T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ENDÜSTRİYEL SÜRDÜRÜLEBİLİRLİK ANABİLİM DALI

AKILLI ŞEHİRLERDE GÖZETİM SİSTEMLERİNİN UYGULANABİLİRLİĞİ: RİSK VE TEHDİT EKSENLİ BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

SAMET YÜKSEL

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ ÖZGÜR SAYIN

BİLECİK, 2025

10751782

T.C.

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ENDÜSTRİYEL SÜRDÜRÜLEBİLİRLİK ANABİLİM DALI

AKILLI ŞEHİRLERDE GÖZETİM SİSTEMLERİNİN UYGULANABİLİRLİĞİ: RİSK VE TEHDİT EKSENLİ BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

SAMET YÜKSEL

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ ÖZGÜR SAYIN

BİLECİK, 2025

10751782

BEYAN

"**Akıllı şehirlerde gözetim sistemlerinin uygulanabilirliği: Risk ve tehdit eksenli bir değerlendirme**" adlı yüksek lisans dönem projesinin hazırlık ve yazımı sırasında bilimsel araştırma ve etik kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmının Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunulmadığını, aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

<table>
<tr><td colspan="4">Bu çalışmanın,
Bilimsel Araştırma Projeleri (BAP), TÜBİTAK veya benzeri kuruluşlarca desteklenmesi durumunda; projenin ve destekleyen kurumun adı proje numarası ile birlikte, ETİK KURUL onayı alınması durumunda ise ETİK KURUL tarih karar ve sayı bilgilerinin beyan edilmesi gerekmektedir.</td></tr>
<tr><td>DESTEK ALINMIŞTIR</td><td></td><td>DESTEK ALINMAMIŞTIR</td><td></td></tr>
<tr><td colspan="4">Destek alındı ise;</td></tr>
<tr><td colspan="4">Destekleyen kurum;</td></tr>
<tr><td colspan="2">Desteğin Türü</td><td colspan="2">Proje Numarası</td></tr>
<tr><td colspan="2">1- BAP (Bilimsel Araştırma Projesi)</td><td colspan="2" rowspan="3"></td></tr>
<tr><td colspan="2">2- TÜBİTAK</td></tr>
<tr><td colspan="2">Diğer;……</td></tr>
<tr><td colspan="4">ETİK KURUL onayı var ise;</td></tr>
<tr><td colspan="2">ETİK KURUL karar tarih/sayı:</td><td colspan="2">……/……</td></tr>
</table>

Öğrenci Adı ve Soyadı

Samet YÜKSEL

Tarih

../../2025

İmza

ÖN SÖZ

Bu çalışmada, akıllı şehir teknolojilerinde bulunması gereken akıllı güvenlik sistemleri incelenmiştir. Bu çalışma ile geleceğin mimarisi olan akıllı şehirlerde bulunma ihtimali olan siber güvenlik açıklıkları, çeşitli saldırı senaryoları ile birlikte incelenecek, akıllı şehir teknolojilerinde siber güvenliğin sağlanabilmesi için bir yol haritası önerisi verilecektir.

Araştırma konusu belirleme ve tamamlama aşamasında pek çok kıymetli insanların fikirleri, yardımları ve destekleri alınmıştır. Bu süreç içerisinde çalışmamı sahiplenerek tecrübelerinden ve fikirlerinden yararlandığım, çalışmalarıma değerli katkılar sunan danışmanlarım Sayın Dr. Öğr. Üyesi Özgür SAYIN ve Sayın Doç. Dr. Yunus DÜGER'e sonsuz teşekkürlerimi sunarım.

Son olarak bu günlere ulaşmamdaki emekleri adına değerli aileme teşekkür ederim.

Samet YÜKSEL

2025

ÖZET

AKILLI ŞEHİRLERDE GÖZETİM SİSTEMLERİNİN UYGULANABİLİRLİĞİ: RİSK VE TEHDİT EKSENLİ BİR DEĞERLENDİRME

Yerleşik hayata geçişle birlikte kentler, insan yaşamının temel odak noktası haline gelmiş; hızlı nüfus artışı ve demografik değişimlerle birlikte göç, plansız kentleşme ve altyapı yetersizlikleri önemli sorunlar olarak ortaya çıkmıştır. Ulaşım, eğitim, sağlık, güvenlik, enerji, su ve atık yönetimi gibi temel hizmet alanlarında artan ihtiyaçlar, mevcut kaynakların etkin ve verimli biçimde kullanılmasını zorunlu kılmaktadır. Bu durum, kent yönetiminde yenilikçi çözümlere duyulan ihtiyacı her geçen gün daha da artırmaktadır.

Bilgi ve iletişim teknolojilerinin gelişimi, şehirlerin kaynaklarını daha verimli kullanabilmesi ve kent sakinlerine daha kaliteli hizmetler sunabilmesi açısından kritik bir fırsat sunmuştur. Bu doğrultuda, kentsel yaşamı kolaylaştıran ve yaşam kalitesini artıran teknoloji merkezli çözümler, "akıllı şehir" kavramının ortaya çıkmasına zemin hazırlamıştır.

Akıllı şehir, yalnızca teknolojik bir dönüşümü değil; aynı zamanda kentlerin yönetiminde etkinlik, sürdürülebilirlik ve güvenliği esas alan bütüncül bir yaklaşımı ifade etmektedir. Dinamik kent yaşamının ortaya çıkardığı sorunlara hızlı, esnek ve yenilikçi çözümler üreten akıllı şehir anlayışı, sınırlı kaynakların en verimli şekilde kullanılmasını hedeflerken aynı zamanda vatandaşların yaşam kalitesini yükseltmeyi amaçlamaktadır. Bu yönüyle akıllı şehirler, modern kentleşme sürecinde karşılaşılan sorunların üstesinden gelmek için stratejik bir model olarak öne çıkmaktadır.

Anahtar kelimeler: Akıllı Şehir**,** Akıllı Güvenlik**,** Akıllı Planlama, Sürdürülebilirlik, İletişim.

ABSTRACT

APPLICABILITY OF SURVEILLANCE SYSTEMS IN SMART CITIES: A RISK AND THREAT-BASED ASSESSMENT

With the transition to a settled lifestyle, cities have become the central focus of human life; however, rapid population growth and demographic changes, coupled with migration, unplanned urbanization, and infrastructural deficiencies, have emerged as major challenges. Increasing demands in essential service areas such as transportation, education, healthcare, security, energy, water, and waste management necessitate the efficient and effective utilization of existing resources. This situation further intensifies the need for innovative solutions in urban governance.

The advancement of information and communication technologies has created a critical opportunity for cities to use their resources more efficiently and to provide higher-quality services to their residents. Accordingly, technology-driven solutions that facilitate urban life and enhance the quality of living have laid the groundwork for the emergence of the concept of the "smart city."

A smart city represents not only a technological transformation but also a holistic approach that prioritizes efficiency, sustainability, and security in urban management. By producing rapid, flexible, and innovative responses to the challenges posed by dynamic urban life, the smart city paradigm seeks to maximize the use of limited resources while simultaneously improving citizens' quality of life. In this respect, smart cities stand out as a strategic model for addressing the challenges of contemporary urbanization.

Keywords: Smart City, Smart Security, Smart Planning, Sustainability, Communication.

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

KISALTMALAR VE SİMGELER LİSTESİ

3D: 3 Boyutlu

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

a-Devlet: Akıllı Devlet

AFAD: Afet ve Acil Durum Yönetimi Başkanlığı

Ar-Ge: Araştırma ve Geliştirme

ASEAN: Association of Southeast Asian Nations (Güneydoğu Asya Ülkeleri Birliği)

BİLGEM: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BİMER: Başbakanlık İletişim Merkezi

BM: Birleşmiş Milletler

BTYK: Bilim ve Teknoloji Yüksek Kurulu

BUMEP: Bursa Mobil Eğitim Projesi

BUSKİ: Bursa Su ve Kanalizasyon İdaresi

CBS: Coğrafi Bilgi Sistemi

CİMER: Cumhurbaşkanlığı İletişim Merkezi

CNU: Congress for the New Urbanism (Yeni Şehircilik Kongresi)

CORDIS: Community Research and Development Information Service (Toplum Araştırma ve Geliştirme Bilgi Servisi)

ÇP: Çerçeve Programı

DBYS: Devlet Belge Yönetim Sistemi

DETSİS: Devlet Teşkilatı Merkezi Kayıt Sistemi

e-Devlet: Elektronik Devlet

EIP-SCC: The European Innovation Partnership on Smart Cities and Communities (Akıllı Kentler ve Topluluklar Yenilikçilik Ortaklığı)

ENoLL: The European Network of Living Labs (Avrupa Yaşayan Laboratuvarlar Ağı)

eGov 2015: e-Government 2015 (e-Devlet 2015)

FIFA: Fédération Internationale de Football Association (Uluslararası Futbol Federasyonları Birliği)

GPS: The Global Positioning System (Küresel Konumlandırma Sistemi)

GSYİH: Gayrisafi Yurt İçi Hasıla

H2020: Horizon 2020 (Ufuk 2020)

HSYS: Hizmet Standartları Yönetim Sistemi

IBM: International Business Machines (Uluslararası İş Makineleri)

ICPC: International Cooperation Partnership Countries (Uluslararası İşbirliği Hedef Ülkeleri)

IoT: Internet of Things (Nesnelerin İnterneti)

ITS: Intelligent Transportation Systems (Akıllı Ulaşım Sistemleri)

İLBANK: İller Bankası A.Ş.

iN2015: Intelligent Nation 2015 (Akıllı Ulus 2015)

İRODES: İlan Reklam Online Denetleme Sistemi

İSBAK: İstanbul Bilişim ve Akıllı Kent Teknolojileri A.Ş.

İSTKA: İstanbul Kalkınma Ajansı

İSTTELKOM: İstanbul Elektronik Haberleşme ve Altyapı Hizmetleri San. ve Tic. A.Ş.

KAYSİS: Elektronik Kamu Bilgi Yönetim Sistemi

KENTGES: Kentsel Gelişme Stratejisi

KMA: Kamu Memnuniyet Anketi

KMS: Kamu Mevzuat Sistemi

KSYS: Kamu Stratejik Yönetim Sistemi

MIT: Massachusetts Institute of Technology (Massachusetts Teknoloji Enstitüsü)

NICT: National Institute of Information and Communications Technology (Japonya Ulusal Bilgi ve Haberleşme Teknolojileri Enstitüsü)

NYC: City of New York (New York Kenti)

OECD: The Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)

PERSİS: Performans Takip Sistemi

PISA: Programme for International Student Assessment (Uluslararası Öğrenci Değerlendirme Programı)

RG: Resmi Gazete

SCADA: Supervisory Control and Data Acquisition (Merkezi Denetleme Kontrol ve Veri Toplama)

SDPS: Standart Dosya Planı Sistemi

SWOT: Strengths Weaknesses Opportunities Threats (Üstünlükler, Zayıflıklar, Fırsatlar, Tehditler)

TBV: Türkiye Bilişim Vakfı

T.C.: Türkiye Cumhuriyeti

TDK: Türk Dil Kurumu

TEK: Türkiye Ekonomi Kurumu

TOKİ: Toplu Konut İdaresi Başkanlığı

TSE: Türk Standardları Enstitüsü

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜRKSAT: Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş.

UNCHS: United Nations Human Settlements Programme (Birleşmiş Milletler İnsan Yerleşimleri Merkezi)

UNDP: United Nations Development Programme (Birleşmiş Milletler Kalkınma Programı)

UN-Habitat: United Nations Human Settlements Programme (BM İnsan Yerleşimleri Programı)

WHO: World Health Organization (Dünya Sağlık Örgütü)

1. GİRİŞ

21. Yüzyılın başından itibaren dünya nüfusunun olağanüstü bir hızla artması ve bu artışın büyük bir bölümünün şehirlerde yoğunlaşması, kentleşme olgusunu tarihte eşi görülmemiş bir boyuta taşımıştır. Birleşmiş Milletler verilerine göre, 2030 yılında dünya nüfusunun yaklaşık %60'ından fazlasının kentsel alanlarda yaşayacağı öngörülmektedir. Bu dönüşüm, şehirleri ekonomik büyüme, toplumsal gelişim ve kültürel etkileşim açısından cazibe merkezleri haline getirirken; altyapı eksiklikleri, çevresel baskılar, trafik sıkışıklığı, sosyal eşitsizlikler ve güvenlik tehditleri gibi çok boyutlu sorunları da beraberinde getirmektedir (Komninos, 2008; Cohen, 2018). Bugünün şehirleri, yalnızca mekânsal planlama değil; aynı zamanda teknoloji, veri yönetimi, kamu politikası ve toplumsal katılım ekseninde yeniden tanımlanan karmaşık sosyo-teknik sistemlerdir.

Akıllı şehir kavramı, bu bağlamda, bilgi ve iletişim teknolojilerinin (BİT) şehir yönetimi süreçlerine bütünleşik biçimde uygulanması ile kentlerin daha verimli, sürdürülebilir, yaşanabilir ve güvenli hale getirilmesini hedefler (Albino vd., 2015; Dameri, 2013). Avrupa Komisyonu'nun yaklaşımına göre akıllı şehirler; ekonomik kalkınma, çevresel sürdürülebilirlik ve yaşam kalitesinin artırılması amacıyla insan odaklı, sosyal sermayeyi güçlendiren ve fiziksel altyapıyı optimize eden stratejilere dayanır. Uluslararası Standartlar Enstitüsü ise kavramı, bulut bilişim, Nesnelerin İnterneti (IoT), büyük veri ve coğrafi bilgi sistemleri gibi teknolojilerin entegre biçimde kullanıldığı kentsel model olarak tanımlar (Akıllı Şehirler Beyaz Bülteni, 2017). Bu kapsamda akıllı şehirler yalnızca kaynak verimliliğini ve hizmet kalitesini yükselten teknolojik platformlar değil; aynı zamanda karmaşık güvenlik sorunlarını çözüme kavuşturmayı amaçlayan, çok katmanlı güvenlik ekosistemleri olarak ele alınmaktadır. Özellikle akıllı güvenlik kavramı, hem bireylerin hem de kentin bütünsel güvenliğini sağlamak üzere sensörlerden yapay zekâ algoritmalarına uzanan geniş bir teknoloji yelpazesini içerir (Arslan, 2014; Şengül ve Altıntaş, 2020). Bu sistemler, suç önleme, afet yönetimi, kritik altyapıların korunması ve kamusal alanların gözetimi gibi çok sayıda işlevi yerine getirerek şehirlerin dayanıklılığını artırır.

Bu tezin temel motivasyonu, hızla dijitalleşen ve birbirine bağlanan kentsel sistemlerin güvenlik perspektifi açısından nasıl yeniden tasarlandığını anlamak ve değerlendirmektir. Günümüzde veri toplama, işleme ve depolama teknolojilerinin yaygınlaşması; şehir güvenliğini güçlendirme potansiyeli taşırken aynı zamanda ciddi mahremiyet ihlali, veri güvenliği açığı ve siber saldırı riski yaratmaktadır (Yıldız ve Baz, 2021). Bu durum, akıllı şehirlerin teknik, yönetsel ve etik boyutlarının birlikte değerlendirilmesini zorunlu kılmaktadır. Çalışmanın

seçilme nedeni, Türkiye'de bu konunun henüz sistematik ve bütüncül bir şekilde araştırılmamış olmasıdır. İstanbul, Ankara, Bursa, Kayseri gibi kentlerde kısmen hayata geçirilen akıllı şehir uygulamaları mevcuttur; ancak bunların güvenlik bileşenleri çoğunlukla proje veya sektör bazlı ele alınmakta, uzun vadeli stratejik yaklaşımlar yeterince kurumsallaşmamaktadır. Ayrıca, kentsel dönüşüm süreçlerinin akıllı şehir teknolojileriyle birleşmesinin güvenlik alanındaki etkileri, literatürde eksik şekilde incelenmiştir. Türkiye'de kentsel dönüşüm öncelikle afet riskinin azaltılması ve fiziksel yapı stokunun yenilenmesi bağlamında ele alınırken, bu dönüşümün akıllı sensörler, veri analitiği, güvenlik otomasyonu gibi dijital çözümlerle bütünleştirilmesi hem afet hazırlığını hem günlük yaşam güvenliğini güçlendirecek potansiyel taşımaktadır (Aslan ve Bulut, 2019).

Literatürde akıllı şehir üzerine yapılan çalışmalar kavramsal çeşitlilik açısından zengin olmakla birlikte, güvenlik meselesi genellikle ya yalnızca siber güvenlik odaklı ya da yalnızca fiziksel güvenlik odaklı ele alınmaktadır (Gaffney ve Robertson, 2018; Mantelero ve Esposito, 2021). Oysa gerçek dünyada bu iki boyut iç içe geçmiştir ve kent güvenliğinin etkin sağlanması, her iki alanın birlikte değerlendirildiği modellerin geliştirilmesini gerektirir. Veri analitiği ve yapay zekâ tabanlı güvenlik sistemlerinin yarattığı fayda-risk dengesi, özellikle mahremiyet ve özgürlükler üzerindeki etkiler bakımından henüz yeterince incelenmemiştir. Kitchin (2016) ve Reuter (2020), bu tür sistemlerde karar mekanizmalarının şeffaf olmaması, algoritmik önyargılar ve hukuki hesap verebilirlik sorunlarına dikkat çekmiştir. Türkiye bağlamında ise akademik yayınlar ve uygulama raporları daha çok teknoloji tanıtımı veya sınırlı ölçekli uygulama değerlendirmeleriyle sınırlı kalmakta; kentsel dönüşüm, akıllı şehir altyapısı ve güvenlik teknolojileri arasında disiplinlerarası bir analiz eksikliği göze çarpmaktadır.

Bu çalışma, söz konusu boşlukları kapatmayı amaçlamaktadır. Birincisi, akıllı şehir ve güvenli şehir kavramlarının kentsel dönüşüm politikaları ile bağlantısını kurarak bütünleşik bir teorik çerçeve geliştirmektedir. İkincisi, güvenlik teknolojilerini (IP tabanlı gözetim sistemleri, video analiz yazılımları, nesne ve yüz tanıma, akıllı sensörler) hem teknik kapasite hem yönetişim boyutlarıyla sınıflandırmakta hem uluslararası örneklerden hem Türkiye uygulamalarından karşılaştırmalı çıkarımlar yapmaktadır. Üçüncüsü, politika ve strateji önerileri geliştirerek sadece literatür katkısı değil, aynı zamanda belediyeler, merkezi idareler ve teknoloji geliştiriciler için pratik bir yol haritası sunmaktadır. Bu öneriler mahremiyetin korunması, etik standartların güçlendirilmesi, veri güvenliği altyapısının iyileştirilmesi, siber saldırı senaryolarına karşı dayanıklılığın artırılması gibi konuları kapsamaktadır.

Bu bağlamda, tez, beş ana bölümden oluşmaktadır: Giriş niteliğindeki birinci bölümde, çalışmanın temel motivasyonu, araştırma sorunsalı ve metodolojik yaklaşım sunulmaktadır. İkinci bölümde, akıllı şehir paradigmasının kavramsal çerçevesi ele alınmaktadır. Bu bölümde, akıllı şehir kavramının tarihsel evrimi, uluslararası ve ulusal tanımlamalar ile akıllı şehir bileşenleri detaylı olarak incelenmektedir. Ayrıca, Asya-Pasifik (Singapur, Seul), Avrupa (Barcelona, Kopenhag, Berlin, Paris) ve Amerika (San Francisco, New York) modellerinin karşılaştırmalı analizi yapılmaktadır. Bölümün son kısmında ise Türkiye'deki ulusal politika çerçevesi ve büyükşehir belediyelerinin (İstanbul, Ankara, İzmir, Bursa, Antalya, Konya) akıllı şehir projeleri değerlendirilmektedir. Üçüncü bölüm, akıllı şehirlerde güvenlik teknolojileri ve sistemlerini kapsamlı biçimde ele almaktadır. Güvenlik perspektifinden akıllı şehir kavramı, IP tabanlı video gözetim sistemleri, video analiz tabanlı şüpheli davranış tespiti, biyometrik sistemler, kalabalık izleme teknolojileri ve kamu güvenliğine yönelik çözümler bu bölümde detaylandırılmaktadır.

Dördüncü bölümde, akıllı şehirlerde dijital güvenlik teknolojilerinin bireysel hak ve özgürlükler üzerinde yarattığı tehditler analiz edilmektedir. Mahremiyet hakkının ihlali, yüz tanıma ve duygu tanıma teknolojilerinin gizlilik sorunları, demokratik katılımdan dışlanma, kent hakkının ihlali, dijital bölünme, ifade özgürlüğünün kısıtlanması, algoritmik ayrımcılık ve Türkiye'de verilerin kötüye kullanımı riskleri bu bölümün ana konularını oluşturmaktadır. Beşinci ve son bölümde, tartışma, sonuç ve öneriler sunulmaktadır. Bu bölümde, çalışmanın bulguları sentezlenerek, Türkiye özelinde akıllı şehirlerde güvenlik teknolojilerinin etik ve sürdürülebilir kullanımına yönelik çok boyutlu bir yol haritası önerilmektedir."

Sonuç olarak, bu çalışma yalnızca teknolojik yeniliklerin entegrasyonu ile ilgilenmeyip, aynı zamanda bu yeniliklerin etik, hukuki, sosyal ve yönetsel boyutlarını bir arada değerlendirmektedir. Akıllı şehirlerin geleceğinin, teknolojinin sunduğu imkânların ötesinde, bu imkanların insan hakları, veri güvenliği ve kamu yararı ekseninde yönetilmesine bağlı olduğu kabul edilmektedir. Bu nedenle tez, hem uluslararası hem de Türkiye literatüründe eksik olan bütüncül akıllı güvenlik modeli ihtiyacına cevap vermeyi ve farklı bağlamlarda uygulanabilecek, analitik ve politika düzeyinde bir çerçeve sunmayı hedeflemektedir.

2. AKILLI ŞEHİRLER: KAVRAMSAL ÇERÇEVE, KÜRESEL VE ULUSAL UYGULAMALAR

Bu bölümde akıllı şehir olgusuna ilişkin kapsamlı bir çerçeve sunulmaktadır. Kavramın tarihsel evrimi ve gelişim süreci ele alınarak akıllı şehir anlayışının hangi aşamalardan geçerek günümüzdeki biçimini aldığı incelenecektir. Uluslararası ve ulusal ölçekte yapılan tanımlamalar karşılaştırmalı olarak değerlendirilecek; farklı yaklaşımların ortak ve ayrışan yönleri ortaya konulacaktır.

