artışı sağlarken kişisel verilerin korunması ve siber güvenlik meselelerini de yönetim süreçlerinin merkezine taşımaktadır. Literatürdeki bulgular, bu kentlerde toplanan devasa veri kütlelerinin sunduğu olanakların yanı sıra, mahremiyet ihlalleri noktasında ciddi riskler barındırdığını teyit etmektedir. Dolayısıyla güvenli bir akıllı kent yapısının tesisi; hukuki zemin, teknik altyapı ve kurumsal yetkinliğin eş güdümlü bir şekilde kurgulanmasına bağlanmaktadır (Özdemir, 2025; Özçağdavul & Sayan, 2023).

Hukuki perspektiften bakıldığında, Türkiye'deki 6698 sayılı KVKK ve Avrupa Birliği müebbetindeki GDPR, veri koruma rejiminin temel sac ayaklarını oluşturmaktadır. Bu düzenlemeler; verinin işlenmesinde hukuka uygunluk, amaçla sınırlılık ve veri minimizasyonu gibi evrensel ilkeleri zorunlu kılmaktadır (KVKK, 2016; Avrupa Parlamentosu ve Konseyi, 2016). Ancak teknolojik dönüşümün hızı, mevcut yasal çerçevede zaman zaman boşluklar yaratmakta; bu durum ise pratik uygulamaların her zaman kağıt üzerindeki ilkelerle örtüşmemesine yol açmaktadır (Özçağdavul & Sayan, 2023). Teknik düzlemde, özellikle Nesnelerin İnterneti (IoT) cihazlarının yaygınlığı, veri güvenliği açısından kırılgan alanlar yaratmaktadır (Görgül, 2024). Bu riskleri bertaraf etmek adına şifreleme yöntemleri, katı erişim kontrolleri ve güvenli depolama çözümleri hayati önem taşımaktadır. Güncel araştırmalar, güvenli veri paylaşımı için geliştirilen yeni nesil mimarilerin, veri koruma ilkelerinin operasyonel hale getirilmesinde kritik rol oynadığını göstermektedir (Makhdoom vd., 2019; Daoudagh vd., 2021).

Kurumsal boyutta ise en temel engel, veri koruma otoritelerinin dijital hıza uyum sağlayabilecek teknik donanım ve uzman personel eksikliğinden kaynaklanmaktadır. Mevcut kapasite yetersizliklerinin aşılması için akademi, kamu ve teknoloji geliştiriciler arasında güçlü iş birliği ağları kurulmalıdır (Çubukcu, 2024). Böylece, akıllı kentlerin sürdürülebilirliği sadece teknolojik mükemmellikle değil, şeffaflık ve farkındalık yoluyla toplumda inşa edilecek "güven" duygusuyla mümkün olacaktır (Özçağdavul & Sayan, 2023). Elde edilen bulgular, akıllı kent uygulamalarında veri güvenliğinin yalnızca teknik çözümlerle sağlanamayacağını, aynı zamanda güçlü bir hukuki çerçeve ve etkin kurumsal yapı gerektirdiğini ortaya koymaktadır. Bu durum, literatürde sıklıkla vurgulanan teknoloji odaklı yaklaşımların yetersizliğini teyit etmekte ve daha bütüncül bir yönetişim modeline ihtiyaç olduğunu göstermektedir. Bu bağlamda çalışma, veri koruma rejimlerinin yalnızca normatif düzenlemeler olarak değil, uygulama kapasitesi ile birlikte değerlendirilmesi gerektiğini ortaya koyarak literatüre katkı sunmaktadır.

Bu çalışma bazı sınırlılıklar içermektedir. Öncelikle araştırma, nitel yöntem kapsamında doküman incelemesine dayandığı için ampirik veri içermemektedir. Bu durum, elde edilen bulguların uygulamadaki yansımalarının doğrudan gözlemlenmesini sınırlandırmaktadır. Ayrıca çalışma, Türkiye

ve Avrupa Birliği veri koruma çerçevesi ile sınırlı tutulmuş olup, farklı ülke örneklerine geniş ölçüde yer verilmemiştir. Gelecek çalışmaların, saha araştırmaları ve nicel veri analizleri ile bu bulguları desteklemesi, literatüre daha güçlü katkılar sağlayacaktır.