2.1. Kavramın tarihsel evrimi ve gelişimi

Akıllı şehir kavramının kökenleri, 1960'lı yıllarda ortaya atılan "sibernetik olarak planlanan şehirler" (cybernetically planned cities) tanımlamalarına kadar uzanmaktadır. Bu erken dönem kavramsallaştırması, kentsel sistemlerin bilgi işlem teknolojileriyle yönetilmesi fikrini içeriyordu. 1980'lerde "ağ şehirler" (networked cities) kavramı, kentlerin birbirine bağlı sistemler olarak yeniden tanımlanmasını sağladı. Manuel Castells'in (1996) "ağ toplumu" teorisi, bu dönemde kentsel mekânın dijital ağlarla dönüşümünü açıklayan temel çerçevelerden biri oldu.

1990'lı yıllarda "akılcı büyüme hareketi" (smart growth movement), sürdürülebilir kentsel gelişim stratejilerini teknolojik yeniliklerle birleştirmeyi hedefledi (Çetin ve Çiftçi, 2019). Bu dönemde, internetin yaygınlaşması ve kişisel bilgisayarların kentsel yönetim süreçlerine entegrasyonu, akıllı şehir kavramının pratik uygulamalarının temelini oluşturdu. 2000'li yılların başından itibaren, Nesnelerin İnterneti (IoT), büyük veri analitiği ve bulut bilişim teknolojilerinin gelişmesiyle, akıllı şehirler somut uygulama alanı bulmaya başladı.

Dameri (2013), akıllı kentlerin gelişimini üç temel evrede inceler: Birinci nesil akıllı şehirler (1.0), teknoloji odaklı ve yukarıdan aşağıya yaklaşımları benimserken; ikinci nesil (2.0), vatandaş katılımı ve yaşam kalitesine odaklanmıştır. Üçüncü nesil akıllı şehirler (3.0) ise, sürdürülebilirlik, dayanıklılık ve kapsayıcılık ilkelerini merkeze alan bütüncül modeller geliştirmektedir. Bu evrimsel süreç, teknolojinin kentsel sorunlara çözüm aracı olarak kullanılmasından, insan merkezli ve katılımcı yönetişim modellerine doğru bir paradigma değişimini yansıtmaktadır.

2.2. Uluslararası ve ulusal tanımlamalar

Akıllı şehir olgusunun hem akademik hem de politik literatürde pek çok farklı tanımlaması olmasına rağmen, ya da belki de tam bu yüzden, kavramın evrensel olarak kabul görmüş bir tanımı henüz bulunmamaktadır. Farklı kurumsal aktörler tarafından geliştirilen

tanımlamalar, bir yönüyle kavramın çok boyutlu doğasını ortaya koyarken, bir yönüyle de kavramın kendiyle ilişkilendirilen ihtiyaçlara ve hedeflere farklı nitelikler kazanabildiğini göstermektedir.

Avrupa Komisyonu'nun tanımına göre akıllı şehirler, "geleneksel ağların ve hizmetlerin dijital ve telekomünikasyon teknolojileri kullanılarak daha verimli hale getirildiği, sakinlerinin ve işletmelerin yararına olan yerler"dir. Bu tanımlama, ekonomik kalkınma, sürdürülebilirlik ve yaşam kalitesinin iyileştirilmesine odaklanan üçlü bir hedef yapısını vurgular (Bakıcı vd., 2012).

Uluslararası Standartlar Örgütü (ISO), akıllı şehirleri "sürdürülebilir kalkınma hedeflerine ulaşmak için bilgi ve iletişim teknolojilerini (BİT) ve diğer araçları kullanan, yaşam kalitesini, kentsel operasyonların ve hizmetlerin verimliliğini ve rekabet gücünü artıran, mevcut ve gelecek nesillerin ekonomik, sosyal, çevresel ve kültürel ihtiyaçlarını karşılayan şehirler" olarak tanımlamaktadır. Bu kapsamlı tanım, akıllı şehirlerin sadece teknoloji odaklı değil, aynı zamanda sürdürülebilirlik ve nesiller arası adalet perspektifini de içerdiğini göstermektedir.

Birleşmiş Milletler İnsan Yerleşimleri Programı (UN-Habitat), akıllı şehirleri "yenilikçi çözümler kullanarak vatandaşlarına daha iyi hizmetler sunan, kaynak kullanımını optimize eden ve çevresel etkilerini azaltan şehirler" olarak tanımlar. Dünya Bankası ise, akıllı şehirleri "teknoloji yoğun çözümlerle kentsel zorlukları ele alan, veri odaklı karar verme süreçlerini benimseyen ve vatandaş katılımını teşvik eden kentsel alanlar" olarak nitelendirir.

Türkiye'de ise 2024-2030 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı'nda akıllı şehir, "paydaşlar arası işbirliği ile hayata geçirilen, yeni teknolojileri ve yenilikçi yaklaşımları kullanan, veri ve uzmanlığa dayalı olarak gerekçelendirilen ve gelecekteki problemleri öngörerek yaşanabilir ve sürdürülebilir çözümler üreten şehirler" olarak tanımlanmıştır. Bu tanım, Türkiye'nin akıllı şehir vizyonunda iş birliği, veri odaklılık ve öngörücü planlama unsurlarını ön plana çıkarmaktadır (ÇŞİB, 2019).

Akıllı şehir kavramı, en geniş tanımıyla bilişim teknolojilerinin kullanılarak şehirdeki varlıkların ve kaynakların entegre edilmesini amaçlayan bir kentsel gelişim vizyonunu ifade eder. Bu tür şehirlerde, bireylerin yaşamları üzerinde ekonomik düzenlemelerden sosyal yönetim ve kamu hizmetlerine kadar birçok alanda Bilgi ve İletişim Teknolojileri (BİT) etkin bir şekilde kullanılmaktadır (Czupich, 2019). Diğer bir bakış açısıyla akıllı şehir, çeşitli teknolojik, sosyoekonomik unsurların ve yönetişim uygulamalarının karmaşık bir etkileşimini içeren nispeten yeni ve gelişmekte olan bir fikirdir. Bu kavramın uygulanabilirliği, her şehrin

belirli politikaları, hedefleri, finansal durumları ve kapsamına bağlı olarak farklılık göstermektedir. Bu farklılıklar, literatürde akıllı şehir kavramını tanımlamak için çeşitli ve birbirinden farklı tanımların ortaya çıkmasına neden olmaktadır. Giffinger'e göre akıllı bir şehir, öz farkındalığa sahip bağımsız vatandaşların kaynaklarının ve eylemlerinin akıllıca birleştirilmesi üzerine inşa edilen bir yapıdır. Bu tür bir şehir, geleceğe yönelik bir perspektife sahip olup ekonomi, yönetişim, hareketlilik, çevre ve yaşam konularında olumlu bir bakış açısı benimsemektedir (Giffinger vd., 2007). Literatürde, akıllı şehir kavramının eşdeğeri olarak bilişim kentleri (informatic cities) ve dijital kentler (digital cities) gibi terimlerin de kullanıldığı gözlemlenmektedir (Akpınar, 2019). Bu terimler, akıllı şehirlerin ifade ettiği genel kavramları yansıtmaktadır. Bu tanımlamalardan hareketle, akıllı şehirlerde vatandaşların tüm hizmetlerden sabit veya mobil sistemler aracılığıyla yararlandığını söyleyebiliriz. Akıllı şehirleri, gelişmiş kentsel bilgi sistemlerine sahip ve bütünleşik bir bilgi organizasyonuna dayanan bir kentsel yapı olarak tanımlayabiliriz.

Ancak akıllı şehir olarak kavramlaştırmada kullanılan “akıllılık” –akıllı– kavramı kendi başına bir araç değildir. Bunun temelinde bir amaç vardır, burada “akıllı” olmaktaki amaç, kamusal alanda bir değeri, sürdürebilirliği, şeffaflığı, toplumsal refahın teşvik edilmesi ve geliştirilmesiyle ilgilidir. Bu kavramsallaştırmada teknoloji önemli bir rol oynamakta, ancak daha çok şehirdeki yaşam kalitesini geliştirmek ve iyileştirmek için bir araç olarak kullanılmakta ve görülmektedir (Mcbride vd., 2022). Akıllı şehir uygulamalarında istenilen amaçlara ulaşılabilmesi için, "akıllılığın" ne anlama geldiği konusunda ortak bir anlayış geliştirilmelidir. Bununla birlikte, her şehrin farklı zorlukları ve tepkileri göz önünde bulundurularak, bu akıllılık göstergeleri karşılaştırılabilir olmalı, ancak yerel bağlam ve ayrıntı düzeyi dikkate alınarak geliştirilmelidir. Bundan dolayı akıllı şehirlerin evrensel bir tanımına veya en azından ortak bir anlayışa ve net hedeflerin belirlenmesine ihtiyaç vardır (Hunt, 2014).

Akıllı şehir savunucularının ortak noktası, yeni teknolojilerin şehirlere uygulanması ve etkili bir şekilde entegre edilmesinin, yaşam kalitesini iyileştirme, ekonomik büyümeyi hızlandırma, iklim değişikliğinin olumsuz etkilerini azaltma ve hatta daha aktif vatandaşlığı teşvik etme potansiyeline sahip olmasıdır (Gaffney ve Robertson, 2018). Akıllı şehir yaklaşımı şehirleşme sürecinin olumsuz ekonomik etkilerini önlemek üzere ekosistemin bilişim teknolojileri tabanlı bilgi yönetimine odaklanmaktadır. Sosyal ve çevresel sürdürülebilirlik kadar altyapı mekanizmalarının akıllı işletimlerine odaklanan sanal bir varlık olarak tanımlanmaktadır. Akıllı şehir çözümleri, şehirlerin bilgi teknolojileri ile bütünleşerek gerçek zamanlı bilgiye dayalı karar almayı amaçlayan sistemler olarak ortaya çıkmaktadır. Planlama

kuramındaki akıllı şehir kavramı ise dünyada ekonomik rekabeti sağlamak amacıyla küresel şehir altyapısının yeniden yapılanmasına yönelik zorunlu teknolojik önlemlerin alınması olarak tanımlanmaktadır. Küreselleşme süreci, ağ şehirlerin planlamasından başlayarak şehirsel hizmetler ve bilgi-iletişim teknolojileri arasındaki ilişkiyi vurgulamaktadır (Castells, 1996).

Başka bir deyişle, akıllı bir şehir temelde bilgi tabanlı bir şehirdir. Akıllı bir şehir iki önemli kriter üzerine kuruludur. Bunlardan birincisi sürdürülebilir kaynakların etkin kullanıldığı, karbondioksit salınımının azaltıldığı, çevresel etkilerin asgariye indirildiği ve kullanıcıların yaşam standardının iyileştirilebildiği bir ortamı ifade etmektedir. İkincisi ise iletişim, başka bir ifadeyle bilgi işlem sisteminin anlık veri toplama ve işletim altyapısının daha etkin işlemlere imkân sağladığı ve kullanıcılarına daha ayrıntılı bilgi edinme ve planlama yapma imkânı veren bir ortam olarak tanımlanmaktadır. Bir şehrin akıllı şehir olarak tanımlanması için çeşitli akademik çalışmalarda yer verilen tanımlamalara göre aşağıdaki alanlarda belirtilen akıllılık unsurlarını taşıması gerekmektedir (Süleymanlı, 2019):

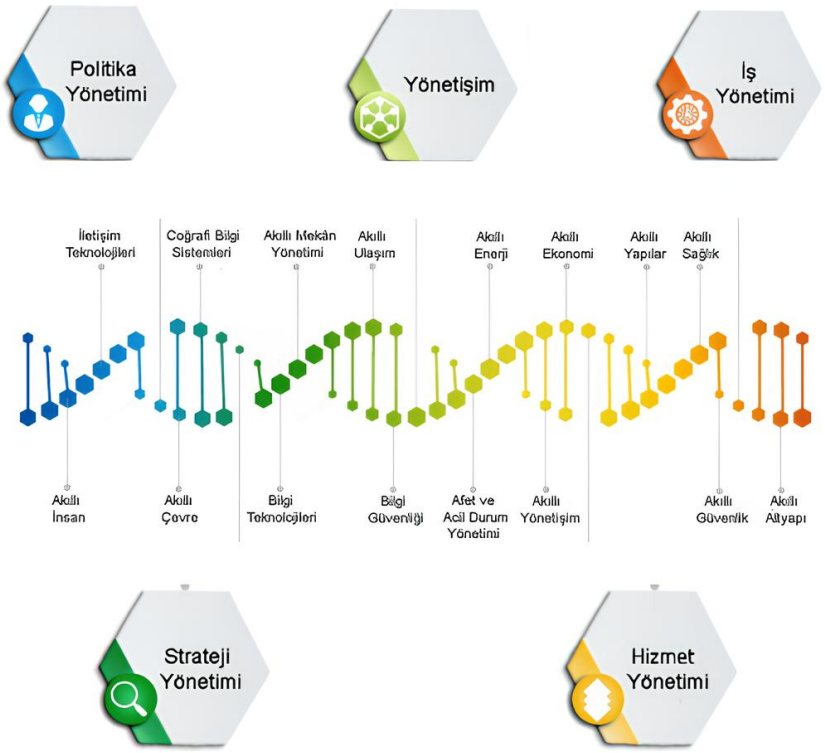
- Haberleşme, enerji dağıtımı ve ulaşım sistemlerinin akıllı altyapı sistemi ile desteklenmesi,
- Eğitim hizmetlerinde bilgi işlem sistemlerinin yaygın olarak kullanılması,
- Bireylerin bilgi işlem sistemi vasıtası ile yönetimin iş ve eylemleri hakkında ayrıntılı bilgi edinmesi,
- Bina ve yapıların, akıllı binaların bütün özelliklerini taşıması,
- Şehirde güvenliğin anlık gözleme ve değerlendirme imkânı sağlayan akıllı güvenlik sistemleri ile desteklenmesi,
- Sağlık hizmetlerinin en kısa sürede yerine ulaştırılması,
- Enerji kullanımında etkinliğin ve verimliliğin akıllı şehir sistemleri vasıtası ile gerçekleştirilmesi,
- Konut/bina, sokak ve altyapı alanlarına ilişkin yapıların akıllı şehir unsurlarının akıllı planlama yöntemleri ile planlanması,
- Şehir suyu dağıtımının ve atık suyun akıllı yöntemler ile toplanmasını ve tekrar kullanıma sunulmasını sağlayan sistemlerin oluşturulması,
- Şehir ulaşım altyapısının akıllı sistemler ile gerçekleştirilmesi,
- Ulaşımda etkinlik ve verimliliğin en üst düzeyde olması.

Hızla değişen küresel dinamikler, vatandaşların yaşamlarını kolaylaştırmak amacıyla teknolojinin daha etkin kullanılması ve bu doğrultuda toplumsal yaşamla bütünleşmiş bir yaşam kalitesi sunulması gerekliliğini ön plana çıkarmaktadır (Akdamar, 2017). Akıllı kent uygulamaları, kentlerde ulaşımdan çevresel kirliliğe, sağlıktan güvenliğe kadar birçok temel sorunla başa çıkma yöntemlerinden biri olarak değerlendirilirken aynı zamanda vatandaşların sosyal ve ekonomik fırsatlarını genişleten çevresel farkındalığı arttıran ve katılımcı bir yönetim anlayışının gelişimine katkı sunan bir araç olarak öne çıkmaktadır (Akdamar, 2017). Bu bağlamda kent ölçeğinde ve kent için gerekli her türlü bilgi ve veriyi en verimli şekilde kullanan uygulamalar, akıllı şehirlerin temel yapı taşlarını oluşturmaktadır. Uygulamalar yalnızca mevcut sorunları çözmekle kalmayıp gelecekte karşılaşılacak zorluklara da çözüm getirmek ve yeni kamu hizmetleri sunacak ağlar oluşturmak gibi önemli bir misyon üstlenmektedir.

Akıllı şehir uygulamaları, sadece ideal bir hedef değil aynı zamanda zorunlu bir dönüşüm sürecini temsil etmektedir. Kent düzeyinde sunulan kamu hizmetlerinin niteliğini ve niceliğini geliştiren bu uygulamalar, şehirlerde yaşam kalitesini ve güvenliği arttırma potansiyeline de sahiptir. Bireylerin günlük yaşamlarına sağlanan katkılar, akıllı kent uygulamalarının bileşenlerinin kendi içlerindeki yeterlilikleri ve birbirleriyle olan entegrasyonları ile doğrudan ilişkilidir. Entegrasyonun başarısı, uygulamaların etkinliği açısından belirleyici bir rol oynamaktadır (Akpulat, 2017).

2.3. Akıllı şehir bileşenleri ve sistemleri

Akıllı şehir uygulaması tek bir cihaz değil, veri ve algoritmalara dayalı çeşitli teknik çözümleri içeren bir şehir konseptidir (Mantelero ve Esposito, 2021). Akıllı şehir kavramının genel kabul gören sekiz unsuru; akıllı altyapı, akıllı güvenlik, akıllı enerji, akıllı yönetim, akıllı eğitim, akıllı sağlık hizmetleri, akıllı bina ve akıllı ulaşım/ hareketlilik olarak sıralanmaktadır. Şehirlerde akıllı dönüşüm, daha modern, rekabetçi ve sürdürülebilir bir kentsel ortam oluşturmak ve dolayısıyla kent sakinlerinin yaşam kalitesini arttırmak amacıyla dijital, fiziksel ve insani sistemlerin entegrasyonunu içeren bir süreç olarak tanımlanmaktadır. Süreç kentsel planlama, yönetim ve operasyonları kapsayan akıllı şehirlerin kavramsal çerçevesini ve çeşitli teknolojileri içermektedir. Akıllı şehirlerin gelişimi, dijital teknolojilerin entegrasyonu ile desteklenmekte olup, bu süreç uzun vadeli kentsel büyüme ve sürdürülebilir hedeflerinin gerçekleştirilmesinde kritik bir rol oynamaktadır (Çetin vd., 2020).



Şekil 1.1. Akıllı Şehir Bileşenleri

Kaynak: (Akıllı Şehirler Portalı, 2023)

Akıllı dönüşümün önemi, vatandaşların yaşam standartlarını ve genel yaşam kalitesini doğrudan etkileyen bir faktör olarak öne çıkmaktadır. Akıllı şehir dönüşümünün temel bileşenleri şunlardır (Arslan, 2014):

- Şehrin ihtiyaçlarını ve hedeflerini açıkça belirlemek,
- Kapsamlı planlama ve uygulama stratejileri geliştirmek,
- Hareketlilik, çevre, ekonomi, insanlar, yaşam ve yönetişim gibi kentsel yaşamın çeşitli yönlerini ele almak için Akıllı Şehirler Çarkı'nın (SCW) entegre edilmesi.

Şehirlerde akıllı dönüşümün etkili bir şekilde uygulanabilmesi için şehir kavramının dönüşüm ve farklılaşma süreçlerinin anlaşılması kritik öneme sahiptir. Akıllı dönüşüm değişimi, kentsel planlama ve gelişimin tarihsel bağlamının yanı sıra modern çağda kentlerin değişen rolleri ve beklentilerinin de incelenmesini gerektirmektedir. Bu bağlamda şehir planlamacıları ve karar vericiler, akıllı şehir konseptlerini ve teknolojilerini mevcut kentsel yapılarla etkili bir şekilde entegre etmektedir. Her şehrin özgün özelliklerini ve ihtiyaçlarını da göz önünde bulundurabilmektedir. Böylece şehir sakinlerine gerçek anlamda fayda sağlayan ve

daha sürdürülebilir sonuçlar elde eden akıllı şehir dönüşümleri gerçekleştirilebilmektedir (Erkek, 2017). Bununla birlikte, akıllı şehirlerin temel bileşenlerinden biri olarak öne çıkan özelleştirme uygulamaları ve kamu-özel sektör işbirlikleri, vatandaşların temel ihtiyaçlarının karşılanması sürecinde çeşitli olumsuzluklara ve eşitsizliklere yol açabilmektedir. Şirketler ve teknoloji sektörü akıllı şehirlerin geliştirilmesi ve uygulanmasında önemli roller oynadıkça, giderek daha fazla sayıda kamu işlevi ve hizmeti özelleştiriliyor ve özel aktörlere devrediliyor. Ekonomik sermayeye dayalı güç, neoliberalizm, rekabete dayalı piyasa ekonomisi ve kapitalizm ideolojilerinin etkisiyle şekillenen akıllı şehir süreçleri, giderek egemen hale gelmektedir. Akıllı şehirlerde hizmetler ve kamusal mallar, şirketlerin kârlarını arttırma amacıyla kullanılır hale gelmekte ve giderek şirketlerin en yüksek kâr için rekabet ettiği pazarlar olarak işlev görmektedir. Özel aktörlere fayda sağlayan şehir politikaları, çoğunluğun refahını ve haklarını sağlamak yerine küçük ve varlıklı bir seçkinler grubunun çıkarına işleyen neoliberal politik ekonomilerin yaratılmasını güçlendirmektedir. Kapitalist neoliberal politikaların şekillendirdiği akıllı şehirlerde eşitsizlikler, sosyal ve mekansal ayrımlar derinleşmektedir. Dolayısıyla yurttaşların ihtiyaçları ve faydaları, en yüksek kar marjlarını elde etme, uzun vadeli yatırımlar yapma gibi konular karşısında ikinci planda kalmaktadır (Reuter, 2020). Akıllı teknolojilerin kamu altyapısının özelleştirilmesine yönelik etkisi, sistematik ayrımcılığın artmasına, toplum içerisinde dijital bölünmeye, bireylerin hak ve özgürlüklerinin tehdit edilmesine yol açabilir (Qarri ve Gill, 2022).

2.3.1. Akıllı altyapı

Akıllı şehirler, sürdürülebilir kalkınmayı destekleyen ve sakinlerinin yaşam kalitesini arttıran yeni teknolojiler ve kentsel planlama teknikleri ile sürekli olarak gelişmekte ve uyum sağlamaktadır. Bu şehirlerde kullanılan kentsel planlama teknikleri, çevresel olarak uyumlu fiziksel, dijital ve insani sistemlerin entegrasyonunu içermekte ve modern, rekabetçi ve sürdürülebilir kentsel ortamlar yaratmayı hedeflemektedir. Bu teknikler, küresel büyümenin ve hızlı kentleşmenin getirdiği zorluklarla başa çıkmak için kritik öneme sahiptir. Akıllı şehirlerin temel unsurları ve kentsel planlamada kullanılan teknolojiler, şu unsurları içermektedir (Örselli ve Akbay, 2019):

- Sürdürülebilir ulaşım sistemleri
- Verimli enerji yönetimi
- Gelişmiş atık yönetimi çözümleri
- Akıllı binalar ve altyapı
- Bağlantılı kamu hizmetleri ve olanakları

- Dijital ve veri odaklı kentsel yönetişim

Teknoloji, sürdürülebilir kentsel kalkınmayı desteklemek için çeşitli sistem ve süreçlerin entegrasyonunu kolaylaştırarak akıllı şehirlerin tanımlanmasında ve etkinleştirilmesinde kritik bir rol oynamaktadır. Akıllı şehirler bağlamında teknoloji, kentsel yaşamın farklı yönlerini birbirine bağlayan ve optimize eden çok çeşitli dijital araçları, platformları ve altyapıları kapsamaktadır. Akıllı şehir projeleri paydaşlar arasındaki işbirliği yoluyla yenilikçi çözümler geliştiren, kentsel planlama, yönetim ve yönetişimi iyileştirmek için yeni teknolojiler ve verileri kullanan şehirler olarak tanımlamaktadır. Bu şehirlerde teknolojinin önemli bir boyutu, şehir yönetimini daha etkili ve verimli hale getirmek amacıyla kullanılan akıllı yönetimdir (Arslan, 2014).

Ancak akıllı altyapıların geliştirilmesi sürecinde çeşitli zorluklarla karşılaşılmaktadır. Bu zorlukların başında gizlilik, güvenlik ve birlikte çalışabilirlik sorunları gelmektedir. Akıllı şehirlerde bilgi ve iletişim teknolojilerinin mevcut kentsel altyapıya entegrasyonu, bu sorunların daha da karmaşık bir hâl almasına neden olabilmektedir. Çoğu durumda bu, gerçek zamanlı veri toplayabilen sensörlerin ve kablosuz sensör ağlarının (WSN) kentte yayılmasını içerir. Bu süreç, kentsel nesnelerin internetinin yaygınlaşması olarak da adlandırılır. BİT ve IoT'nin kentsel sistemlerle birleşimi, yüksek derecede birlikte çalışabilirlik gerektirir. Çalışabilirlik, farklı sistemlerin etkileşime girme ve bilgi paylaşma yeteneğini ifade eder. Dolayısıyla akıllı şehirlerde tüm sistemlerin entegre bir şekilde çalışması önem taşır. Çünkü akıllı şehirlerin gelişimi için bir araya getirilmesi gereken çok sayıda eski ve karmaşık bir teknolojik sistem bulunur. Akıllı şehir gelişimi için birlikte çalışabilirlik sorunlarının üstesinden gelmenin hayati önem taşıdığı açıktır (Pierce ve Andersson, 2017).

2.3.2. Akıllı şehir güvenliği

Şehir güvenliği ve sağlığı kavramları, yalnızca bireylerin sağlık ve güvenliğini korumayı değil, aynı zamanda şehirlerin doğal afetler ve kazalar gibi olağanüstü durumlar sonrasında hizmetlerini ve ulaşım altyapısını onarma ve sürdürülebilir bir şekilde yeniden yapılandırma kapasitesini de ifade etmektedir. Dijital bilgi altyapısı, bu tür beklenmedik durumları yönetme, kavrama ve hassas durumları ayırt etmede kritik bir rol oynamaktadır. Sağlıklı şehir güvenliği, asayiş, kurtarma ve acil sağlık hizmetleri gibi unsurları kapsamaktadır. Örneğin şehirdeki güvenlik kameraları, akıllı yönetim ağında bulunan yönetim binasına entegre edilmekte ve şehrin her noktasının izlenmesini sağlamaktadır. Bu entegrasyon sayesinde, suç

oranları şehirlerde azalmakta ve genel güvenlik seviyeleri artmaktadır (Şengül ve Altıntaş, 2020).

Bir kentin akıllı olarak kabul edilebilmesi için, dijital teknolojilerin etkin bir şekilde kullanılmasıyla birlikte, akıllı ekonomi, akıllı ulaşım, akıllı yönetişim, akıllı yaşam, akıllı vatandaş ve akıllı çevre gibi bileşenlerin kentteki dönüşüm sürecine katkıda bulunması gerekmektedir. Gelişmiş teknolojiye sahip Avrupa, Amerika Birleşik Devletleri ve Çin gibi ülkelerde, kentlerin stratejik planlarına entegre edilen akıllı uygulamalar, Türkiye'de ise İstanbul, İzmir, Ankara, Bursa, Kayseri ve Yalova gibi şehirlerde kısmi uygulamalar olarak hayata geçirilmiştir. Akıllı kent uygulamaları, kentsel yaşamla ilgili temel verilerin çeşitli yazılımlar aracılığıyla işlenmesini içerdiği için, bu yazılımların sürdürülebilirliğinin sağlanması aynı zamanda güvenlik açısından önemli bir mesele oluşturur. Örneğin, akıllı ulaşım sistemine yapılacak bir dijital müdahale, tüm trafik düzenini bozabilir. Benzer şekilde, akıllı enerji sistemine yapılacak bir saldırı, tüm sistemin işleyişini olumsuz etkileyebilir (Uçar vd., 2017). Kişisel veriler, 24 Mart 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (KVKK) "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır (KVKK, 2016). Bu kapsamda, kişisel veriler, bireyi tanımaya yarayan özgün bilgilerin (ad, soyad, anne adı, baba adı, doğum tarihi ve yeri gibi) yanı sıra, fotoğraf, ev ve e-posta adresi, banka bilgileri, tıbbi bilgiler, sosyal medya paylaşımları ve IP adresi gibi fiziksel, fizyolojik, ekonomik, kültürel, sosyal veya psikolojik pek çok bilgiyi içermektedir. Kanuna göre, kişisel verilerin ilgili kişinin izni olmadan kullanılması yasaktır ve bu yasağa uymayanlar, ciddi cezai yaptırımlara tabi tutulmaktadır.

Teknolojik gelişmeler ve yenilenen sistemler ile birlikte, akıllı şehirlerde yaşayan bireylerin teknolojiye uyum sağlama, teknolojiyi etkin şekilde kullanma ve değişime hızla adapte olma becerilerine sahip olmaları gerekmektedir. Buradan hareketle şehirdeki tüm bireyleri ve eğitim kurumlarını kapsadığı söylenebilir. Akıllı şehirlerin bir diğer önemli hedefi, şehirleşmenin doğaya verdiği zararı azaltmak ve ortadan kaldırmaktır. Bu kapsamda kaynakların etkin bir şekilde yönetilmesi ve kullanılmasının yanı sıra atıkların kontrol edilmesi ve geri dönüştürülmesi, doğa dostu teknolojilerin uygulanması ve enerji kaynakları olarak öncelikle yenilenebilir enerji kullanımı hedeflenmektedir. Bu hedeflere ulaşmak için, doğal kaynaklar, enerji yönetimi ve atık kontrol merkezleri gibi unsurlar temel bileşenler olarak değerlendirilmelidir. Kaynakların doğru ve verimli bir şekilde kullanılması sağlanırken, sistemlerin güvenliğinin sağlanması, kaynak israfını ve verimsiz kullanımını önlemek açısından kritik öneme sahiptir. Akıllı güvenli şehir konseptinde, her bir boyut, sistemin ayrılmaz bir

parçası olarak ele alınmalı ve her boyutun güvenliği ayrı ayrı sağlanarak, bütüncül bir işleyiş gerçekleştirilmelidir (Arslan, 2014).

2.3.3. Akıllı enerji

Günümüzde şehirler, enerji üretimi ve tüketimine bağlı olarak ciddi çevresel sorunlarla karşı karşıya kalmaktadır. Bu bağlamda, modern şehircilik yaklaşımlarının hava, su ve toprak gibi temel çevresel unsurları gözeterek, söz konusu kaynakları sürdürülebilir ve akıllı şehir modelleriyle bütünleştirmesi büyük bir önem arz etmektedir. Bu bağlamda, akıllı enerji kavramı, enerjide sürdürülebilir yenilikçiliği temsil etmektedir. Akıllı enerji stratejileri, beş ana hedef çerçevesinde yapılandırılmaktadır. Birincisi, enerji tüketimi ve taşımacılığında etkinliğin arttırılmasıdır. İkincisi, yenilenebilir enerji kaynaklarının verimliliğinin yükseltilmesidir. Üçüncüsü, akıllı mekân yönetimi için yeni yöntemlerin geliştirilmesidir. Dördüncüsü, şehir düzeyinde enerji üretiminin teşvik edilmesi veya iyileştirilmesidir. Sonuncusu ise enerji ihtiyacının ve çevresel etkilerin azaltılması amacıyla yapılan düzenlemelerdir. Bu hedefler, şehirlerin enerji yönetimini daha etkin, sürdürülebilir ve çevre dostu hale getirmek için kritik öneme sahiptir (Çodur ve Topdağı, 2018).

Akıllı şehirlerde kullanılan akıllı ulaşım teknikleri, kentsel mobilitenin etkinliğini arttırma ve sürdürülebilirliğini sağlama amacıyla çeşitli yenilikçi uygulamalar içermektedir. Bu tekniklere şu örnekler verilebilir (Kocaman, 2020):

- Akıllı trafik yönetim sistemleri
- Gerçek zamanlı toplu taşıma bilgileri
- Entegre multimodal ulaşım ağları
- Otonom araçlar ve araç paylaşımı hizmetleri
- Bisiklet paylaşım programları ve elektrikli araç şarj istasyonları

Enerji, akıllı şehirlerin işleyişinde merkezi bir rol oynamaktadır. Ulaşım, su yönetimi, sağlık hizmetleri, çevresel yönetim ve güvenlik gibi birçok kentsel sorun, etkin enerji yönetimi ve kaynak tahsisi ile doğrudan ilişkilidir. Bu nedenle, enerji yönetimi akıllı şehirlerin başarısı için kritik öneme sahiptir. Şehri akıllı kılan önemli unsurlar arasında teknoloji ve enerji yer alır. Akıllı şehirlerde, çeşitli faktörlerin uyumlu bir şekilde entegre çalışması esastır ve bu entegrasyonun başarısı büyük ölçüde teknolojiye bağlıdır. Teknolojik unsurlar, akıllı şehirlerin işleyişinde merkezi bir rol oynar. Bu unsurların eksikliği, şehirlerin verimliliği ve işlevselliği üzerinde olumsuz etkiler yaratabilir. Teknoloji, kentsel sistemlerin optimize edilmesini, veri

analizi ve yönetimini ayrıca çeşitli hizmetlerin entegre edilmesini sağlayarak şehirlerin akıllı olma özelliklerini destekler ve güçlendirir (Akpulat, 2017).

2.3.4. Akıllı yönetim

Akıllı yönetim bir kurum faktörü olarak düşünülebilir. Kurum yönetimi şehir yönetiminde önemli bir bileşendir. İlk bakışta akıllı kentleşme üzerinde doğrudan bir etkisi yokmuş gibi görünse de aslında bu faktör akıllı şehirlerin başarısında vazgeçilmez bir rol oynar. Şehrin planlanması, stratejik hedeflerin belirlenmesi ve finansman sağlanması gibi kritik süreçlerde önemli sorumluluklar üstlenir. Yürütücü güç olarak kurumlar, yapılan yatırımlardan olumlu sonuçlar elde edilmesinden sorumlu olup akıllı şehir projelerinin başarısını doğrudan etkiler. Bu nedenle, alacakları kararlar ve gerçekleştirecekleri yatırımlar, şehrin geleceği açısından belirleyici olacaktır. Kurumların attıkları adımlar ve çıkardıkları yasalar, iş birliği ortamını güçlendirmek ve paylaşımcı ekonomiyi teşvik etmek açısından büyük önem taşır. Yaşanabilecek olumsuz olaylara karşı şehrin zarar görmesini en aza indirme ve vatandaşların mahremiyetini koruma sorumluluğunu da taşımaktadır (Arslan, 2014).

Belediye ve özel idareler gibi yerel yönetimler, idari sorumluluk alanlarındaki vatandaşların artan taleplerini karşılamak ve bu talepler doğrultusunda çalışma programlarını hayata geçirmek konusunda kritik bir rol oynamaktadır. Ekonomik daralma dönemlerinde ve şehir yönetim sistemlerinin yeniden yapılandığı süreçlerde daha da önemli hale gelmektedir. Teknolojinin bu tür yönetim süreçlerine entegrasyonu, açık yönetim, şeffaflık ve verilerin net bir şekilde sunulması gibi unsurların ön plana çıkmasını sağlamaktadır. Bu sayede, yerel yönetimler, hem vatandaşlarla daha etkin bir iletişim kurmakta hem de kaynakların verimli kullanılmasını mümkün kılmaktadır (Akpulat, 2017).

Günümüzde dünya nüfusunun yaklaşık yarısını barındıran şehirler, nüfus artışı, altyapı ihtiyaçları ve hizmet yoğunluğu gibi boyutlarda hızla büyümektedir. Hem iç hem de dış bağlantıları ve bağımlılıkları artarak karmaşık bir yapıya bürünmektedir. Bu durum, şehirlerin ekonomik, çevresel ve yönetişim bağlamında karşı karşıya kaldıkları sorunların daha da derinleşmesine yol açmaktadır. Sürdürülebilirlik niteliğini kaybeden şehirler, iklim değişikliği, hava kirliliği ve kent yoksulluğu gibi küresel sorunların büyümesine yol açmaktadır. Teknolojik imkanların şehir yönetimlerine entegrasyonu, etkinlik ve verimlilik ilkelerine katkı sunarak şehirleri daha sürdürülebilir kılma potansiyeline sahiptir (Kocaman, 2020).

Şehirlerin yönetim süreçlerinde bilgi ve iletişim teknolojilerine yer vermesi, bu alanın akademik olarak incelenmesine zemin hazırlamıştır. Teknolojinin yönetime ilk kez dahil

edilmesi, bilgisayarların icadı ve özellikle mali işlemler gibi yönetsel faaliyetlerde kullanımıyla gerçekleşmiştir. Teknolojinin kamu sektöründeki erken dönem kullanım örneklerinden biri olan kent bilgi sistemleri projesi, yerel yönetimler ve kentsel ölçek açısından, özellikle akıllı şehir kavramı bağlamında büyük önem taşımaktadır (Arslan, 2014). Bilgisayar ve internetin günlük yaşamda ve kamu yönetiminde daha yaygın kullanıldığı yeni kamu yönetimi anlayışı, yerel yönetimlerin önemini artırmış ve teknolojinin ekonomik, ulaşım, çevresel ve yönetişim boyutlarına daha fazla entegre olmasını sağlayan bir fırsat yaratmıştır. Bu yaklaşım, insan merkezli bir yönetim anlayışı benimseyerek etkinlik, verimlilik ve ekonomiklik ilkelerini, şeffaflık, hesap verebilirlik ve sürdürülebilirlik prensipleri doğrultusunda politika geliştirme ve hizmet sunumuna entegre etmiştir (Akpulat, 2017).

Akıllı şehir yönetimi yaklaşımının yurttaşlar için avantajlarından sıkça bahsedilirken, akıllı şehirleri eleştirenler tarafından akıllı şehir yönetimi yaklaşımlarının olumsuz yönlerinden de bahsedilmektedir. Bu bağlamda öne sürülen en çarpıcı eleştiri, akıllı şehirlerde yukarıdan aşağıya ve teknokratik bir yönetişim anlayışına sahip olma potansiyelidir. Başka bir deyişle, akıllı şehirlerde gündeme gelen ve çözülmesi planlanan birçok sorun ve uygulama, yurttaşların katkısı ve düşünceleri yerine yukarıdan aşağıya doğru yürütülmekte, özellikle özel örgütsel-kamu yönetimi işbirliğiyle yönetilir. Bu durum yurttaş merkezli müzakereci demokratik bir yönetim yerine teknokratik yönetime yol açmaktadır. Bu nedenle, vatandaşlar dolaylı bir rol oynayabilir veya hiç rol oynamayabilir. Bu anlayışta vatandaşlar, tüketiciler veya veri toplamada araçsal rolleri olan kişiler olarak görülebilir (Reuter, 2020).

Kitchin'e göre, bu yönetim anlayışında, kararların doğası gereği otomatik bir yönetim uygulaması söz sahibi olabilir. Bu tür otomatik sistemlerde, veriler üzerinde hareket etme ve karar alma kuralları şeffaflıktan çok uzak ve gizli olarak kabul edilebilir. Sistem uygulayıcıları ve programcılar, başlangıçta bunu yapacak özel yetkileri olmamasına rağmen, kuralları bilgisayar koduna dönüştürürken, istemeden de olsa, kuralların içeriğini değiştirmeyi rutin olarak kolaylaştırırlar. Dahası, zayıf algoritmalar ve hataya açık veriler yüksek oranda yanlış pozitif ve temelsiz kararlara yol açabilir. İdari kural koymanın şeffaflığı, doğruluğu ve politik hesap verebilirliği kaybolur, politika ve hukuk istemeden çarpıtılır ve kritik prosedürel güvenlik önlemleri potansiyel olarak ortadan kaldırılır. Bu durum, özellikle sistemin kararları gizli aldığı veya denetimin pek mümkün olmadığı durumlarda dışarıdan denetim ve incelemeyi zorlaştırmaktadır. Bu tür otomatik sistemler endişe verici ve tehdit edici olabilir; örneğin, uçuş yasağı olan kişilerin listeye neden eklendikleri kendilerine söylenmeyebilir ve bu karara itiraz etme hakları da olmayabilir (Kitchin, 2016).

Kitchin'e göre, bu yönetim anlayışında, "bireylerin verileri doğrulamak, sorgulamak, düzeltmek veya silmek için erişim talep etmesini, hatta kime soracağını bilmesini; kendileri hakkında toplanan verilerin nasıl kullanıldığını bilmesini; veriler üzerinde yapılan herhangi bir eylemin ne kadar adil olduğunu değerlendirmesini ve veri denetleyicilerini sorumlu tutmasını zorlaştırır". Dahası otomatik sistemler, bildirim ve onayı neredeyse imkânsız hale getirir, çünkü kamuoyunun gizli kaynak kodlarına yerleştirilmiş yeni kuralları inceleme fırsatı yoktur ve bireyler kendilerini bağlayacak yeni kurallardan haberdar değildir (Kitchin, 2016).

2.3.5. Akıllı binalar

Dünyanın pek çok ülkesinde konut yapımında ve konut iletişim sistemlerinde ileri düzeyde bilgi teknolojilerinin kullanımı giderek yaygınlaşmaktadır. Bu sayede akıllı bina ve mekânlar ile çevreye duyarlı yapılar ortaya çıkmaktadır. Bu tür binaların öne çıkan özellikleri arasında izleme, değerlendirme ve raporlama esaslarına dayalı gelişmiş bilgi işlem altyapısı yer alır. Binalarda kullanılan bu sistemler, giriş çıkış işlemlerinin yönetimi, enerji akışı ve tüketiminin kontrolü, sürekli görsel kayıt sistemleri, yangın ihbar sistemleri, izinsiz girişlerin denetimi, sıcaklık ve soğutma sistemlerinin yönetimi gibi pek çok işlevi entegre bir şekilde yürütmektedir. Bilgi işlem altyapısı sayesinde bu veriler sistem bileşenleri arasında paylaşılarak işletim sisteminin bağımsız bir şekilde süreçleri yönetmesine olanak tanımaktadır (Akpulat, 2017).

Akıllı şehirlerde, kaynakların verimli kullanımı ve çevresel sürdürülebilirliğin sağlanması amacıyla çeşitli atık yönetimi stratejileri ve teknolojileri hayata geçirilmektedir. Özellikle akıllı çevre bileşeni, kentsel planlama, kaynak yönetimi ve akıllı binaların entegrasyonuyla atık yönetimi süreçlerini optimize etmeye odaklanır. Bu gelişmiş teknolojiler, şehirlerin atık yönetim sorunlarını daha etkin bir şekilde analiz etmesine ve çözmesine olanak tanıyarak, kentsel sürdürülebilirliğe ve yaşam kalitesinin artmasına katkıda bulunur. Aynı şekilde, akıllı su yönetimi, su kaynaklarının kullanımını, dağıtımını ve korunmasını optimize etmek için yenilikçi stratejiler ve ileri teknolojilerin entegrasyonunu kapsar. Su temini, atık su arıtımı ve yağmur suyu yönetimi sistemlerinin verimliliğini arttırmak amacıyla gerçek zamanlı izleme, veri analizi ve akıllı karar alma mekanizmalarını içerir. Akıllı su yönetimi, kentsel su altyapısının kalitesini, güvenilirliğini ve dayanıklılığını geliştirmede kritik bir rol oynar (Arslan, 2014).

Diğer taraftan dünya nüfusunun büyük çoğunluğu artık kentsel alanlarda yaşamaktadır. Kırsal nüfusun azalacağı ve kentsel nüfustaki artışın gelecekte de devam edeceği

öngörülmektedir. Bu bağlamda şehirlerde su yönetimi giderek daha kritik bir hale gelmektedir. Kentsel alanlar büyüdükçe su kaynaklarına olan talep artacak su kıtlığı, kirlilik ve eskiyen altyapı gibi sorunlarla başa çıkmak için yenilikçi yaklaşımlara ihtiyaç duyulacaktır. Akıllı su yönetimi stratejileri, şehirlerin su kaynaklarını sürdürülebilir bir şekilde kullanmasını çevresel dengeyi korumasını ve şehir sakinlerinin yaşam kalitesini arttırmasını sağlayabilir. Özellikle akıllı şehirlerde su yönetimi, hızlı kentleşme ve nüfus artışının getirdiği zorlukların çözümünde merkezi bir rol oynamaktadır. Bu stratejilerin örnekleri arasında su tüketiminin izlenmesi amacıyla kullanılan akıllı sayaçlar, yağmur suyunun toplanarak depolanmasını sağlayan sistemler ve su kirliliğini azaltmayı amaçlayan ileri teknolojilere sahip atık su arıtma tesisleri yer almaktadır. Bu tür yenilikçi çözümlerle akıllı şehirler, su kaynaklarını etkin bir şekilde yönetebilir, çevresel sürdürülebilirliği teşvik edebilir ve vatandaşların refahını arttırabilir (Akpulat, 2017).

Akıllı şehirlerde akıllı bina ve altyapı uygulamalarının pek çok avantajına rağmen, eleştiriler de dile getirilmektedir. Örneğin akıllı şehir altyapısına kimin sahip olduğu, kontrol ettiği ve kimin erişebildiği; mahremiyet ve gözetim sorunları; katılım ve erişim açısından eşitsizlikler; ve algoritmik kültürün vatandaşlık ve kamusal alan üzerindeki ihlali gibi eleştiriler de bulunmaktadır (Heitlinger ve Comber, 2018).