5.SONUÇ VE ÖNERİLER

Bu akıllı kent ekosistemlerinde kişisel veri güvenliği ve mahremiyetin çok katmanlı bir problem odağı olduğunu göstermiştir. Elde edilen bulgular doğrultusunda; kentsel alanlarda üretilen yoğun veri akışının sunduğu teknolojik imkânların, beraberinde ciddi güvenlik açıklarını ve mahremiyet ihlallerini getirdiği söylenebilir. Bu noktada veri koruma olgusu, salt teknik bir güvenlik katmanından ziyade; hukuki, kurumsal ve toplumsal dinamiklerin iç içe geçtiği bütüncül bir yapı olarak değerlendirilmelidir. Araştırma sürecinde incelenen yasal zemin, Türkiye'deki 6698 sayılı KVKK ile Avrupa Birliği'nin GDPR düzenlemesinin bu alandaki temel referans noktaları olduğunu teyit etmektedir. Her iki metin de verinin işlenmesinde; hukuka uygunluk, amaçla sınırlılık ve veri minimizasyonu gibi evrensel prensipler üzerinden birey haklarını güvence altına almayı hedeflemektedir (KVKK, 2016; Avrupa Parlamentosu ve Konseyi, 2016). Ancak teknolojik dönüşümün hızı, uygulamada uyum sorunlarını ortaya çıkarmakta, özellikle karmaşık akıllı kent sistemlerinde veri işleme süreçlerinin bu hukuki ilkelerle her zaman örtüşmediği müşahede edilmektedir.

Teknik boyutta, şifreleme ve erişim kontrolü gibi yöntemler güvenliği tahkim etse de Nesnelerin İnterneti (IoT) tabanlı ağların genişlemesi, kontrol edilmesi güç yeni zafiyet alanları meydana getirmektedir. Kurumsal açıdan bakıldığında, denetleyici otoritelerin uzman personel ve teknik kapasite yetersiziği nedeniyle denetim mekanizmalarını işletmekte zorlandığı görülmektedir. Toplumsal düzlemde ise kişilerin dijital farkındalık hakkında bilgi eksikliği ve sistemlerdeki şeffaflık az olması, akıllı kent uygulamalarına yönelik bir koruma kalkanı oluşturmaktır.

Sonuç olarak, akıllı kentlerde veri güvenliğinin tesisi; hukuki altyapı, teknik donanım, kurumsal yetkinlik ve toplumsal bilincin uyumlu bir şekilde yönetilmesine bağlıdır. Bu bileşenler arasında bütüncül bir koordinasyon olmadığı sürece, akıllı kent projelerinin sürdürülebilir bir toplumsal kabulle hayata geçirilmesi güç görünmektedir.

Araştırma bulgularından hareketle, akıllı kent ekosistemlerinde veri güvenliğini tahkim etmek ve kişisel verilerin korunmasına yönelik dirençli bir mekanizma inşa etmek amacıyla şu stratejik öneriler geliştirilmiştir:

Yasal ve Düzenleyici Reformlar: Veri koruma mevzuatının, teknolojik inovasyonun dinamizmine ayak uydurabilecek esnek ve güncel bir yapıya kavuşturulması kritiktir. Uygulamada

karşılaşılan muğlak alanların netleştirilmesi, hukuki belirliliği artıracaktır. Bu noktada veri koruma otoritelerinin denetim ve yaptırım kapasitesinin güçlendirilmesi, sadece ihlallere karşı bir savunma hattı oluşturmakla kalmayacak; aynı zamanda proaktif ve güven esaslı bir veri yönetişim rejiminin tesisine imkan tanıyacaktır.

Teknik Altyapı ve Standardizasyon: Akıllı şehir bileşenlerinde uçtan uca şifreleme yöntemlerinin standart hale getirilmesi ve veri transfer süreçlerinin yüksek güvenlikli prosedürlerle yönetilmesi öncelikli bir durum olmaktadır. Özellikle IoT (Nesnelerin İnterneti) ekosistemine yönelik bağlayıcı güvenlik standartlarının ihdası, altyapısal zafiyetlerin minimize edilmesi ve mahremiyetin teknik katmanda güvence altına alınmasında belirleyici olacaktır.

Kurumsal Kapasite ve Stratejik Ortaklıklar: Kamu kurumlarında veri güvenliği ve hukuku alanında uzmanlaşmış nitelikli iş gücü kapasitesinin artırılması elzemdir. Kurumsal farkındalık çalışmalarının ötesine geçilerek; akademi, kamu ve özel sektör paydaşları arasında kurulacak dinamik ortaklıklar, yeni nesil siber risklere karşı daha çevik ve önleyici çözüm modellerinin geliştirilmesine zemin hazırlayacaktır.

Toplumsal Bilinç ve Şeffaflık Modeli: Dijital dönüşümün öznesi olan kişilerin, kişisel veri hakları konusundaki farkındalığının artırılması ve veri işleme süreçlerinin izlenebilir, şeffaf bir yapıya büründürülmesi sürecin başarısını belirleyecektir. Vatandaşların sürece aktif katılımını teşvik eden projeler, akıllı kent uygulamalarına duyulan toplumsal güveni pekiştirecek temel unsurdur.