2.3.6. Akıllı ulaşım

Akıllı Ulaşım Sistemleri (ITS), modern ulaşımın hızla gelişen yapısında köklü bir değişim yaratarak insanların ve nesnelerin taşınmasında önemli bir dönüşüme öncülük etmiştir. Akıllı Ulaşım Sistemleri (ITS), ulaşım ağlarının etkinliğini, güvenliğini ve çevrenin korunmasını ve iyileştirilmesini amaçlayan teknoloji, veri analitiği ve iletişim sistemlerini bir araya getirirler. ITS, trafik yönetimi, araç işletimi ve toplu taşıma sistemleri dahil olmak üzere ulaşımın çeşitli alanlarını geliştirmek için ileri bir teknolojik bilgi ve iletişim teknolojisini kullanır. ITS, gerçek zamanlı veriler, sensör ağları ve akıllı algoritmalar kullanarak trafik sıkışıklığını hafifletmeyi, yolculuk sürelerini kısaltmayı, güvenliği iyileştirmeyi ve çevresel etkileri sınırlamayı amaçlamaktadır. ITS'nin kapsamı, akıllı trafik sinyal sistemleri, otonom araç teknolojisi, dinamik rota planlaması, elektronik geçiş ücreti toplama ve gerçek zamanlı toplu taşıma takibi gibi çok çeşitli uygulamaları kapsayacak şekilde geniştir. Araç Ad-hoc Ağları (VANET'ler), Akıllı trafik ışıkları (ITL), Sanal Trafik Işıkları (VTL) ve Hareketlilik Tahmini, Akıllı Ulaşım Sistemleri şemsiyesi altında yer alan temel sistemlerdir. Bu teknolojik gelişmeler, bireylerin günlük ulaşım deneyimini iyileştirmenin yanı sıra enerji tasarrufu, düşük

emisyon ve geliştirilmiş kentsel planlama gibi daha geniş sosyal hedeflere de önemli katkılar sağlar (Elassy vd., 2024).

Nüfus artışıyla birlikte şehirlerin hem yatay hem de dikey olarak yeniden yapılandırılması, iklim değişikliklerinin etkileri ve fosil yakıtların giderek azalması gibi çeşitli faktörler, akıllı şehir uygulamalarını önemli ölçüde etkilemektedir. Bu bağlamda ulaşım konusu akıllı trafik yönetimi, sür ve park et uygulamaları ve anlık araç takip sistemleri gibi başlıklar altında ele alınmaktadır. Elektrikli otobüsler, yaya ve bisiklet kullanımının entegre edilmesiyle sıfır karbon salınımına yönelik çevresel sürdürülebilirliğe katkı sağlanmaktadır (Kocaman, 2020).

Akıllı ulaşım sistemleri, şehirlerin sürdürülebilirlik, verimlilik ve yaşam kalitesini arttırmak amacıyla trafik yönetimi, ulaşım planlaması ve yol güvenliği gibi kritik alanlarda yenilikçi teknolojiler kullanarak önemli çözümler sunmaktadır. Bu sistemler, şehir trafiğini optimize etmeyi ve hava kirliliğini azaltmayı hedeflerken akıllı şehirler daha geniş bir dijital altyapı ile enerji, atık, su yönetimi ve acil durum müdahaleleri gibi çeşitli alanlarda etkin çözümler sunarak yaşam kalitesini yükseltmektedir. Böylelikle akıllı şehir teknolojileri vatandaşlara daha güvenli, sürdürülebilir ve yaşanabilir bir çevre sağlama potansiyeli taşır.

Öte yandan akıllı şehirlerde akıllı ulaşımlar kentlerin karşılaştığı ulaşım zorluklarına yenilikçi çözümler getirerek şehir yaşamını optimize etmektedir. Bu teknoloji, özellikle trafik sıkışıklığı, hava kirliliği ve enerji tüketimi gibi sorunları ele alarak sürdürülebilir bir ulaşım ağı oluşturmayı amaçlar. Trafik akışının izlenmesi, veri analitiği ve sensör teknolojileri gibi yeniliklerle donatılan akıllı ulaşım sistemleri, trafik yoğunluğunu azaltarak hem zaman hem de enerji tasarrufu sağlar. Güvenli ve etkili toplu taşıma sistemleri, paylaşımlı taşıma modelleri ve otonom araçlar gibi ileri teknoloji uygulamalarıyla, vatandaşlara daha çevre dostu, ekonomik ve erişilebilir ulaşım seçenekleri sunularak şehirlerin yaşanabilirliği arttırılır. Büyük şehirlerin yönetimleri, trafik sıkışıklığı gibi sorunları çözmek ve ulaşımı daha verimli hale getirmek için yapay zekâ ve büyük veri analitiği temelli çözümlere yönelmektedir. Yapay zekâ algoritmaları, trafik akışını izlemek, yoğunlukları öngörmek ve sıkışıklığı azaltmak için kullanılırken büyük veri analitiği ise trafik modellerini oluşturma, hareketlilik trendlerini analiz etme ve ulaşım altyapısını optimize etme süreçlerinde kritik bir rol oynamaktadır. Bu teknolojilerin entegrasyonu, şehirlerin trafik yönetiminde daha akıllı ve sürdürülebilir kararlar almasını mümkün kılmaktadır (Güvendik, 2016).

Elektrikli ve otonom araçlar, akıllı şehirlerin geleceğini şekillendiren temel unsurlardan biri olarak öne çıkmaktadır. Elektrikli araçlar, fosil yakıtlara kıyasla daha çevre dostu bir ulaşım alternatifi sunarken otonom araçlar ise trafik akışını optimize ederek hem güvenliği artırmakta hem de trafik sıkışıklığını azaltmaktadır. Bu sayede, elektrikli ve otonom araçların yaygınlaşmasıyla çevresel sürdürülebilirlik ve ulaşım verimliliği önemli ölçüde arttırmaktadır. Aynı zamanda trafik kazaları ve hava kirliliği gibi sorunların azalması beklenmektedir. Ulaşım verilerinin analizi, şehir planlamacılarının ulaşım altyapısını optimize etmelerine ve sürdürülebilir stratejiler geliştirmelerine olanak tanır. Trafik yoğunluğu, seyahat süreleri, ulaşım araçlarının kullanım oranları ve yolculuk tercihleri gibi çeşitli faktörlerin analizi, gerçek zamanlı verilerle desteklenen daha etkili kararlar alınmasına imkân verir. Bu sayede, akıllı şehirlerin ulaşım sistemleri daha kullanıcı dostu, güvenli ve verimli hale gelmektedir (Çetin vd., 2020).

2.4. Küresel akıllı şehir modelleri ve stratejileri

Bu bölümde akıllı şehir kavramının küresel ölçekte nasıl yorumlandığı ve uygulandığı incelenmektedir. Farklı ülkelerde geliştirilen akıllı şehir modelleri ele alınarak bu modellerin temel özellikleri, yaklaşımları ve öncelikleri değerlendirilecektir.

2.4.1. Asya-pasifik deneyimleri

- Singapur: Akıllı Ulus Vizyonu

Akıllı şehir planının vizyonu, bilgi ve iletişim teknolojilerini büyütmek, başlıca ekonomik sektörlerdeki rekabetçiliği geliştirmek ve bağlantılı bir toplum inşa etmek olarak belirlenmiştir. Tüm bu unsurlar, gelecekteki on yılda vatandaşların yaşam kalitesini iyileştirmeyi hedeflemektedir. Singapur'daki akıllı şehir vizyonu, bir süredir gündemde olup şehrin temel odak noktaları arasında insanların sosyal yaşamı, çevrenin korunması ve ekonomik sürdürülebilirlik bulunmaktadır (Cities In Motion, 2018). Singapur'un akıllı şehir girişimlerinde yer alan kamu sektörü, bu alanda sorumlu olan çeşitli hükümet kurumları ve bakanlıklardan oluşmaktadır.

Singapur'daki İletişim ve Bilgi Bakanlığı (MCI), halkı topluluklarla, hükümetle ve fırsatlarla birleştirme misyonunu üstlenmektedir. Bu bakanlığın altında yer alan Singapur'un yasal kuruluşu olan İletişim ve Medya Otoritesi (IDA), bilgi teknolojisi ve telekomünikasyon alanlarında Singapur'daki her yaştan vatandaş ve şirketlere hizmet sunmayı amaçlamaktadır (Harrison ve Donnelly, 2011). Singapur hükümeti, farklı hükümet kurumlarının akıllı şehir hedeflerine ulaşmak için çabalarını koordine etmek üzere Akıllı Ulus Program Ofisi'ni (SNPO)

kurmuştur (Cities In Motion, 2018). Bu ofis, akıllı şehir stratejilerinin uygulanmasında merkezi bir rol oynamaktadır.

Singapur'un Akıllı Şehir stratejisi, hükümet tarafından geliştirilen çeşitli planlara dayanarak hayata geçirilmektedir. 2014 yılında başlatılan Akıllı Ulus 2014 ve 2015 planları, akıllı şehir girişimlerini gerçekleştirmek için kurumsal ve eylem odaklı bir çerçeve sunmuştur (Townsend, 2013:24). Hükümet, yenilikçi projeleri desteklemek ve risk almayı teşvik etmek amacıyla uygun altyapıyı ve politikaları hazırlayarak, denemelere ve yeniliklere olanak tanımaktadır. Hindistan, Çin ve Birleşik Arap Emirlikleri (BAE) gibi gelişmekte olan akıllı şehirlerle işbirlikleri yapmaktadır. Singapur'un ulusal bilgi altyapısını geliştirme yaklaşımı yalnızca yerel ihtiyaçlarla sınırlı kalmayıp, ekonomik stratejileriyle uyumlu olarak bölgesel ve küresel düzeyde genişlemektedir (Dijital Ekosistem, 2017). Siber tehditlerle mücadele için uluslararası kuruluşlarla işbirliği yapılmaktadır. Bu sayede küresel güvenlik ağları güçlendirilmektedir.

Singapur'da Bulut Servisi Sağlayıcıları (CPS'ler) için belirlenen "Çok Ayaklı Bulut Güvenliği" (MTCS) standardı, Bilgi Teknolojisi Standartları Komitesi (ITCS) altında geliştirilmiştir. Bu standardın oluşturulmasında, hükümet kurumları, üçüncü sektör kuruluşları, meslek kuruluşları ve bilgi teknolojileri endüstrisi arasındaki işbirliği çabaları önemli bir rol oynamıştır (Townsend, 2013). Bu süreç, fikir birliği temelinde ve güvenli bir veri altyapısı sağlamak amacıyla yürütülmüştür.

- Seul: U-City Konsepti

"Her zaman ve her yerde var olan şehir" anlayışıyla tanımlanan Güney Kore'deki U-Kent modeli, sürdürülebilir bir ekonomi oluşturmayı amaçlamakta olup; bu hedef, etkin iletişim, ulaşım altyapısı ve doğal kaynakların verimli yönetimi üzerine temellendirilmiştir. Akıllı şehirler, her zaman ve her yerde bulunan bilgi teknolojilerini etkin bir şekilde yönetir. Şehirdeki tüm bilgi sistemleri birbirine entegre edilmiş olup, neredeyse her şey kablosuz ağlar gibi teknolojilerle bir bilgi sistemine bağlanmaktadır. Seul, 1990'ların sonlarından itibaren geniş bant interneti başarılı bir şekilde kullanarak, tarihsel olarak bağlantılı şehirlerin örneklerinden biri olmuştur (Boz ve Çay, 2019).

Seul Büyükşehir Hükümeti (SMG), 1990'lı yıllarda e-hükümet programını başlatarak bu süreci başlatmıştır. Bu programın ilk aşamaları, hükümet veri tabanlarının oluşturulması, internet üzerinden kamu hizmetlerinin ve bilgilerin sağlanması ve bilişim teknolojileri (BİT) altyapısının güçlendirilmesi üzerine odaklanmıştır. 2011 yılına gelindiğinde, SMG,

vatandaşların mobil cihazları aracılığıyla hükümet hizmetlerine ve bilgilere ücretsiz erişimini sağlamak amacıyla Wi-Fi ve kapalı devre televizyon (CCTV) ağlarından oluşan yüksek hızlı bir telekomünikasyon ağı kurmuştur. Seul'de yürütülen akıllı şehir girişimleri; ulaşım (%20), kamu hizmetleri yönetimi (%20), kamu yönetimi (%13) ile turizm, kültür ve dinlenme (%12) gibi alanlarda yoğunlaşmaktadır. Bu hizmetler büyük ölçüde 2006 yılında kurulan Bilgi Teknolojileri (BT) departmanı üzerinden geliştirilmiş ve bu servislerin tekrarı engellenmek amacıyla akıllı şehir ekibi tarafından koordine edilmiştir. Seul'ün bu girişimleri, şehirdeki yaşam kalitesini artırmanın yanı sıra verimliliği ve sürdürülebilirliği sağlamayı da amaçlamaktadır (Bilici ve Babahanoğlu, 2018).

Seul, teknoloji ve inovasyonu desteklemek amacıyla çeşitli stratejik merkezler ve projeler geliştirmiştir. Bu merkezlerden biri olan Seongsu BT Merkezi, şehrin BT (bilgi teknolojisi) alanındaki yakınlaşmasını, biyoteknoloji endüstrisini ve araştırma-geliştirme (Ar-Ge) faaliyetlerini desteklemeyi hedeflemektedir. Bu merkez, Seul'ün teknoloji alanındaki liderliğini pekiştirmeyi amaçlayan önemli bir girişimdir. Seongsu BT Merkezi, özellikle biyoteknoloji ve bilgi teknolojisi sektörlerinin birleşiminden doğacak yenilikçi çözümler ile ekonomik büyümeyi hızlandırmayı hedefler (Tozkoparan, 2019).

Seul, akıllı şehir uygulamalarının bir parçası olarak çeşitli veri yönetimi düzenlemeleriyle dikkat çekmektedir. Bu düzenlemeler, şehrin veri kullanımını şeffaf, erişilebilir ve güvenli bir şekilde yönetmek amacıyla geliştirilmiştir (Boz ve Çay, 2019).

- Seul Veri Marketi Düzenlemesi: "Seul Veri Marketi", kamuya ait bilgilerin veri işlemeye açıldığı açık bir platformdur. Bu platformda, Seul Açık Veri Plazası aracılığıyla kaydedilen veriler, açık API formatında sunulmakta olup, geliştiriciler ve araştırmacılar tarafından kolayca erişilebilir hale getirilmektedir. Bu açık platform, kamuya ait verilerin şeffaf bir şekilde paylaşılmasına olanak sağlar ve bu verilerin çeşitli yenilikçi projeler için kullanılmasına zemin hazırlar.
- Büyük Veri Politikası Geliştirme: Seul Büyükşehir Hükümeti (SMG), politika geliştirmede Büyük Veri kullanımına büyük önem vermektedir. Şehir yönetimi, büyük veriden faydalanarak bilimsel analitikler geliştirmiş, bu sayede kişiselleştirilmiş idari hizmetler sunmuş ve kamu kaynaklarının israfını azaltmıştır. Bu yaklaşım, kamu hizmetlerinin daha etkin, verimli ve ihtiyaçlara yönelik hale gelmesine katkı sağlamaktadır. Bu süreç, şehirdeki çeşitli hizmetlerin daha doğru analiz edilmesine olanak tanımakta ve yerel yönetim kararlarını veri temelli bir şekilde yönlendirmektedir.

- Veri Gizliliği: 2011 yılında kabul edilen Kişisel Bilgilerin Korunması Yasası, kişisel verilerin korunmasına yönelik kapsamlı bir çerçeve sunmaktadır. Bu yasa, veri kontrolörlerinin yükümlülüklerini, veri sahiplerinin rızasına dayalı olarak kişisel verilere erişim haklarını ve verilerin toplanmasına itiraz etme hakkını düzenlemektedir. Aynı zamanda, kişisel bilgilerin güvenliğini sağlamak amacıyla çeşitli güvenlik gerekliliklerini de içermektedir. Bu yasal düzenleme, bireylerin gizliliğini ve verilerin güvenliğini teminat altına alarak, dijital dönüşümün sağlıklı bir şekilde gerçekleşmesini amaçlamaktadır.

2.4.2. Avrupa yaklaşımları

- Barselona – İspanya

Barselona, akıllı şehir olma yolunda önemli bir dönüşüm geçirmiştir ve bu süreç, teknolojinin ve sürdürülebilirliğin birleşimiyle şekillenmiştir. Akıllı şehir tanımında, şehirlerin üretken bölgeler oluşturması, günlük yaşam ritmiyle uyumlu, çevre dostu, doğallaştırılmış, enerji bakımından bağımsız ve emisyon oranı sıfırlanmış bir yapı oluşturması hedeflenir. Bu yapılar birbirine bağlı birimlerden oluşarak metropolde yüksek hızda iletişim sağlar. Barselona, akıllı şehir olma yolunda bu vizyonu benimsemiştir (Bulkeley ve Betsill, 2005). Akıllı şehri şekillendiren teknolojik temellerin atılması, 1980'lere dayanır. Bu dönemde, Barselona'da iki belediye binası arasında fiber optik hatların kurulması, şehrin bugünkü dijital altyapısının temelini oluşturmuştur. Bu altyapı, Barselona'nın modern ağ yapısının belkemiği haline gelmiş ve şehirdeki veri akışının verimli şekilde yönetilmesini sağlamıştır (Bulkeley ve Betsill, 2013).

Barselona'nın akıllı şehir olma süreci, 1992 Yaz Olimpiyatları'ndan sonra, şehre uluslararası bir etkileşim kazandırarak hız kazanmıştır. Bu dönemde, Barselona, sadece bir turistik destinasyon olmaktan çıkıp mobil dünya başkenti olarak adlandırılmaya başlanmış ve Avrupa'nın ilk akıllı şehirlerinden biri olarak öne çıkmıştır. 2010 ile 2015 yılları arasında, Barselona'da özel bir akıllı şehir ekibi kurulmuş ve şehirdeki çeşitli akıllı altyapı projeleri bir araya getirilerek şehir genelinde kapsamlı bir dijital dönüşüm süreci başlatılmıştır. Bu süreç, Barselona'nın kentsel planlamasını yeniden şekillendirirken, şehrin sürdürülebilirlik hedeflerini de güçlendirmiştir (Bibri ve Krogstie, 2017).

Barselona'nın akıllı şehir stratejisi, günümüzde şehri dijital altyapısının güçlü olduğu, sürdürülebilir uygulamaların ön planda olduğu ve yaşam kalitesini artıran bir şehir haline getirmeyi amaçlayan önemli bir modeldir. Barselona'nın Akıllı Şehir Politikaları, şehri verimli bir şekilde yönetmeye yönelik kapsamlı bir yaklaşım benimsemiştir. Bu yaklaşım, şehri üç merkezi bileşene ayıran Şehir Anatomisi modeli ile başlamaktadır: toplum, bilgi ve yapılar. Bu

model, şehrin farklı bileşenlerinin bir arada nasıl etkileşimde bulunduğunu ve nasıl birbirini desteklediğini anlamak için kullanılmıştır (Bulkeley ve Betsill, 2005). Böylece, şehirdeki paydaşlar, son kullanıcılar, bilgi akışları ve şehir servisleri arasındaki ilişkiler daha açık bir şekilde görselleştirilmiştir.

Akıllı Şehir alanları bu modelle belirlenmiş olup, şehri çeşitli kategorilere ayıran 12 ana alanı içermektedir. Aşağıdaki alanlar şehri yönetmeye yönelik çeşitli teknolojik, sosyal ve çevresel stratejilerin uygulanmasını sağlar (Bibri ve Krogstie, 2017):

- Açık Yönetim: Şeffaf ve katılımcı bir yönetim anlayışını benimsemek.
- Kamusal ve Toplumsal Hizmetler: Halkın ihtiyaçlarını karşılayan verimli kamu hizmetleri.
- Altyapılar: Şehrin fiziksel altyapısının sürdürülebilir ve verimli bir şekilde yönetilmesi.
- Şehir Ölçeği: Şehrin genel yapısının, büyüklüğünün ve gelişiminin yönetilmesi.
- Kamusal ve Özel Alanlar: Şehirdeki kamusal ve özel alanların dengeli bir şekilde düzenlenmesi.
- Bilgi ve İletişim Teknolojisi (BİT): Dijital altyapının güçlendirilmesi ve bilgi paylaşımının kolaylaştırılması.
- Su: Su kaynaklarının verimli kullanımı ve yönetimi.
- Enerji: Yenilenebilir enerji kaynaklarının entegrasyonu ve enerji verimliliği.
- Madde: Şehirdeki malzeme yönetimi ve geri dönüşüm süreçlerinin düzenlenmesi.
- Ulaşım: Ulaşım altyapısının iyileştirilmesi, akıllı ulaşım çözümleri.
- Doğa: Şehirdeki yeşil alanların korunması ve doğayla uyumlu gelişim.
- Çevre: Şehirdeki çevre kirliliğini azaltma, sürdürülebilir çevre politikaları.

Barselona'da, belirlenen 12 odak alanı doğrultusunda geliştirilen 22 program kapsamında, 100'ün üzerinde Akıllı Şehir projesi hayata geçirilmiştir (Bulkeley ve Betsill, 2005). Bu projeler, şehrin sürdürülebilirliğini artırmayı, yaşam kalitesini yükseltmeyi ve kaynakları verimli bir şekilde kullanmayı hedeflemektedir. Bu projeler sayesinde şehirdeki çeşitli sorunlara çözüm üretmek ve dijital dönüşüm sürecinde önemli adımlar atmak amaçlanmıştır. Bu projeler arasında ulaşımda akıllı çözümler, enerji verimliliği uygulamaları, atık yönetimi, çevre koruma, su tasarrufu gibi farklı alanlarda yapılan girişimler yer almaktadır.

- Kopenhag Danimarka

Kopenhag, sürdürülebilirlik ve yaşam kalitesi açısından akıllı şehir vizyonunu benimseyerek önemli stratejik adımlar atmıştır. Şehrin temel hedefleri arasında, karbon salınımını sıfıra indiren bir başkent olma, mavi ve yeşil alanlarla çevre dostu bir kent kimliği oluşturma, temiz ve sağlıklı bir yaşam ortamı sunma ile bisiklet dostu şehirler arasında lider konumda yer alma bulunmaktadır. Bu hedefler, Kopenhag'ın yaşam kalitesini artırmaya, çevresel etkilerini azaltmaya ve şehirdeki insanların sağlıklı bir yaşam sürmelerini sağlamaya yöneliktir. Kopenhag'ın akıllı şehir düşüncesi, kenti daha yaşanabilir ve sürdürülebilir bir hale getirmeyi amaçlayan bir araç olarak görülmektedir. Şehirdeki akıllı şehir geçmişi, 1971'de Danimarka hükümetinin ekolojik dostu politikalarla başlatılmıştır. Bu tarihten itibaren şehir, çevreye duyarlı politikalarla şekillenmeye başlamıştır Kopenhag'ın bugünkü sürdürülebilirlik yolculuğunun temellerini atmıştır (İTÜ Vakfı Yayını, 2019a).