Önerilen bu stratejilerin eş güdümlü olarak uygulanması; akıllı şehir projelerinin yalnızca teknolojik bir başarı hikayesi olarak kalmamasını, aynı zamanda hukuki, toplumsal ve etik düzlemde sürdürülebilir ve meşru bir zeminde gelişimini sağlayacaktır.

AUTHORS' STATEMENT /YAZARLARIN BEYANI

Contribution Statement/Katkı Oranı Beyanı: The authors contributed equally to the work. / Yazarlar çalışmaya eşit oranda katkı sağlamıştır.

Support and Acknowledgments Statement/Destek ve Teşekkür Beyanı: No support was received from any institution or organization for this study. / Çalışmada herhangi bir kurum ya da kuruluştan destek alınmamıştır.

Conflict of Interest Statement/Çatışma Beyanı: There is no potential conflict of interest in this study./ Çalışmada herhangi bir potansiyel çıkar çatışması söz konusu değildir.

KAYNAKÇA

Avrupa Parlamentosu ve Avrupa Birliği Konseyi. (2016). Gerçek Kişilerin Kişisel Verilerinin İşlenmesi ve Bu Verilerin Serbest Dolaşımı İle İlgili Olarak Korunmasına İlişkin (AB) 2016/679 Sayılı Tüzük (Genel Veri Koruma Tüzüğü – GDPR). Avrupa Birliği Resmî Gazetesi, L119/1.

Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). A Smart City Iot Platform Respecting GDPR Privacy And Security Aspects. IEEE Access, 8, 23601–23623.

Chen, M. (2021). Smart City And Cyber Security: Technologies Used, Main Challenges And Future Recommendations. Energy Reports, 7, 7999–8012. Https://Doi.Org/10.1016/J.Egyr.2021.08.124

Çubukçu, Z. (2024). Dijital Çağda Kişisel Verilerin Korunmasında Veri Koruma Otoritelerinin Rolü. Toplum,Ekonomi ve Yönetim Dergisi, 5(3), 454–468. Https://Doi.Org/10.58702/Teyd.1485163

Daoudagh, S., Marchetti, E., Savarino, V., Bernabé, J. B., García-Rodríguez, J., Torres Moreno, R., & Skarmeta, A. F. (2021). Smart Cities Data Protection By Design: GDPR-Based Access Control. Sensors, 21, 7154. Https://Doi.Org/10.3390/S21217154

Görgül, Ş. G. (2024). Akıllı Şehir Teknolojilerinde Nesnelerin İnterneti (Iot) Teknolojisinin Önemi: Dünya Ve Türkiye Karşılaştırılması (Dönem Projesi). İzmir Kâtip Çelebi Üniversitesi.

Hayta, Y. (2021). Akıllı Kent Uygulamalarında Kişisel Verilerin Gizliliği ve Güvenliği. Fırat Üniversitesi Sosyal Bilimler Dergisi, 31(2), 929–941. Https://Doi.Org/10.18069/Firatsbed.897321

Kocabıyık, O. (2023). Kamu Hizmeti Yönüyle Akıllı Şehirlerde Kişisel Verilerin Korunması Hakkı (Yüksek Lisans Tezi). İstanbul Kültür Üniversitesi.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2019). Privysharing: A Blockchain-Based Framework For Privacy-Preserving And Secure Data Sharing İn Smart Cities. Computers & Security. Https://Doi.Org/10.1016/J.Cose.2019.101653

Özçağdavul, M., & Sayan, H. H. (2023). Akıllı Şehirler ve Kişisel Verileri Koruma Kanunu Uyumu. TYB Akademi Dil Edebiyat & Sosyal Bilimler Dergisi, (37).

Özdemir, S. (2025). Akıllı Şehirler ve Yasal Mevzuat. Thinking Of Urban Decoding Journal, 2(1), 13–42. https://Doi.Org/10.69992/0.2025.9

T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı. (2019). 2020–2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı.

Türkiye Cumhuriyeti Resmî Gazete (2016). 6698 Sayılı Kişisel Verilerin Korunması Kanunu (7 Nisan 2016, Sayı: 29677).

Türkiye Cumhuriyeti Anayasası. (1982). Resmî Gazete (9 Kasım 1982, Sayı: 17863).

Ünsal, Ö., & Avcı, S. (2023). Akıllı Şehir Tartışmaları Üzerine Bir Değerlendirme ve Türkiye. Mavi Atlas, 11(1), 87-104. https://doi.org/10.18795/gumusmaviatlas.1229850