Eko-metropol - Kopenhag 2015 vizyonu, şehri dünyadaki en iyi kentsel çevreye sahip yer haline getirmeyi amaçlayan bir plan olarak ortaya çıkmıştır. Bu vizyon, Kopenhag'ın akıllı şehir olma yolundaki ilk adımlarını attığı bir dönemi simgeler. Şehir konseyi, bu plan çerçevesinde çalışmalarına başladığında, şehirdeki sürdürülebilirlik ve çevre dostu yaklaşım her geçen yıl daha belirginleşmiştir (Çevre ve Şehircilik Bakanlığı, 2019b). Kopenhag'ın akıllı şehir olma yolundaki daha somut adımları ise, 2010'ların sonlarına doğru atılmaya başlanmıştır. 2014 yılında Kopenhag'da ilk akıllı şehir konseyi kurulmuş ve bu konseyi, şehirdeki yedi farklı yönetim birimini koordine etmekle sorumlu kılınmıştır. Bu konsey, aynı zamanda açık veri ve dijital altyapı projelerine öncülük ederek şehirdeki dijital dönüşüm sürecine katkı sağlamıştır.

Kopenhag'ın bu girişimleri, şehri yalnızca bir akıllı şehir değil, aynı zamanda çevre dostu, sosyal açıdan sürdürülebilir ve ekonomik olarak verimli bir yer haline getirmeyi amaçlamaktadır. Bu doğrultuda, akıllı şehir politikaları, ulaşımda, enerji kullanımında, atık yönetiminde ve şehir altyapısının genelinde dijital ve sürdürülebilir çözümler geliştirmeyi hedeflemektedir (Ahvenniemi vd., 2017). Kopenhag, dünyanın en yaşanabilir şehirlerinden biri olmayı sürdürürken, aynı zamanda çevre dostu teknolojileri ve dijital yenilikleri kullanarak daha sürdürülebilir bir gelecek için önemli bir model oluşturmuştur.

Kopenhag, temiz teknoloji alanında öncü bir şehir olarak, akıllı şehir çözümleri ve siber güvenlik alanlarında önemli adımlar atmıştır. 2009 yılında kurulan Kopenhag Temiz Teknoloji Grubu (CCC), temizlik teknolojilerinin araştırılması, geliştirilmesi ve uygulanmasına yönelik uygun iş ortamlarını oluşturmayı hedefleyen küresel ölçekte etkili bir girişim olarak öne çıkmaktadır (Ahvenniemi vd., 2017). Bu grup, Kopenhag'ın çevresel verimliliğini artırmayı ve sürdürülebilir şehir çözümleri geliştirmeyi hedeflerken, aynı zamanda Danimarka'nın

teknolojilerinin dünyanın dört bir yanındaki akıllı ve eko şehirlerde uygulanmasını sağlamaktadır (İTÜ Vakfı Yayını, 2019a). CCC, bu stratejiyle, çevresel etkileri en aza indirgemek ve daha yaşanabilir şehirler inşa etmek için önemli katkılar sunmaktadır.

Danimarka'nın enerji politikalarını desteklemek amacıyla kurulan Akıllı Enerji Danimarka Ortaklık Ağı, ülkenin enerji çözüm ihtiyaçlarını karşılamada katalizör rolü oynamaktadır. Bu kamu-özel sektör ortaklığı, enerji verimliliğini artıran projeler ve çözümler geliştirmek için ulusal düzeydeki iş birliklerini güçlendirmeyi amaçlamaktadır. Özellikle çevresel ve dijital endüstrilerdeki güçlü performansıyla Danimarka, Avrupa'da bu alandaki en önde gelen ülkeler arasında yer almaktadır. Kopenhag'da ayrıca, özel sektör, kamu sektörü ve akademik dünyadan paydaşları bir araya getiren Akıllı Şehir Siber Güvenlik Laboratuvarı (CSL) kurulmuştur. CSL'nin temel amacı, akıllı şehir hizmetlerinin güvenliğini sağlamak ve bu hizmetlerin gizliliğini korumaktır. Kentsel verilerin toplanması ve erişimi için standartlar ve en iyi uygulamalar belirlenerek şehir altyapılarının siber saldırılara karşı korunması sağlanmaktadır (Ahvenniemi vd., 2017). Şehirlerin dijital dönüşümünü güvenli bir şekilde ilerletirken veri güvenliğinin sağlanmasını ve gizliliğin korunmasını da garanti altına almaktadır.

Kopenhag'ın akıllı şehir vizyonunun temel bileşenlerinden biri olan Şehir Verileri Alışverişi sistemi, şehir genelindeki tüm paydaşlar arasında veri paylaşımını kolaylaştıran bütüncül bir platform sunmaktadır. Bu sistem aracılığıyla verilerin kamu kurumları ve özel sektör tarafından erişilebilir ve kullanılabilir hale getirilmesi, kent yönetiminde daha isabetli ve verimli kararların alınmasına olanak tanımaktadır. Bu sistem, şehri daha etkili yönetmenin yanı sıra, yaşam kalitesini artırmaya yönelik veriye dayalı çözümler geliştirilmesine olanak tanımaktadır.

- Berlin – Almanya

Berlin, hızlı kentleşme sürecinin getirdiği zorlukları aşmak amacıyla ulaşım, enerji, sağlık, altyapı ve binalar gibi alanlarda akıllı çözümler geliştirmeye odaklanmaktadır. 2030 yılına kadar şehir nüfusunun en az 500,000 artacağı tahmin edilmektedir (Bulkeley ve Betsill, 2005). Bu durum Berlin'i akıllı şehir çözümlerine yatırım yapmaya teşvik etmektedir. Berlin'in akıllı şehir olma yolunda sahip olduğu bazı benzersiz avantajlar vardır. Almanya'nın başkenti, en büyük şehri ve aynı zamanda en önemli siyasi, sosyal ve kültürel merkezidir (Harrison ve Donnelly, 2011). Bu özellikleri, Berlin'i bölgesel ve küresel anlamda bir teknoloji ve yenilik merkezi haline getirmektedir. Şehir, araştırma ve geliştirme (Ar-Ge) faaliyetlerine ve büyük

ölçekli kentsel gelişim projelerine yılda yaklaşık 1.5 milyar Euro yatırım yapmaktadır (Herzberg, 2017).

Berlin'in akıllı şehir stratejisi"nin ana hedefleri, sınırlı kaynakların daha verimli kullanılmasını sağlamak, yenilenebilir enerji kaynaklarının yaygınlaşmasını desteklemek, 2050 yılına kadar kaynak verimliliği ve iklim nötralitesinde önemli bir artış sağlamak ve yoğun nüfuslu kentsel bir ortamda yaşamın olumsuz etkilerini en aza indirmektir. Bu hedefler doğrultusunda çevresel sürdürülebilirliği artırmayı ve vatandaşların yaşam kalitesini iyileştirmeyi amaçlamaktadır (Harrison ve Donnelly, 2011). Akıllı şehir çözümleri, sadece şehirdeki altyapıyı iyileştirmekle kalmayacak, aynı zamanda Berlin'in karşı karşıya olduğu kentleşme, çevre ve sosyal eşitsizlik gibi sorunlarla mücadele için de güçlü araçlar sunacaktır.

Federal hükümet, Almanya'nın gelecekteki sürdürülebilirliğini ve yaşanabilirliğini tartışmak amacıyla uzmanları davet ederek "Geleceğin Şehri için Ulusal Platform"u kurmuş ve 2015 Bilim Yılı'nın lansmanını, geleceğin şehirleri için bir araştırma ve inovasyon ajandası sunmak için bir fırsat olarak kullanmıştır. Ulusal seviyede çeşitli stratejik örnekler, bu platformun etkinliğini pekiştiren girişimler arasında yer alır. Bunlar arasında Ulusal Platform, Dijital Almanya 2015 ve Ulusal e-yönetim Stratejisi öne çıkmaktadır (Herzberg, 2017).

Şehir ölçeğinde Berlin, Paris ve Bologna gibi kentler, Avrupa Birliği'nin 2015 yılında yayımladığı Akıllı Şehirler Çağrısı'na yanıt vererek, dijital altyapı ile tamamen entegre olmuş şehir yapıları oluşturma ve sürdürülebilir enerji ile ulaşım çözümlerine geçişi destekleyen stratejik öneriler geliştirmiştir. Berlin, bu alanda bir "yol gösterici şehir" olma yolunda önemli adımlar atmıştır. Bu çerçevede Berlin'in akıllı şehir stratejileri arasında Berlin Senatosu'nun Akıllı Şehir Stratejisi, Kentsel Gelişim Konsepti Berlin 2030 ve Berlin Enerji ve İklim Koruma Programı gibi önemli planlar bulunmaktadır (Dijital Ekosistem, 2017). Bu stratejiler, şehrin gelecekteki sürdürülebilir kalkınma hedeflerine ulaşmasını sağlamak için kapsamlı bir yol haritası sunmaktadır.

- Paris – Fransa

Dünyadaki çeşitli akıllı şehir modelleri arasında Paris, kendine özgü bir yol izlemektedir. Diğer akıllı şehirlerden farklı olarak, Paris'in yaklaşımı, bağlantılı ve sürdürülebilir bir şehir inşa etmenin yanı sıra, bu hedeflere ulaşmak için açık inovasyonu benimsemektedir. Paris, Akıllı Şehir girişimini, şehrin uzun tarihine dayanan bir inovasyon geleneğinin parçası olarak görmekte ve bu gelenekle uyumlu bir şekilde hareket etmektedir.

Resmi Akıllı Şehir stratejisi, "Akıllı ve Sürdürülebilir Paris" adıyla 2015 yılında yayınlanmıştır (Boz ve Çay, 2019).

2014 yılında başlatılan katılımcı bütçe programı, şehrin halkının aktif katılımını teşvik etmek amacıyla tasarlanmıştır. Bu program çerçevesinde, şehir bütçesinin %5'lik bir kısmı, vatandaşların katılımıyla belirlenen projelere ayrılmaktadır. 2020 yılına kadar bu miktarın 500 milyon euro seviyelerine ulaşması beklenmektedir. Paris'in Akıllı Şehir stratejisinin odaklandığı ana alanlar, daha fazla start-up çekmek, dinamik bir girişimci topluluğu oluşturmak ve uluslararası ortaklıklar kurmaktır. Paris, San Francisco gibi diğer şehirlerle işbirlikleri geliştirmeyi hedeflemektedir (Bilici ve Babahanoğlu, 2018).

Paris'in Akıllı Şehir stratejisi, üç temel şehir modelini birleştirerek şehri daha verimli, sürdürülebilir ve yaşanabilir bir hale getirmeyi amaçlamaktadır (Boz ve Çay, 2019):

- Açık Şehir: Bu model, işbirlikçi yöntemlere dayanarak, kent sakinlerinin, ekonomik aktörlerin ve yönetimin kolektif zekâsına dayanmaktadır. Bu sayede şehri geliştirme süreci, toplumun çeşitli paydaşlarının katılımıyla şekillendirilir.
- Yetenekli Şehir: Bu yaklaşım, kentsel ağların nasıl işlediğini, planlandığını ve aktığını sorgulayarak kaynakları en verimli şekilde kullanmayı ve tasarruf sağlamayı amaçlar. Kentsel hizmetlerin ve altyapının optimize edilmesine odaklanır.
- Bağlantılı Şehir: Teknolojik modernleşmeyi ve ilerici altyapıyı destekler. Kullanıcıların ihtiyaçlarına uyarlanmış dijital servisler ve platformlar, birlikte çalışabilirliği ve paylaşımı teşvik eder.

Paris'te bu stratejilerin uygulaması, belediye başkanlığı tarafından öncülük edilmekte ve hükümet görevlileri ile yerli ve yabancı paydaşlardan oluşan bir Akıllı Şehir Ortaklar Komitesi ile düzenli toplantılar ve yıllık strateji komite toplantıları ile şekillendirilmektedir. Fransa'nın Geleceğin Endüstrisi Stratejisi, endüstriyel yeniden canlanmayı hedefleyen bir yol haritası sunar. Bu strateji, Akıllı Şehirler, eko-hareketlilik, veri ekonomisi ve dijital güvenlik gibi alanları içerir. Fransa'daki şehirlerin aksine, bu strateji, Akıllı Şehir çözümleri geliştiren Fransız kurumlarına odaklanmaktadır. Stratejinin amacı, inovasyonu ve ulusal ekonomiyi desteklemektir. Dijital Şehir Master Planı, Akıllı ve Sürdürülebilir Paris planının desteklenmesi için gerekli bilgi ve teknoloji stratejilerini açıklar. Bu planın başlıca hedefleri arasında dijital eşitsizlikle mücadele etmek, şehir servislerine farklı erişim kanallarını kişiselleştirmek ve maliyetleri azaltırken verimliliği artırmak yer almaktadır. Ayrıca, şehrin açık veri politikasını da destekler. Akıllı Şehir girişimleriyle ilgili standartlar, Association Francaise de

Normalisation (AFNOR) tarafından yönetilmektedir. AFNOR, dijitalleşme, dijital ekonomi, iklim ve çevre ile ilgili standartların benimsenmesini önceliklendirmiştir. Ayrıca AFNOR, ISO/TC 268 Sürdürülebilir Şehirler ve Topluluklar standartlarının geliştirilmesine yardımcı olmaktadır (Boz ve Çay, 2019).

2.4.3. Amerika modelleri

- San Francisco: Teknoloji Ekosistemi Entegrasyonu

San Francisco, teknoloji ve sürdürülebilirlik alanlarında küresel bir lider olarak, vatandaşları ve iş dünyasıyla önemli bir etki yaratmaktadır. Şehir, aynı zamanda gelir eşitsizliği, uygun fiyatlı konut, işe gidip gelme süreleri ve iklim değişikliği gibi önemli sorunlarla mücadele etmektedir (Herzberg, 2017). San Francisco'nun Akıllı Şehir statüsü, karşılaştığı zorlukları aşarak ve çeşitli girişimler başlatarak zamanla organik bir şekilde şekillenmiştir.

1996–2004 yılları arasında San Francisco Belediye Başkanlığı görevini yürüten Willie Brown, internet şirketlerinin hızlı yükselişi ve teknoloji yatırımlarının artışı doğrultusunda kentin küresel ölçekte bir teknoloji merkezi haline geleceğini öngörmüştür. Onun ardından göreve gelen Belediye Başkanı Gavin Newsom, çevresel sorunlara yönelik aktif politikalar geliştirmiş ve bu çabaları sayesinde kamuoyunda "Amerika'nın En Yeşil Belediye Başkanı" olarak anılmıştır. Günümüzde ise Belediye Başkanı Daniel Lurie, kentin teknoloji odaklı gelişim süreci ile çevresel duyarlılığını bir araya getirerek, San Francisco için daha bütüncül ve akıllı şehir çözümleri üretmeye yönelik stratejiler geliştirmektedir (Deloitte, 2016). Şehir, bir sonraki aşamasında, çok sayıda kişinin aktif rol alacağı ve çabaların disiplinler arası nitelik taşıyacağı Akıllı Şehir 2.0 uygulamasını hedeflemektedir. Şehri daha sürdürülebilir ve teknolojik açıdan daha entegre bir hale getirmeyi amaçlamaktadır.

Akıllı şehir planlaması ve politikalarını destekleme, çeşitli ulusal ve şehir düzeyinde uygulamalarla şekillenmektedir. Ulusal düzeyde, teknoloji uzmanları, araştırmacılar ve toplulukları bir araya getiren Beyaz Saray Akıllı Şehir Girişimi, bu alandaki işbirliklerini güçlendiren önemli bir platformdur. Bu girişim kapsamında desteklenen bazı programlar arasında Ulusal Bilim Vakfı'nın siber-fiziksel sistemler üzerine yaptığı araştırmalar, İç Güvenlik Bakanlığı'nın müdahale teknolojileri programı ve Ulaştırma Bakanlığı'nın birbirine bağlı araçlar programı yer almaktadır (Deloitte, 2016).

Şehir düzeyinde ise başkanlığın bütçe teklifleri, şehir vizyonunu ve odak alanlarını belirleyerek kamu fonlarının tahsis edilmesini sağlar. Örnek olarak, Bilgi ve Haberleşme Teknolojileri Planı, kentsel hizmetlerin iyileştirilmesini hedefleyen ve Bilişim Teknolojisi

Komitesi (COIT) tarafından izlenen projeleri tanımlar. Ayrıca, San Francisco'nun İnovasyon Modeli, şehir yönetiminde yeniliği teşvik etmek için Sivil Yenilikler Başkanlık Ofisi (MOCI) tarafından geliştirilmiş bir araçtır. Standartlar bakımından ise, 80X50 hedefi, 2050 yılına kadar karbon emisyonlarında %80 azalma sağlamayı amaçlayan bir çerçeve sunmaktadır. San Francisco, çevre dostu yeşil binaları teşvik eden yönetmelikler uygulamaktadır ve tüm belediye binaları için LEED Gold başarı standardına ulaşmayı hedeflemektedir. Ayrıca, ENERGY STAR sertifikası, 10.000 kare fitin üzerindeki tüm binaların uyması gereken bir standarttır. San Francisco, Kyoto Protokolü'nün hedeflerine ulaşmayı bağımsız bir şekilde taahhüt etmiştir (Herzberg, 2017). Bu tür standartlar, şehri sürdürülebilirlik ve çevresel sorumluluk açısından daha ileriye taşımaktadır.

- New York: Veri Odaklı Yönetişim

New York City'nin OneNYC stratejisi, sürdürülebilirlik, dayanıklılık, eşitlik ve büyüme hedeflerini entegre eder. Mayor's Office of Data Analytics (MODA), şehir genelindeki veri entegrasyonu ve analitiği koordine eder. NYC Open Data portalı, 2.700'den fazla veri setini paylaşır.

LinkNYC, telefon kulübelerini ücretsiz WiFi, şarj istasyonu ve bilgi kiosku sunan dijital bağlantı noktalarına dönüştüren dünyanın en büyük kentsel iletişim ağıdır. 1.800'den fazla Link kiosku kurulmuştur. NYC311, vatandaşların şehir hizmetlerine 24/7 erişim sağladığı entegre hizmet platformudur.

FireCast, yangın riski tahmin modeli olarak makine öğrenmesi kullanarak binaları risk seviyelerine göre sınıflandırır. NYC Connected Communities programı, dijital uçurumu kapatmak için düşük gelirli mahallelere ücretsiz internet erişimi sağlar. Hudson Yards, sensörler ve veri analitiği kullanan akıllı mahalle projesidir.

2.4.4. Karşılaştırmalı model analizi

Küresel akıllı şehir modellerinin karşılaştırmalı analizi, farklı yaklaşımların güçlü ve zayıf yönlerini ortaya koymaktadır. Asya-Pasifik modelleri genellikle merkezi planlama, büyük ölçekli altyapı yatırımları ve hızlı uygulama kapasitesiyle öne çıkar. Singapur'un yukarıdan aşağıya yaklaşımı, kapsamlı dijital dönüşüm sağlarken, veri mahremiyeti ve gözetim konularında endişeler yaratmaktadır.

Avrupa modelleri, vatandaş katılımı, sürdürülebilirlik ve veri koruma konularına öncelik verir. Barcelona'nın teknolojik egemenlik vurgusu, yerel inovasyon kapasitesini güçlendirirken, Amsterdam'ın bottom-up yaklaşımı toplumsal sahiplenmeyi artırır.

Kopenhag'ın sürdürülebilirlik odağı, çevresel hedeflerle teknolojik yeniliği başarıyla entegre eder.

Amerika modelleri, özel sektör işbirliği ve veri odaklı yönetişimde güçlüdür. San Francisco'nun startup ekosistemiyle entegrasyonu hızlı inovasyon sağlarken, New York'un veri analitiği kapasitesi kanıta dayalı politika geliştirmeyi destekler. Ancak, dijital eşitsizlik ve özelleştirme riskleri önemli zorluklar oluşturur.

2.5. TÜRKİYE'DE AKILLI ŞEHİR UYGULAMALARI VE STRATEJİLER

Bu bölümde Türkiye'de akıllı şehir yaklaşımının kurumsal, yerel ve stratejik boyutları ele alınmaktadır. Ulusal politika çerçevesi ve stratejik planlama süreçleri incelenerek devletin akıllı şehir vizyonu ve bu vizyonu destekleyen yasal, idari düzenlemeler değerlendirilecektir. Büyükşehir belediyeleri tarafından yürütülen akıllı şehir projeleri örnekler üzerinden tartışılacak ve yerel yönetimlerin bu süreçteki rolü ortaya konulacaktır.

2.5.1. Ulusal politika çerçevesi ve stratejik planlama

Türkiye'nin akıllı şehir vizyonu, 2024-2030 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı ile sistematik bir çerçeveye oturtulmuştur. Bu strateji, "yaşanabilir ve sürdürülebilir şehirler" vizyonuyla, altı temel stratejik amaç belirlemiştir: yönetişim ve yönetim, ekonomi ve finans, altyapı, çevre, insanlar ve yaşam. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı koordinasyonunda yürütülen strateji, 2030 yılına kadar tüm büyükşehirlerin ve il merkezlerinin akıllı şehir dönüşümünü tamamlamasını hedeflemektedir. Yerel bağlamda ise Türkiye Belediyeler Birliği, akıllı şehir dönüşümünde yerel yönetimlere rehberlik etmek üzere Akıllı Şehir Yol Haritası hazırlamıştır. Bu yol haritası, belediyelerin dijital olgunluk seviyelerini değerlendiren, önceliklendirme kriterleri sunan ve uygulama adımlarını tanımlayan pratik bir kılavuz niteliğindedir.

Novusens İnovasyon ve Girişimcilik Enstitüsü bünyesindeki Akıllı Şehir Enstitüsü tarafından, Türkiye Bilişim Vakfı ve İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Fakültesi iş birliğinde, Mastercard ve Intel'in desteğiyle hazırlanan "Türkiye Akıllı Şehirler Değerlendirme Raporu"na göre; akıllı kent yaklaşımı çerçevesinde gerçekleştirilen uygulamaların %36'sı ulaşım, %34'ü su yönetimi ve %21'i enerji ile ilişkili alanlarda yoğunlaşmaktadır. Geriye kalan %9'luk kısımda ise Coğrafi Bilgi Sistemleri (CBS) ve elektronik ödeme çözümleri öne çıkan başlıklar arasında yer almaktadır. Raporda yer alan verilere göre, envanter çalışmasına katılan 25 büyükşehir belediyesinin 20'si su yönetimi, 18'i ise ulaşım alanında akıllı kent uygulamaları yürüttüklerini ifade etmiştir (Gürsoy, 2019).

Özellikle Ankara, İstanbul, İzmir, Konya ve Antalya gibi büyükşehirlerde geliştirilen pilot uygulamalar, dijital altyapıların kentsel hizmetlerle entegrasyonu açısından dikkat çekici örnekler sunmaktadır (Akgül, 2013; Aydınbaş, 2023).

2.5.2. Büyükşehir belediyelerinin akıllı şehir projeleri

- İstanbul: Mega Kent Yaklaşımı

İstanbul Büyükşehir Belediyesi, "Big Smart Istanbul" vizyonuyla Türkiye'nin en kapsamlı akıllı şehir programını yürütmektedir. İSBAK (İstanbul Bilişim ve Akıllı Kent Teknolojileri A.Ş.), şehrin akıllı şehir projelerini koordine eden ve uygulayan kuruluş olarak faaliyet göstermektedir. İstanbul'un akıllı şehir stratejisi, mega kentin karmaşık sorunlarına entegre çözümler geliştirmeyi hedeflemektedir (Gürsoy, 2019).

İstanbul Akıllı Trafik Sistemleri (İSTKA), 7.500 km'lik yol ağında 156 kavşakta adaptif sinyal kontrolü, 2.400 kamera ile trafik izleme ve 450 değişken mesaj işareti ile sürücü bilgilendirme sağlar. İBB Cep Trafik uygulaması, 5 milyondan fazla kullanıcıya gerçek zamanlı trafik bilgisi sunar. Yol Gösteren uygulaması, toplu taşıma rotalarını optimize eder ve 3 milyon aktif kullanıcıya sahiptir.

İstanbul Büyükşehir Belediyesi Coğrafi Bilgi Sistemi (İBB CBS), 3D şehir modeli, 1:1000 ölçekli sayısal haritalar ve 500'den fazla katman veri içeren kapsamlı mekansal veri altyapısı sunmaktadır. Kent Bilgi Sistemi, şehir planlama, altyapı yönetimi ve afet hazırlığı için kritik veriler sağlar. İBB Açık Veri Portalı, 150'den fazla veri setini araştırmacılar ve geliştiricilerle paylaşmaktadır.

İSKİ'nin SCADA sistemi, 23 içme suyu arıtma tesisi, 87 atık su arıtma tesisi ve 50.000 km'lik şebekeyi uzaktan izler ve kontrol eder. Akıllı sayaç projesi kapsamında 500.000'den fazla sayaç uzaktan okunabilir hale getirilmiştir. İstanbul WiFi projesi, 1.200'den fazla noktada ücretsiz internet erişimi sağlamaktadır. Beyazmasa uygulaması, e-belediyecilik hizmetlerini dijital platforma taşımıştır.

- Ankara: Başkent Modeli

Ankara Büyükşehir Belediyesi, "Dijital Başkent" vizyonuyla akıllı şehir dönüşümünü gerçekleştirmektedir. Ankara Akıllı Şehir Stratejisi 2025, beş ana eksende (akıllı yönetişim, akıllı ekonomi, akıllı yaşam, akıllı mobilite, akıllı çevre) 75 proje tanımlamıştır. BELTEK (Ankara BŞB Teknoloji A.Ş.), şehrin teknoloji projelerini yürütmektedir.

Başkent Mobil uygulaması, 100'den fazla belediye hizmetini tek platformda sunarak 2 milyon kullanıcıya ulaşmıştır. EGO Cepte uygulaması, toplu taşıma araçlarının gerçek zamanlı takibi, rota planlama ve dijital ödeme imkanları sunar. Ankara Akıllı Trafik Yönetim Merkezi, 850 kavşakta trafik kontrolü, 1.500 kamera ile izleme ve dinamik yönlendirme sağlar.

ASKİ Akıllı Su Yönetimi Sistemi, 2.5 milyon aboneye hizmet veren su altyapısını dijital platformda yönetir. Uzaktan okunan sayaçlar, kaçak tespit sistemleri ve su kalitesi izleme sensörleri entegre edilmiştir. Ankara Yeşil Şehir Projesi, 150 parkta akıllı sulama sistemleri, 500 noktada hava kalitesi sensörleri ve enerji verimli aydınlatma sistemleri kurmuştur.

- İzmir: Akdeniz Akıllı Şehri

İzmir Büyükşehir Belediyesi, "Akdeniz'in Akıllı Şehri" vizyonuyla, sürdürülebilirlik ve yaşam kalitesine odaklanan projeler geliştirmektedir. İzmir Akıllı Şehir Stratejisi, Akdeniz iklimi ve kıyı şehri özelliklerini dikkate alan özgün çözümler üretmektedir. İZBELKOM, şehrin bilişim altyapısını yönetmektedir.

İzmir Akıllı Ulaşım Sistemi (İZULAŞ), 420 km metro ve tramvay hattı, 1.800 otobüs ve 40 vapur ile entegre mobilite çözümleri sunar. İzmirim Kart, 3.5 milyon kullanıcıyla çoklu ulaşım modlarında kullanılabilen akıllı kart sistemidir. Bisim bisiklet paylaşım sistemi, 2.500 bisiklet ve 140 istasyonla hizmet vermektedir.

İZSU'nun Akıllı Su Yönetimi, SCADA sistemleriyle 9.000 km su şebekesini izler. Körfez İzleme Sistemi, İzmir Körfezi'nin su kalitesini 24 istasyonda sürekli ölçer. İzmir Deprem Master Planı kapsamında, 120 ivmeölçer istasyonu kurulmuş, Erken Uyarı Sistemi geliştirilmiştir. HİM (Hemşehri İletişim Merkezi), vatandaş taleplerini 7/24 alarak ortalama 48 saat içinde çözüme kavuşturmaktadır.

- Bursa: Endüstri 4.0 Entegrasyonu

Bursa Büyükşehir Belediyesi, sanayi kenti kimliğiyle uyumlu olarak Endüstri 4.0 teknolojilerini kentsel hizmetlerle entegre etmektedir. Bursa Akıllı Şehir Yol Haritası, özellikle akıllı üretim, lojistik ve enerji yönetimi alanlarında projeler geliştirmektedir.

BursaRay Akıllı Metro Sistemi, 39 km hat uzunluğu ve günlük 300.000 yolcu kapasitesiyle sürücüsüz metro teknolojisini kullanmaktadır. BURULAŞ tarafından işletilen sistem, enerji verimliliği ve tahminsel bakım sistemleriyle donatılmıştır. Bursa Trafik Kontrol Merkezi, 450 kavşakta akıllı sinyalizasyon ve 800 kamerayla trafik yönetimi sağlamaktadır.

BUSKİ Akıllı Su Yönetimi, 1.8 milyon aboneye hizmet veren altyapıda %25 su kaybını önlemeyi hedeflemektedir. Bursa 3D Kent Modeli, şehrin tamamını kapsayan fotogrametrik haritalar ve lazer tarama verileriyle oluşturulmuştur. Mobil Bursam uygulaması, 80'den fazla belediye hizmetini dijital platforma taşımıştır.

- Antalya: Akıllı Turizm Destinasyonu

Antalya Büyükşehir Belediyesi, turizm odaklı akıllı şehir stratejisiyle, ziyaretçi deneyimini iyileştiren ve sürdürülebilir turizmi destekleyen projeler yürütmektedir. Antalya Akıllı Destinasyon Yönetimi, turist akışlarını optimize eder ve taşıma kapasitesini yönetir.

AntalyaKart, toplu taşıma, müze girişleri, otopark ve bisiklet paylaşımında kullanılabilen entegre kart sistemidir. Antalya Akıllı Turizm Platformu, 12 dilde mobil uygulama, sanal tur ve artırılmış gerçeklik deneyimleri sunar. Plaj yönetim sistemi, 630 km sahil şeridinde su kalitesi, doluluk oranı ve güvenlik parametrelerini izler.

ASAT Akıllı Altyapı Yönetimi, turizm bölgelerinde kesintisiz hizmet sağlamak için kritik altyapıları 7/24 izler. Antalya Akıllı Tarım Projesi, 50.000 hektar sera alanında IoT sensörleri ve drone teknolojisi kullanarak verimlilik artışı sağlamaktadır.

Konya: Akıllı Tarım ve Sanayi Kenti

- Konya Büyükşehir Belediyesi, tarım ve sanayi potansiyelini akıllı teknolojilerle güçlendiren projeler geliştirmektedir. Konya Akıllı Şehir Vizyonu 2030, özellikle akıllı tarım, su yönetimi ve yenilenebilir enerji alanlarına odaklanmaktadır.

Konya Akıllı Tarım Vadisi, 2 milyon hektar tarım arazisinde hassas tarım teknolojileri, drone görüntüleme ve toprak sensörleri kullanmaktadır. KOSKİ Akıllı Su Yönetimi, Konya Kapalı Havzası'nda su kaynaklarının sürdürülebilir kullanımı için dijital izleme sistemleri kurmuştur.

Konya Bilim Merkezi ve Akıllı Şehir Laboratuvarı, yerel inovasyon ekosistemini güçlendirmektedir. Konya Enerji Parkı, 100 MW güneş enerjisi kapasitesiyle şehrin elektrik ihtiyacının %15'ini karşılamaktadır. Mevlana Kültür Vadisi Akıllı Turizm Projesi, dijital rehberlik ve çok dilli bilgi sistemleri sunmaktadır.

2.5.3. Türkiye modelinin değerlendirilmesi

Türkiye'nin akıllı şehir yaklaşımı, kendine özgü güçlü yönler ve gelişim alanları barındırmaktadır. Güçlü yönler arasında, genç ve dinamik nüfus yapısı, gelişmiş telekomünikasyon altyapısı, e-devlet sisteminin yaygın kullanımı ve yerel yönetimlerin

teknolojiye yatırım istekliliği sayılabilir. E-devlet kapısı üzerinden sunulan 5.800'den fazla hizmet ve %75'lik kullanım oranı, dijital dönüşüm için güçlü bir temel oluşturmaktadır.

Coğrafi konum avantajı, Türkiye'yi Avrupa, Asya ve Afrika arasında akıllı şehir teknolojileri için köprü konumuna getirmektedir. Yerli teknoloji üretimi kapasitesinin gelişmesi, özellikle savunma sanayii, elektronik ve yazılım sektörlerindeki başarılar, akıllı şehir çözümlerinin yerelleştirilmesi için fırsat yaratmaktadır.

Ancak, Türkiye'nin akıllı şehir dönüşümünde karşılaştığı zorluklar da mevcuttur. Bunların başında, farklı kurumlar arasında koordinasyon eksikliği, standartlaşma ve birlikte çalışabilirlik sorunları gelmektedir. Veri paylaşımı konusundaki kurumsal dirençler, entegre çözümlerin geliştirilmesini zorlaştırmaktadır.

Finansman modelleri konusunda belirsizlikler, özellikle yerel yönetimlerin bütçe kısıtları, büyük ölçekli projelerin hayata geçirilmesini engellemektedir. Kamu-özel sektör işbirliği mekanizmalarının yetersizliği, inovasyon ekosisteminin gelişimini yavaşlatmaktadır. Dijital okuryazarlık seviyesindeki bölgesel farklılıklar, akıllı şehir hizmetlerinden yararlanmada eşitsizlikler yaratmaktadır.

Siber güvenlik kapasitesinin güçlendirilmesi ihtiyacı, kritik altyapıların korunması açısından öncelikli konudur. Veri mahremiyeti ve kişisel verilerin korunması konusundaki toplumsal farkındalığın artırılması gerekmektedir. Akıllı şehir projelerinin sosyal etki değerlendirmelerinin yapılmaması, toplumsal kabul ve sahiplenme sorunlarına yol açmaktadır.

Türkiye'nin akıllı şehir modelinin geliştirilmesi için öneriler arasında, ulusal akıllı şehir standartlarının belirlenmesi ve uygulanması, merkezi bir akıllı şehir veri platformunun kurulması, yerel yönetimlere teknik destek ve kapasite geliştirme programlarının sunulması yer almaktadır. Living lab yaklaşımıyla pilot bölgelerin oluşturulması, yenilikçi çözümlerin test edilmesi için önemlidir.

Üniversite-sanayi-kamu işbirliğinin güçlendirilmesi, Ar-Ge faaliyetlerinin desteklenmesi ve teknoloji transfer mekanizmalarının geliştirilmesi, yerli akıllı şehir teknolojilerinin üretimini teşvik edecektir. Vatandaş katılımı mekanizmalarının güçlendirilmesi, dijital platformlar üzerinden geri bildirim ve öneri sistemlerinin kurulması, toplumsal sahiplenmeyi artıracaktır.

Uluslararası işbirlikleri ve deneyim paylaşımı, Türkiye'nin küresel akıllı şehir ağlarına entegrasyonunu sağlayacaktır. AB Horizon Europe, Smart Cities Mission gibi uluslararası programlara katılım, teknoloji transferi ve finansman imkanları yaratacaktır. Türkiye'nin akıllı

şehir deneyiminin, özellikle Orta Asya, Orta Doğu ve Afrika ülkeleriyle paylaşılması, bölgesel liderlik potansiyelini güçlendirecektir.

Sonuç olarak, Türkiye'nin akıllı şehir yolculuğu, küresel trendlerle yerel ihtiyaçların dengeli bir sentezini gerektirmektedir. Teknolojik altyapının güçlendirilmesi kadar, kurumsal kapasitenin geliştirilmesi, toplumsal farkındalığın artırılması ve sürdürülebilir finansman modellerinin oluşturulması kritik başarı faktörleridir. Akıllı şehir dönüşümü, sadece teknoloji yatırımı değil, aynı zamanda yönetişim reformu, sosyal inovasyon ve kültürel değişim sürecidir. Bu bütüncül yaklaşımla, Türkiye'nin akıllı şehirleri, vatandaşların yaşam kalitesini artıran, sürdürülebilir kalkınmayı destekleyen ve küresel rekabet gücünü güçlendiren platformlar haline gelecektir.

3. AKILLI ŞEHİRLERDE GÜVENLİK TEKNOLOJİLERİ VE SİSTEMLERİ

Akıllı şehirlerin sürdürülebilir ve etkin bir şekilde işleyebilmesi için kritik öneme sahip olan güvenlik teknolojileri ve sistemleri ele alınmaktadır. Akıllı şehirler, yoğun veri akışı ve dijital altyapı üzerine inşa edildiklerinden, hem fiziksel güvenlik hem de siber güvenlik boyutlarında yeni gereksinimler doğurmaktadır. Bu çerçevede gelişmiş gözetim sistemleri, akıllı sensörler, büyük veri analitiği ve yapay zekâ tabanlı çözümler gibi teknolojiler incelenecektir. Bu sistemlerin şehir güvenliğini artırmadaki rolü tartışılacaktır.

3.1. Güvenlik perspektifinden akıllı şehirler: kavramsal çerçeve

Akıllı şehirlerin gelişimi, yalnızca yaşam kalitesinin artırılması ve kaynakların verimli kullanılmasıyla sınırlı değildir; aynı zamanda güvenliğin sürdürülebilir bir biçimde sağlanmasını da gerektirir. Yoğun veri akışı, dijital altyapıların karmaşıklığı ve artan nüfus yoğunluğu, güvenlik konusunu akıllı şehirlerin temel bileşenlerinden biri hâline getirmektedir. Bu bağlamda güvenlik, hem fiziksel alanların korunmasını hem de dijital sistemlerin güvenliğini kapsayan çok boyutlu bir kavram olarak ele alınmaktadır. Kavramsal çerçevede, akıllı güvenlik yaklaşımları; gözetim teknolojilerinden yapay zekâ destekli risk analizlerine, siber güvenlik çözümlerinden vatandaş katılımına kadar geniş bir yelpazede incelenmekte ve akıllı şehirlerin sürdürülebilirliğinin vazgeçilmez unsuru olarak değerlendirilmektedir.

3.1.1. Akıllı güvenlik tanımı ve uygulamaları

Akıllı güvenlik, şehirlerin güvenliğini ve dayanıklılığını arttırmak amacıyla teknoloji ve dijital altyapının entegrasyonunu sağlayan kritik bir bileşendir. Akıllı şehir teknolojilerinin bu alandaki kullanımı, olası tehditleri öngörmek, krizleri yönetmek ve vatandaşları korumak için tasarlanmış kapsamlı çözümler sunmaktadır. Bu sistemler, sensörler ve yapay zekâ gibi ileri teknolojiler kullanarak güvenlik verilerini toplayıp analiz etmektedir. Bu sayede potansiyel tehlikeler proaktif bir şekilde değerlendirilmektedir. Akıllı güvenlik bileşenleri arasında, şehir güvenliği ve vatandaşların güvenlik algısını arttırmaya yönelik uygulamalar ön plandadır. Örneğin fiziksel güvenlik bilgi yönetimi sistemi ile tüm güvenlik cihazları ve uygulamalarının tek bir arayüz üzerinden denetlenmesi sağlanmaktadır. Yeni nesil video kameralar ve sensörlerle donatılmış sistemler, gerçek zamanlı görüntü işleme ve veri analizi yaparak suçların önlenmesinde ve krizlerin erken aşamada tespit edilmesinde kullanılmaktadır (Arslan, 2014).

Akıllı şehirlerde akıllı güvenlikler özellikle şehirlerin dayanıklılığını arttırmada kritik rol oynar. Doğal afetler, teknolojik krizler ve terör olaylarına karşı güvenlik katmanları

oluşturarak şehrin bu tür tehditlere karşı daha güçlü hale gelmesini sağlamaktadır. Yerel yönetimlerin sınır güvenliği ve göçmen kontrolü gibi konularda ek önlemler almasına da olanak tanımaktadır. Beklenen faydalar arasında, vatandaşların yaşam kalitesinin artması, güvenlik algısının yükselmesi ve yerli teknolojilerin kullanımıyla ülke ekonomisine katkı sağlanması yer almaktadır. Şehirlerin daha dayanıklı ve sürdürülebilir hale gelmesi, akıllı güvenlik çözümlerinin ulusal ve yerel düzeyde entegrasyonu ile mümkün kılınır. Bu çözümler, güvenli şehirler inşa ederek toplumsal refahı arttırırken, kriz anlarında daha etkili ve hızlı müdahale imkânı sunmaktadır (Erkek, 2017). Bu etkili ve hızlı müdahale akıllı güvenlik teknolojileri ve bu teknolojiler ile korunmaya alınan alan türleriyle mümkündür. Aşağıda bazı sorunlar ve bu sorunlara akıllı güvenlik müdahale türleriyle alınan önlemler verilmiştir.

1. Bluetooth Üzerinden Zararlı Yazılım Enjeksiyonu: Saldırgan, aracın Bluetooth ağına kötü amaçlı bir truva atı göndererek aracı hedef alabilir ve sistemine erişim sağlayabilir. Bu şekilde, aracın güvenlik açısından kritik öneme sahip Elektronik Kontrol Üniteleri (ECU) ile, örneğin ABS sistemi gibi, iletişim kurma imkânı elde edebilir. Yapılan araştırmalar, Bluetooth kontrol kodunun, eşleştirilmiş herhangi bir Bluetooth cihazından kod yürütülmesine olanak tanıyan bir bellek istismarını barındırdığını ortaya koymuştur (Parkinson vd., 2017).

2. Jamming (Karıştırma) Saldırısı: Bu saldırı türü, araçtaki LiDAR sensörünü hedef alır ve lazer ışınıyla sensörü yanıltır. Saldırgan, düşük maliyetli bir Raspberry Pi ve düşük güçlü bir lazer kullanarak, aracın sensörlerini sıkıştırmak için bu tür bir sistemi devreye sokabilir. Bu saldırı, araçtaki temel sensörlerin (hız, sıcaklık, vites, hız sabitleyici ayarları ve pil durumu) Elektronik Kontrol Ünitesi (ECU) ile iletişim kurmasını engelleyebilir ve bu bilgilerin sunucuya iletilmesini önleyebilir. Bu tür saldırılara karşı, LiDAR sensörlerinin güvenliğini artırmak ve bu tür karıştırma saldırılarını tespit edebilecek gelişmiş güvenlik önlemleri almak önemlidir (Fraiji vd., 2018).

3. Sybil Saldırısı: Bu saldırı türü, aracın veya kullanıcının kimliğini tahrif ederek ağın normal işleyişini bozmayı hedefler. Saldırgan, kimlik hırsızlığı veya kimlik sahteciliği yoluyla aracın sistemine sızabilir ve araçla iletişimdeki güvenliği tehdit edebilir. Bu tür saldırılara karşı çözüm olarak, araçlarda kimlik doğrulama ve şifreleme yöntemlerinin güçlendirilmesi önerilmektedir. Ağ üzerindeki tüm iletişimlerin sürekli izlenmesi ve anormal aktivitelerin hızlı bir şekilde tespit edilmesi için gelişmiş güvenlik protokollerinin kullanılması önemlidir (Jan vd., 2018).

4. Anahtarla ve Anahtarsız Aracı Ele Geçirme: Bu tür bir saldırı, kötü niyetli içeriden bir kişi ya da gözetimsiz bir araçta dışarıdan biri tarafından gerçekleştirilir. Saldırgan,

aracın sensörlerini değiştirebilir veya bozabilir. Bu tür saldırıları önlemek için araçlardaki donanım ve yazılım bileşenlerinin sıkı güvenlik denetimlerinden geçirilmesi ve araç sistemlerine erişimlerin sürekli izlenmesi gerekmektedir (Amoozadeh vd., 2015).

5. Hava Trafik Kontrol Sistemi İstilası: 4 Kasım 2016'da İsveç'te, Hava Trafik Kontrol Sistemi siber saldırıya uğramıştır. Bu saldırı sonucunda, ülke içindeki ve dışındaki tüm uçuşlar 1 gün süreyle iptal edilmiştir. Hava trafik kontrol sistemine yönelik gerçekleştirilen bu siber saldırı, büyük bir aksaklığa yol açmış ve havacılık sektöründe ciddi operasyonel sorunlara neden olmuştur. Sorunların çözümü için kritik altyapıların sürekli izlenmesi, güvenlik açıklarının hızla giderilmesi, yedekleme ve felaket kurtarma planları oluşturulmuştur (https://siberbulten.com, 2019).

6. Fidye Yazılımı Saldırısı: 18 Kasım 2017'de Sacramento'da meydana gelen fidye yazılımı saldırısında, 30 milyon dosya silinmiş ve saldırganlar 1 Bitcoin (8000$) talep etmiştir (www.cnbc.com, 2019). Bu tür saldırıların önlenebilmesi için, ağ güvenliğinin güçlendirilmesi, yedekleme sistemlerinin düzenli olarak yapılması ve fidye yazılımlarına karşı korunma sağlamak amacıyla gelişmiş antivirüs yazılımlarının kullanılması önemlidir.

7. Taksilerde Ücretlendirme Dolandırıcılığı: Şehir haritasındaki gerçek hizmet mesafesini hesaplamak ve hileli davranışları tespit etmek için GPS hızı ve konum verileri kullanılabilir.

3.1.2. Karmaşık kentsel sistemlerde güvenlik sorunları

Akıllı güvenlik kavramını daha derinlemesine incelemeden önce, şehirleri genel olarak etkileyen güvenlik sorunları ve bu sorunlara dair eğilimlerin ele alınması gerekmektedir. Günümüzde dünya nüfusunun önemli bir kısmı şehirlerde yaşamaktadır. Bu hızlı şehirleşme süreci, yaşam kalitesinin korunması, kentsel altyapının güvenliğinin sağlanması, kamu hizmetlerinin sürekliliğinin temin edilmesi ve temel can ve mal güvenliğinin korunması açısından çeşitli zorluklar yaratmaktadır. Artan asayiş sorunları, tekrar eden suç olayları, nadiren görülen ancak etkileri büyük olan sosyal olaylar, doğal ve teknolojik afetler ile terör saldırıları, şehirlerin güvenliğini sağlama görevini zorlaştırmaktadır (Hessel, 2018).

Altyapı yetersizliklerinin yarattığı tehditler de bu bağlamda önem arz etmektedir. Örneğin dünya genelinde her yıl yaklaşık 20 milyon çocuk, altyapı eksiklikleri nedeniyle hayatını kaybetmektedir. Bu ölümler, hava kirliliği, yetersiz beslenme, kazalar ve erişim sorunları gibi faktörlerden kaynaklanmaktadır. Ancak afetler daha az sıklıkta etkili olmaktadır (Ramaswami vd., 2016: 21). Aynı zamanda küresel düzeyde; iklim değişikliği, ekonomik dengesizlikler, çevre kirliliği, salgın hastalıklar, obezite ve kanser gibi kronik hastalıklar,

toplum sağlığını olumsuz etkileyen karmaşık faktörler olarak karşımıza çıkmakta, şehirleri yeni tehlikelerle karşı karşıya bırakabilmektedir.

Bunun yanı sıra, bölgesel kırılganlıklar ve bu kırılganlıklardan kaynaklanan kayıplar da dikkate değerdir. ABD'de eski içme suyu altyapısındaki kurşun borular ve fosil yakıtlar nedeniyle çocukların kurşun zehirlenmesine maruz kalması ve bunun sonucunda nöro davranış bozukluklarının ortaya çıkması ile ilgili araştırmalar bulunmaktadır (Nevin, 2007). Doğu Bloku'nun çöküşüyle birlikte Avrupa'da göç ve yoksulluk artmış, 1990-2000 döneminde uyuşturucu kullanımına dayalı suç oranları yükselmiş, mülke yönelik saldırılar ise başlangıçta artış göstermiş, sonrasında ise azalmıştır (Aebi, 2004). Bu örnekler bazı sosyal olumsuzlukların uzun süreli ve yapısal olabileceğini, bazılarının ise geçici ve akut etkiler taşıyabileceğini göstermektedir. Bu bağlamda dünya yerleşimlerinin çeşitli küresel, bölgesel ve yerel güvenlik sorunlarıyla karşı karşıya olduğu söylenebilir. Güvenlik, yaşam kalitesi, ekonomik ve kültürel işlevler ile ekosistem işlevlerinin sürdürülmesi açısından kritik bir öneme sahiptir. Bu nedenle, bir şehri akıllı olarak nitelendirebilmek için en uygun ve etkili güvenlik stratejilerinin uygulanması temel bir gerekliliktir. Büyükşehirler, geniş kapsamlı faaliyetler nedeniyle çeşitli ek güvenlik sorunlarıyla karşı karşıya kalmaktadır. Özellikle büyük ölçekli etkinlikler, doğal ve teknolojik afetler, gıda zehirlenmeleri veya terör olayları gibi riskler, özel olarak değerlendirilmeli ve uzun vadeli planlamalar gerektiren durumlar arasında yer almalıdır (Hessel, 2018).

Akıllı şehir uygulamaları, aynı zamanda kendine özgü güvenlik sorunlarını da beraberinde getirmektedir. Altyapının dijitalleşmesi, veri birleştirme ve ilişkilendirme işlemleri aracılığıyla daha geniş bir saldırı yüzeyinin oluşmasına neden olabilmektedir. SCADA sistemleri gibi altyapı izleme araçları, eski donanımlar nedeniyle güvenlik açıkları oluşturabilmektedir (Igure vd., 2006). Bu nedenle, akıllı şehirlerin bilişim güvenliği modelleri ve teknolojilerine yönelik ihtiyaçları artmaktadır.

3.1.3. Akıllı kentlerde sistemlerin güvenliği

Teknolojik çözümler ve hizmetler, akıllı şehirler için büyük potansiyel taşırken, aynı zamanda bazı önemli soruları gündeme getirmektedir. Özellikle, veri paylaşımı ve veri madenciliğine dayalı sistemlerde, kişisel verilerin güvenliği ve mahremiyetin korunması konusu en kritik meselelerden biridir (Lugaric vd., 2010). Akıllı şehirlerin altyapısı, birçok aktörün veri paylaşımında bulunmasına olanak tanıdığı için, bu verilerin güvenliğini sağlamak büyük bir sorumluluk gerektirir. Veri bütünleştirilmesi ve birleşik uygulamaların kullanımı, dijital yüzeyin genişlemesine ve potansiyel güvenlik ihlallerine yol açabilir (Sınmaz, 2013). Bu

nedenle, bu tür sistemlerin tasarımında ve işletilmesinde kişisel verilerin korunmasına yönelik stratejik çözümler gerekmektedir.

Bu sorulara verilecek yanıt, akıllı ağlar üzerinde karşılaşılan güvenlik tehditlerini basitçe yamalarla veya geçici çözümlerle aşmaya çalışmak yerine, daha güçlü bir sistem güvenliği sağlayarak yanıt verilmelidir. Güvenliği sağlamlaştırmanın en etkili yollarından biri, tabakalı bir güvenlik yaklaşımını benimsemektir. Bu bağlamda, "Soğan Modeli" olarak bilinen güvenlik yaklaşımı, akıllı ağlar için önerilen sağlam bir güvenlik katmanı sunmaktadır. Soğan Modeli, her bir akıllı ağ aygıtının özgün bir kimlik numarasına sahip olduğu ve üç temel güvenlik tabakasının bir arada çalıştığı bir sistemi tanımlar. Boyd Cohen'e göre akıllı kent bileşenlerinin ortak özellikleri şöyledir (Cohen, 2018):

- Sunucu için veri koruması uygulaması (Data protection application for the server): Bu tabaka, sunucular arasında değiş tokuş edilen verileri analiz eder ve ağın geri kalanındaki verilerle karşılaştırarak sunuculara zarar verebilecek zararlı yazılımları tespit etmeye çalışır. Bu, akıllı ağda güvenlik sağlamak adına bir tür ağ polisi gibi işlev görür.
- Veri sorgulama tabakası (Data scrutiny layer): Bu katman, akıllı ağ şebekesi içinde sunucularla doğrudan iletişim kurulmasını engeller ve bir güvenlik duvarı gibi çalışarak sunucuları kötü niyetli işlemlerden korur.
- Aygıtlara özel güvenli akıllı yazılımlar (Secure smart software for devices): Bu tabaka, doğrudan cihaz düzeyinde koruma sağlar, böylece ağda olabilecek sızıntıları önler ve cihazların güvenliğini garanti altına alır.

Soğan Modeli, akıllı şehirlerin güvenliğini sağlamak için yerel yönetim kontrol alanı (domain), akıllı şehir sakinleri ve altyapı ile hizmet sunucuları arasında bir dizi katman şeklinde düşünülebilir. Bu yapı içinde yerel yönetim, ağın düzenleyici otoritesi olarak işlev görmekte olup, akıllı ağın yasal çerçeveler ve yönetmeliklerle uyumlu bir şekilde işlemesini sağlamaktadır (Singh, 2015). Akıllı şehir sakinleri ve altyapı tabakası, akıllı ağdaki kullanıcıları yetkilendirir ve kötü niyetli girişimlerden korur. Hizmet tabakası ise, güvenilir ve güvenilmeyen yetki alanları arasında güvenli veri paylaşımını mümkün kılar. Bu yapı, kişisel güvenlik ihlalleri olmadan yaşam kalitesini ve verimliliği artırmak için akıllı şehirlerin temel yapı taşı haline gelir (Khan vd., 2014). Kişisel verilerin güvenliği ve mahremiyetinin sağlanması, akıllı şehirlerin başarısı için kritik bir unsurdur. Bu güvenliği sağlayan katmanlı sistemler, akıllı ağların işleyişinde daha güçlü ve güvenli bir altyapı oluşturulmasına olanak tanır ve akıllı şehirlerde yaşam kalitesinin yükselmesini güvence altına alır.

3.2. Akıllı şehirlerde güvenlik teknolojileri

Akıllı kent uygulamaları, belediyeler açısından hizmet önceliklerini belirlemede güncel ve doğru veriye erişim sağlayarak etkin karar alma süreçlerini desteklemektedir. Bu sayede zamandan tasarruf edilmekte, belediye kaynakları daha verimli yönetilmekte ve bilgiye dayalı stratejik planlar geliştirilebilmektedir. Ayrıca, yönetişim süreçlerinin güçlenmesi ve belediye çalışanlarının motivasyonunun artması gibi faydalar da sağlanmaktadır. Kent sakinleri açısından belediye hizmetlerine mekândan bağımsız erişim, standart ve eşit hizmet sunumu, bürokrasinin azaltılması ve kent yönetimine katılım gibi avantajlar öne çıkmaktadır (Altunışık, 2018: 139). Bu bağlamda, akıllı kentlerde dijital hizmetlerin yaygınlaşması, kent yönetiminde etkinlik ve sürdürülebilirliği arttıran önemli bir faktör olarak değerlendirilmektedir. Tablo 3.1'de, akıllı şehirlerde enerji yönetiminden güvenliğe kadar uzanan çeşitli dijital hizmet alanlarına yer verilmektedir.

Tablo 3.1. Akıllı Kentlerde Sunulan Dijital Hizmetler

Enerji	**Sağlık**	**Güvenlik**	**Ulaşım**
Yenilenebilir enerji	E-Nabız	Mobese	Ulaşım bilgi sistemi
Akıllı sayaç sistemi	E-Reçete	Panik butonları	Akıllı sinyalizasyon
Uzaktan sayaç okuma sistemleri	MHRS (Merkezi Hasta Randevu Sistemi) mobil uygulaması		Akıllı duraklar
Akıllı şebekeler			Toplu taşıma güzergâh bilgilendirme
Güneş enerjili şarj istasyonları			Yolcu bilgilendirme sistemleri
Güneş ışığı panelleri			
Rüzgâr türbinleri			
Akıllı aydınlatma			
Vatandaş	**Doğal Afet ve Acil Durum**	**Yönetim**	**Çevre**
Adres ve Nüfus Kayıt Sistemi	Afet Bilgi Sistemi	E- yönetişim	Atık Yönetim Sistemi
E-Mezarlık	Akıllı Haritalar	Coğrafi Bilgi Sistemi	Yeşil binalar
E-İmar		E-belediye	Akıllı konteynır

Kaynak: (Yaman ve Çakır, 2018: 1124-1138)

Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler, beraberinde yeni ihtiyaç ve uygulama alanlarını ortaya çıkarmıştır. Bu ihtiyaçların başında ise dijitalleşen yaşam alanlarında güvenliğin sağlanması gelmektedir. Geleneksel anlamda güvenlik, can ve mal güvenliğini ifade ederken teknolojinin gelişmesiyle güvenlik kavramı daha geniş bir kapsamda ele alınmaya başlanmıştır. Bilgi toplumunun bilgiye erişim, işleme ve yönetme yeteneği geliştikçe, afet yönetimi, finansal güvenlik, trafik güvenliği ve dezavantajlı grupların takibi gibi birçok alanda güvenlik ihtiyacı artmıştır. Bu ihtiyacı karşılamak için akıllı şehir uygulamaları, yenilikçi ve sürdürülebilir çözümler sunarak önemli bir rol oynamaktadır (Aslan, 2018: 67).

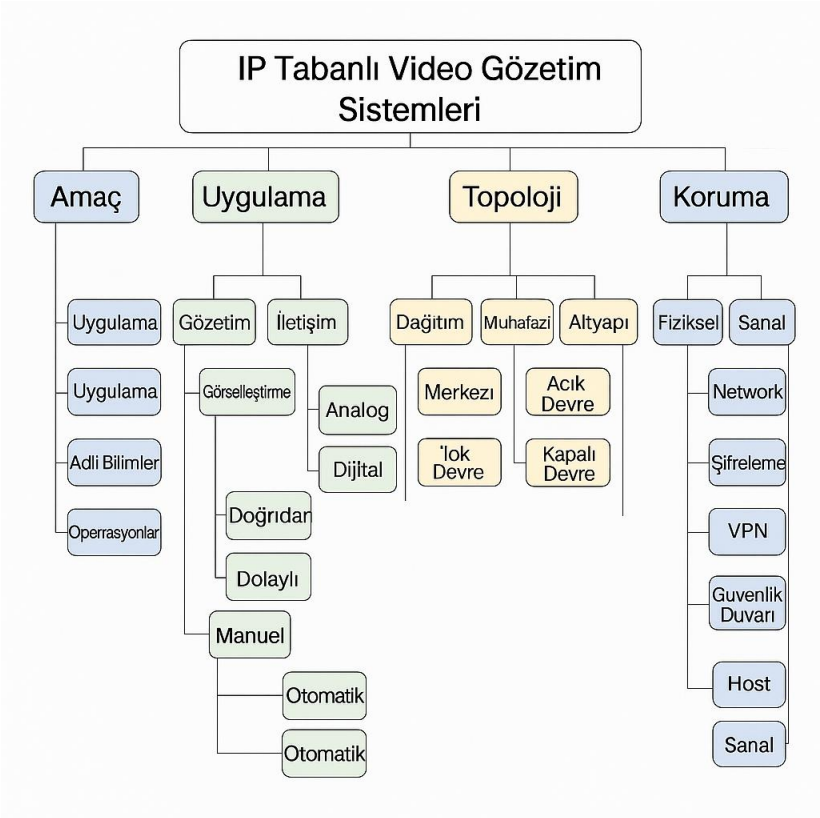
Yönetim açısından bakıldığında güvenlik, yerel yönetimlerin sorumluluğunda olan su yönetimi, ulaşım yönetimi ve enerji yönetimi gibi kamuya açık alanlarda sağlanmalıdır. Bu bağlamda, akıllı şehir uygulamaları, teknolojik altyapı sağlayarak güvenliğin arttırılmasına yardımcı olmaktadır. Akıllı şehir uygulamaları, hem vatandaşların hem de yönetimlerin güvenlik ihtiyaçlarına yanıt verirken kent dokusunu göz önünde bulundurarak yenilikçi ve sürdürülebilir çözümler sunmaktadır (Yapraklı ve Noksan, 2021). Mevcut teknolojik imkanlar, daha etkin ve modern yönetim tekniklerinin gelişimini desteklemektedir.

Akıllı şehirlerin temelini oluşturan veri, kentin çeşitli noktaları arasında ve veri merkezleriyle bilgi akışını sağlamaktadır. Ancak özellikle açık kaynak ve açık veri kullanan sistemlerde veri kontrolü ve yönetimi açısından potansiyel tehditler bulunmaktadır. Türkiye'de 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu gibi hukuki düzenlemeler mevcut olsa da akıllı şehir güvenlik uygulamaları ile ilgili veri yönetimine yönelik yeni düzenlemeler gerekmektedir (Yıldız ve Baz, 2021; Resmî Gazete, 24.03.2016). Kısacası etkili bir veri yönetimi hem bireysel hem de kentsel güvenlik açısından kritik öneme sahiptir. Dijitalleşme ile birlikte gelen yenilikler, güvenlik alanında kolaylıklar sağlasa da yeni güvenlik açıklarını da beraberinde getirmektedir. Kurumsal yapılar ve bireyler, kullandıkları dijital platformlarda etkili güvenlik sistemleri oluşturmak zorundadır. Akıllı şehirler, kurumsal verilerin yanı sıra kişisel verilerin korunması ve olası güvenlik ihlallerinin önlenmesi konusunda da sorumluluk taşımaktadır. Bu nedenle, akıllı şehir uygulamaları, toplumsal yaşam ve kent yönetimlerinde etkinliği artırırken veri kullanımına bağlı güvenlik ihlallerini önlemek için gerekli çözümleri üretmelidir.

3.2.1. Ip tabanlı video gözetim sistemleri

Günümüzde sokaklardan tren istasyonlarına, işyerlerinden evlere kadar her yerde yaygınlaşan video gözetim sistemleri, akıllı uygulamalar sayesinde yüz tanıma, tehdit belirleme, olay algılama, nesne takibi ve hızlı olay inceleme gibi özelliklerle geniş coğrafi alanlarda binlerce kamerayı pratik bir şekilde yönetilebilir hale getirmiştir (Kalbo vd., 2020).

Yeni nesil video kamera sistemleri ve bunlara entegre edilen yazılım ve donanımlar, görüntülerin algılanmasından anlık iletimine ve analizine kadar tüm süreçleri kapsamlı bir şekilde yönetebilir. IP video sistemlerine entegre edilen sensörler, görüntüleri yakalayıp dijital verilere dönüştürebilirler. Bu veriler, yapay zeka tabanlı analiz çözümleri aracılığıyla işlenir. Uzun süreli kamera görüntüleri, akıllı sıkıştırma teknikleriyle dakikalık kayıtlara dönüştürülerek analiz süreci hızlandırılır. Bu bilgiler ışığında IP tabanlı video gözetim sistemlerine genel bir bakışı aşağıdaki görselde bulabilirsiniz.



Şekil 3. 1. IP Tabanlı Video Gözetim Sistemlerine Genel Bakış

Kaynak: (T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2024)

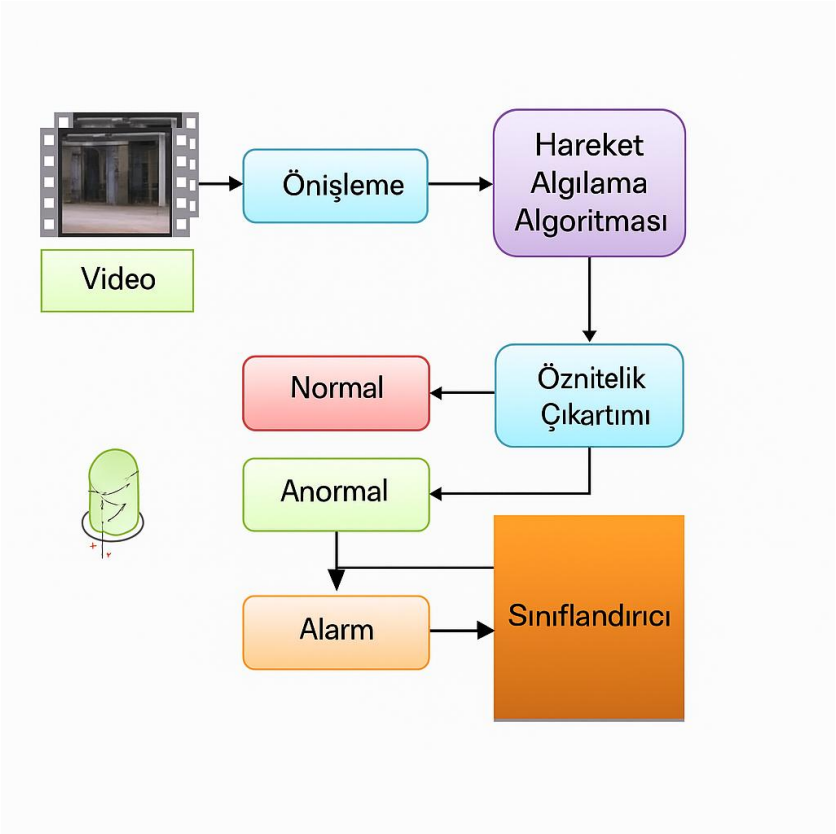
Günümüzde ev ve iş yaşamında günlük aktivitelerin kolaylaştırılması amacıyla teknoloji daha yaygın bir şekilde kullanılmaktadır. Teknolojik ilerlemeler, internet ve uzaktan kontrol sistemlerinin yeni çağın vazgeçilmez unsurları haline gelmesini sağlamıştır. İletişim alanındaki hızlı gelişmelere paralel olarak bireyler bulundukları mekândan bağımsız olarak ev ve işyerlerini internet veya kablosuz sistemler aracılığıyla izleme ve kontrol etme talebindedir. Uzaktan kontrol ve görüntüleme sistemleri, robot teknolojilerinde de etkin bir şekilde kullanılmaktadır. Örneğin bir robot araca entegre edilen mini kamera, uzaktan görüntü sinyallerini kumanda merkezine ileterek kullanıcıya radyo sinyalleri aracılığıyla aracı kontrol etme imkânı sunmaktadır. Bu tür sistemlerde, uzaktan kumandalı bir araç üzerindeki kamera yardımıyla, bilgisayar başındaki kullanıcı, aracın yönelimi hakkında bilgi sahibi olabilir. Bu otomasyon ve kontrol sistemlerinin kritik bir bileşeni olan kameraların, tam bir güvenlik sağlamak için her eksende hareket edebilme yeteneğine sahip olması gerekmektedir. Bilgisayar kontrollü kameralı robot kollar, ortamdan görüntü aktarımı sağlayarak kullanıcıların kolun hareketlerini bilgisayar üzerinden kontrol etmelerini mümkün kılmaktadır (Canpolat, 2024).

Kameralı sistemler ve uzaktan kumandalı robotlar, uzaktan eğitimde çeşitli aktivitelerin gerçekleştirilmesini desteklemektedir. Uzaktan eğitimin önem kazandığı günümüzde, eğitim

laboratuvarlarının uzaktan erişilebilir olması, öğrencilerin laboratuvar imkanlarına her zaman erişim sağlaması açısından kritik bir aşamadır. Uzaktan eğitimde, kameranın güvenli bir şekilde kontrol edilmesi, deneylerin güvenli bir şekilde gerçekleştirilmesi ve bilgisayar başındaki deney operatörünün deney standını izlemesi için büyük önem taşır. Operatör, tehlikeli durumlarda deneyleri bilgisayardan durdurabilir. İstemci arayüz yazılımı ile uzaktaki deney ortamına bağlantı kurulabilmesi, deneylerin gerçek zamanlı olarak gözlemlenmesini mümkün kılar. Bu sistemler, ses aktarımı da sağladığı için fakültelerde internet üzerinden canlı ders izleme veya sınav sırasında öğrencilerin izlenmesi gibi çeşitli uygulamalara olanak tanır. Ayrıca kontrol sistemlerinin entegrasyonu ile internet üzerinden görüntülü ameliyat gibi ileri düzey amaçlar için kullanılabilir. Dünya genelinde web üzerinden güvenlik ve izleme sistemlerinin yaygın kullanımı gözlemlenmektedir. AVA uygulamaları, bağlı oldukları bilgisayarlardan aldığı görüntüleri internet üzerinden başka bir bilgisayara veya GPRS yoluyla cep telefonlarına aktarma işlevi görebilmektedir (Alp, 2018).

3.2.2. Video analiz tabanlı şüpheli davranış tespiti

Video gözetim sistemlerinde insan davranışının tespiti, şüpheli aktiviteleri otomatik ve akıllı bir şekilde belirlemek için kullanılan bir yöntem olup, havaalanları, tren istasyonları, bankalar, ofisler ve sınav salonları gibi halka açık alanlarda bu amaçla geliştirilen birçok verimli algoritma kullanılmaktadır. Bilgisayarlı veya video gözetim yöntemleri, ortamların modellenmesi, hareketin tespiti, hareket eden nesnelerin sınıflandırılması, izleme, davranışların analiz edilmesi ve birden fazla kameradan gelen bilgilerin birleştirilmesi gibi aşamaları içermektedir (Amrutha vd., 2020). Görüntülerde anormal davranışı ya da olayı bulmak için bu aşamalar, belirli bir metodoloji üzerinden işlemektedir.



Şekil 3. 2. Video Analiz Sistemlerinin Alarm Oluşturması Süreci

Kaynak: (T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2024)

İnsan davranışlarının ve çevreyle etkileşimlerinin otomatik olarak anlaşılması, çok çeşitli alanlarda potansiyel uygulamalar sunduğundan dolayı günümüzde önemli bir araştırma konusu haline gelmiştir. Bu araştırmalar, insan davranışlarını kapsamlı bir şekilde modellemeyi hedefler bu kapsamda duygular, ilişkisel tutumlar, eylemler ve yüz ifadeleri gibi birçok yönü ele alır. Esakky Selvi ve arkadaşları tarafından video analiz tabanlı şüpheli davranış tespitine yönelik gerçekleştirilen araştırmada, söz konusu sistemlerin hangi alanlarda etkin biçimde kullanılabileceği ortaya konmuştur (Selvi vd., 2022):

- Kamu Güvenliği: Havalimanları, tren istasyonları ve metro gibi yoğun alanlarda şüpheli hareketlerin algılanması
- Bankacılık ve Finans: ATM önlerinde bekleyen ya da olağan dışı hareket eden bireylerin tespiti
- Eğitim Kurumları: Okullarda ve üniversitelerde kavga, hırsızlık ve akademik etik ihlali gibi durumların belirlenmesi
- Perakende ve Ticaret: Mağazalarda hırsızlık girişimlerini tespit etmek
- Askeri ve Kritik Tesisler: Yetkisiz giriş ve sabotaj gibi riskleri tespit etmek

- Ulaşım ve Toplu Taşıma: Şüpheli bavullar, şüpheli kişilerin hareketleri ve yasa dışı faaliyetlerin izlenmesi.

Yukarıdaki kullanım alanlarında şüpheli davranışlar bazı sınıflandırmalara ayrılmıştır. Şüpheli davranışlar, güvenlik önlemleri ve izleme sistemleri açısından çeşitli kategorilere ayrılmaktadır. Şiddet içeren davranışlar, toplumsal huzuru tehdit eden önemli unsurlar arasında yer alır. Kavga, saldırı, silah kullanımı ve özellikle kamuya açık alanlarda şiddet içeren eylemleri kapsamaktadır. Bir diğer önemli sınıflandırma ise hırsızlık ve vandalizm ile ilgilidir. Mağaza içi hırsızlık, duvarlara zarar verme ve araç hırsızlığı gibi eylemler, bu kategorinin içinde değerlendirilir. Loitering (amaçsız dolaşma) davranışları, özellikle bankalar, okullar veya kritik altyapıların çevresinde şüpheli şekilde uzun süre bekleyen kişileri ifade eder. Şüpheli davranışlar arasında terk edilmiş nesneler de dikkatle izlenmelidir. Havalimanları ve toplu taşıma alanlarında uzun süre sahipsiz bırakılmış nesneler, güvenlik açısından tehdit oluşturabilir. Yasak bölgelere giriş, yetkisiz alanlara giren veya sınırları aşmaya çalışan kişilerle ilgili bir diğer önemli şüpheli davranış kategorisidir (Selvi vd., 2022). Bu sınıflandırmalar içinde bazı teknolojiler kullanılarak şüpheli davranışlar tespit edilmektedir.

Şekil 3.3. Şüpheli Görülebilecek Grup Aktiviteleri Algılama Sistemi

Kaynak: (Ak, 2024: 1005-1029)

Şüpheli davranış tespitinde kullanılan teknolojiler, yapay zeka ve makine öğrenimi tabanlı gelişmiş algoritmalar ile desteklenmektedir. Bu sistemlerde Makine Öğrenimi ve Derin Öğrenme teknikleri, özellikle Convolutional Neural Networks (CNN) ve Recurrent Neural Networks (RNN) modelleri aracılığıyla insan hareketlerini ve davranış kalıplarını analiz etmektedir. Hareket Tespiti Algoritmaları, arka plan çıkarmaya dayalı yöntemler ve optik akış teknikleri kullanarak olağan dışı hareketleri belirlemekte ve anormal aktiviteleri tespit etmektedir. 3D Nesne Tanıma Teknolojileri, insan vücut hareketlerini ve objelerle olan etkileşimlerini analiz ederek şüpheli davranışların belirlenmesine yardımcı olmaktadır (Xia vd., 2015).

Öte yandan bu teknolojilerin gelişimi, bilgiye dayalı analizlerin ve verilerin işlenmesinin giderek daha önemli hale gelmesini sağlamaktadır. Tarihsel süreç boyunca bilgi, uluslararası, ulusal ve özel sektör girişimlerinde merkezi bir rol üstlenmiş; teknolojik ve stratejik bir unsur olarak önemini daima korumuştur. İnsanlık var oldukça, bilginin bu belirleyici ve yönlendirici niteliği sürdürülebilirliğini devam ettirecektir. Öte yandan, bilgi sızıntıları çoğu zaman ancak eylemler gerçekleştikten ve olumsuz sonuçlar ortaya çıktıktan sonra tespit edilebilmiştir. 21. yüzyılda teknolojinin hayatımızın her alanına entegre olmasıyla birlikte, bilgi sızıntıları da teknolojik araçlar aracılığıyla gerçekleşmektedir. Bu tür sızıntıların sıklığı, önceki dönemlere kıyasla artış göstermektedir. Akıllı cihazlar ve diğer teknolojik araçlar, bilgi güvenliği açısından yeni zorluklar ve riskler ortaya çıkarmaktadır. Bu nedenle sürekli izleme ve güvenlik önlemleri gerektirmektedir (Ateş ve Önder, 2019).

Yapay zekâ, genel olarak insan zihninin bilişsel, öğrenme ve muhakeme özelliklerini makineler üzerine aktarma çabası olarak tanımlanabilir. Bu çaba, yüzyıllardır süregelen geniş bir çalışma alanını kapsamaktadır. Derin öğrenme, bu alanda insan düşünce süreçlerini veri setlerindeki örüntüler aracılığıyla bilgisayarlara öğretmeyi amaçlayan bir makine öğrenmesi alt dalıdır ve multidisipliner bir yaklaşımla birçok farklı alanla etkileşimde bulunabilir (Kocaman, 2020).

Yüz ifadeleri, hareket pozisyonları ve nesneler, suç eğilimleri hakkında beklenenden daha fazla bilgi sunabilir. Bir kişinin davranışları hakkında bilgi edinmek ve yüz ifadelerinden duygularını çıkarmak mümkündür. İnsan davranışının özel durumları hakkında önemli çıkarımlar yapılmasına olanak tanır. Derin öğrenme modellerindeki son gelişmeler, görüntülerden anlamsal örüntülerin tanınmasında büyük bir ilerleme sağlamıştır. Yüz görüntülerinden bir bireyin duygusal durumu, karakter özellikleri ve pozisyon özellikleri gibi çeşitli durumlar tahmin edilebilir. Çeşitli derin öğrenme mimarilerinin öğrenme

yeteneklerinden yararlanılarak yüz ve nesne görüntülerinden suç eğilimleri veya suç tahminleri yapılabilmektedir. Araştırmalar, suçluların görüntüleri üzerinden yakalanması durumunda, bilinmeyen bir kişinin suç eğilimlerini belirlemek için kullanılabilecek bir dizi yüz ve nesne özelliği sunduğunu ortaya koymuştur. Suç tahmini ve tespiti açısından derin öğrenme tekniklerinin potansiyelini vurgulamaktadır (Çalışkan vd., 2022).

Video analizi, suç unsurları oluşturabilecek şüpheli durumları veya gerçek zamanlı olayları algılamak ve tanımlamak amacıyla kameralar aracılığıyla elde edilen video görüntülerinin sayısal olarak incelenmesini sağlayan bir sinyal işleme sistemidir. Bu teknoloji, yaşanan veya yaşanabilecek olayları mekân ve zamana göre tespit etmek için yapay zekâ tekniklerini kullanır. Modern teknolojinin gelişimiyle birlikte sektörde giderek daha fazla önem kazanmaktadır. Geleneksel video izleme sistemlerinde operatörler, birçok kamerayı aynı anda teknik olarak kontrol edememekte ve mevcut olaylar sonrası geriye dönük kayıtlar delil olarak kullanılsa da, kullanıcıların anlık bilgi almasını sağlamamaktadır. Bu durum, özellikle istasyon, yerleşke veya teknik alanlarda olumsuzlukların önceden tespit edilip müdahale edilmesini zorlaştırmakta ve yolcu güvenliğini tehlikeye atabilmektedir. Bu nedenle, video analiz sistemlerinin, kameralar aracılığıyla elde edilen görüntüleri işleyerek kullanıcıyı otomatik olarak alarm ile bilgilendirmesi ve müdahale edilmesini sağlaması önem arz etmektedir (Öz ve Görgünoğlu, 2016).

Canlı görüntüler üzerinde yapılan yazılım algoritmaları, kullanıcılara gerekli uyarıları sağlayarak olayın yaşandığı yerin, en yakındaki personele haber verilmesini ve müdahalede bulunulmasını mümkün kılar. Ayrıca video analiz sistemleri acil durum senaryolarını sisteme tanıtarak, personelin olay yerine gitmesine gerek kalmadan kamera sistemindeki röle çıkışları aracılığıyla diğer sistemlere de entegre edilebilmektedir. Duman dedektörlerinin kamera röle çıkışlarına bağlanmasıyla yangın durumunda kamera algoritmaları olayı algılayarak yangın senaryosunu başlatabilir. Video analizi, piksel sayımı ile gerçekleştirilen bir işlemdir. Piksel, elektronik cihazların ekran görüntülerinin en küçük birimidir. Ekranda meydana gelen piksel değişiklikleri yazılım tarafından analiz edilir. Analiz süreci, ekranda belirli bir alan çizilerek başlar ve bu alandaki hareketler piksel değişimlerine neden olur. Kullanıcı, ne kadar değişim olduğunda alarm almak istediğini belirler. Ancak en düşük piksel değişimlerinde alarm alınması durumunda, yüksek sayıda alarm listesi oluşturulabilir. Bu nedenle, ekran üzerinde hassasiyet ve boyut değerleri ayarlanarak istenilen alan ve değerler belirlenmelidir. Alarm kriterleri buna göre düzenlenmelidir (Axxon, 2024).

Video analiz sistemleri, basit bir “tak ve çalıştır” yaklaşımıyla değil, kullanıcı etkileşimleri ve ekran üzerindeki gözlem süreçleriyle yön kazanan dinamik yapılardır. Sistem yapılandırıldıkça yeni hata türleri ortaya çıkabilmekte; bu hatalar ise sürekli izleme ve iyileştirme süreçleri aracılığıyla en aza indirilmeye çalışılmaktadır. Her kamera farklı mesafeye odaklanabilir ve lens özellikleri nedeniyle standart bir analiz sağlamak zordur. Bu sebeple, analizler belirli bir kalıba oturtulamaz ve sürekli iyileştirme ile zaman içinde istenilen sonuçlar elde edilir. Video analizi, tüm donanım ve yazılım sistemlerinin yönetimi, kontrolü, izlenmesi ve diğer sistemlerle entegrasyonu için geliştirilen bir haberleşme sistemidir. Bu sistemler temel olarak üç ana işlevi yerine getirir: anlık veri akışını sağlayan “canlı izleme”, geçmiş görüntülerin analizine olanak tanıyan “geri dönük izleme” ve belirli hareket ya da olaylara tepki veren “harekete duyarlı izleme”. Olaylardan aksiyon oluşturma, kullanıcı yönetimi, donanım yönetimi ve yapılandırma yönetimi gibi ek fonksiyonlar da sağlar. Yazılım sistemlerinde en yaygın terimlerden biri Video Yönetim Sistemi (VMS) olarak bilinir. Temel bir video yönetim sistemi, gözetim süreçlerinin etkin şekilde yürütülmesini sağlayan "kamera", "kayıt cihazı" ve "izleme ekranı" olmak üzere üç ana bileşenden oluşmaktadır. Donanım üreticileri ve yazılım geliştiricileri, kullanıcı ihtiyaçlarına göre farklı yazılımlar sunabilir ancak bu tür sistemler de genellikle VMS olarak adlandırılır (Netser, 2024).

Kamera nesnesi oluşturulduktan sonra her bir durumu analiz edebilmek için bir algılama bölgesi belirlenir. Bir kamera altında birden fazla algılama bölgesi tanımlanabilir ve her biri için ayrı analiz yöntemleri uygulanabilir. Hareket tespiti, odaklama, kararlılık, kaplama, kızılötesi, arka plan değişikliği, kör nokta ve terkedilmiş nesne algılaması gibi çeşitli algılama bölgeleri mevcuttur. Bu bölgelerin türüne göre hassasiyet, kontrast, filtre ve boyut parametreleri farklılık göstermektedir. Örneğin kameranın sol veya sağ tarafında hareket tespiti yapmak mümkündür. Yazılım algoritmaları ile yapılandırılmış analizler, belirlenen takvim doğrultusunda belirli tarihlerde veya saatlerde çalışacak şekilde programlanabilir. Gündüz belirli bir algılama bölgesi aktif olurken gece farklı bir bölgenin etkinleştirilmesi sağlanabilir. Senaryo çeşitliliği kullanıcı taleplerine göre genişletilebilir. Nesne takibi için kullanılan bu sistemler, daha önce meta veri üretmemiştir. Ancak meta veriler artık nesnelerin izini sürerek ilgili bölgelere getirilmesini sağlamaktadır. Hassasiyet ve kayıp bekleme süresi olmak üzere iki temel parametresi bulunur. Bir nesne kameranın açısına girdiğinde kısa bir süre hareketsiz kaldığında kayıp bekleme süresi belirlenerek takip süresi ayarlanabilir. Hareketli nesnelerin kısa süreli duraklamalarını dikkate alarak kesintisiz takibin sağlanmasına yardımcı olur (Netser, 2024)

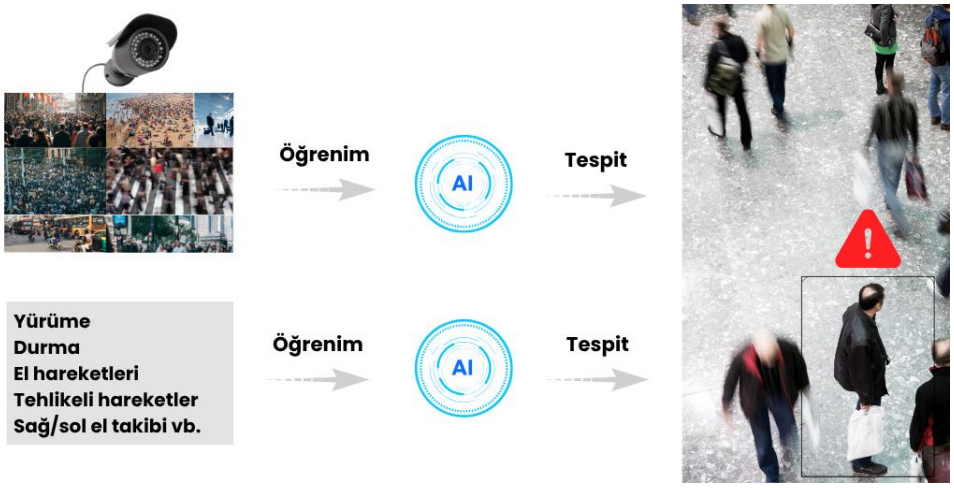
Sistem arama yapılacak nesne sayısını sınırlandırabilir. Örneğin beş nesneye kadar takip yapılabilir. Hareketli nesneler, izleme ekranında belirli çerçeveler içinde takip edilebilir. Ayrıca terkedilmiş nesnelerin analizi de mümkündür. Sistem önce bölgenin arka plan dokusunu ve renklerini kaydeder. Bölge içinde hareket olduğunda kontrast değişikliği meydana gelir. Hareket sırasında bir nesne başka bir nesne bırakıyorsa ve bu bırakılan nesne arka planı bozuyorsa, sistem terkedilmiş nesne olarak tanımlar. Algoritmalar, hırsızlık gibi durumları da algılayarak kontrast değişikliklerini terkedilmiş nesne olarak değerlendirip bilgilendirme yapar. İzleyici nesnesinin parametre ayarları da genişletilebilir. İzci maskesi, algılama parametreleri, perspektif ve nöro filtre ayarları gibi seçenekler mevcuttur. İzci maskesi, belirli alanlarda analiz işlemlerinin yapılmadığı ölü bölgeleri tanımlar. Aynı görüntü üzerinde birden fazla maskeleme işlemi yapılabilir (Netser, 2024). Algılama bölgelerinde, nesnelerin en küçük ve en büyük boyut ayarları yapılır. Perspektif ayarı, ekran görüntüsündeki nesnelerin uzaklık farklarını dikkate alarak boyut farklarını telafi eder. Bu ayar, en düşük ve en yüksek değerler üzerinden gerçek sayılarla işlem yaparak ekran üzerindeki gerçek boyutları sistemde kaydeder. Bu aşamada yapılan işlemler, donanım mimarisi ve nesnelerin tanınması ile ilgili olup yazılım otomatik olarak bu bağlantıyı gerçekleştirir. Ekranda belirlenen alanda çekilen çizgide nesne geçtiğinde canlı alarm üretimi sağlanır. Bu yapılandırma, izleyici nesnesi altında oluşturulan Video Medya Veri Analiz Algılama (VMDA) nesnesi ile gerçekleştirilir. Tek çizgi veya çoklu çizgi olarak iki parametre sunulur. Tek çizgi parametresi ile ekranda bir çizgi çekilir ve hangi yönden geçiş olduğunda alarm vereceği tanımlanabilir. Çift yönlü analiz de mümkündür. Aranılan nesnenin türü farklı olarak ayarlanabilir. Çoklu çizgi parametresinde ise video görüntüsünde çizgiler birleştirilerek belirli bir bölge oluşturulur. Bölgedeki alarm durumu, nesnenin kaç saniye içinde bulunması gerektiği düzenlenebilir. Alana giriş çıkış anındaki alarm seçenekleri ayarlanabilir (Axxon, 2024).

3.2.3. Görüntülerden insan davranışı tespiti

İnsan hareketlerinin görüntülerde etiketlenmesi ile davranış tespiti ve kayıt altına alınması gibi özellikleri içerir. Oluşturulan belli algoritma ve eylem sınıflarında video yayınlarının analiz edilmesi bir uygulama örneğidir. Buradan hareketle video analizi, tehditlerin, şüpheli olayların veya gerçek zamanlı davranışların tespit edilip tanımlanmasını sağlayan sayısal görüntü işleme sistemidir. Bu sistem, video kayıtlarını analiz ederek potansiyel riskleri ya da anormal olayları belirlemek amacıyla kullanılmaktadır. Video içerik analizi, iki farklı şekilde gerçekleştirilebilir. Birincisi, gerçek zamanlı olarak belirlenen olayların sisteme alarm gönderecek şekilde tetiklenmesidir. İkinci ise kayıt sonrası adli amaçlı analizler yapılarak

belirli bir aktivitenin ya da olayın bulunması için ileri düzeyde arama yapılmasıdır. Analiz edilen veriler, farklı video kaynaklarından elde edilebilir (Yaman ve Çakır, 2018). En yaygın kullanılanlar arasında CCTV kameraları, trafik izleme kameraları ve çevrimiçi video akışları bulunmaktadır. RTSP veya HTTP gibi uygun protokolleri destekleyen herhangi bir video kaynağı, video analiz sistemlerine entegre edilebilir. Anormal insan davranışlarının video tabanlı olarak tanınması, son yıllarda güvenlik ve izleme alanlarında önemli bir araştırma konusu olmuştur. Bu alandaki çalışmalar, insan davranışlarını modelleyerek olağan dışı etkinlikleri tespit etmeyi amaçlamaktadır. Popoola ve Wang (2012) tarafından yapılan bir inceleme, bu alandaki mevcut yöntemleri kapsamlı bir şekilde ele almıştır. Anormal davranışların tespitinde kullanılan yöntemler genellikle iki ana yaklaşıma ayrılmaktadır (Popoola ve Wang, 2012).

- Özellik Tabanlı Yaklaşımlar: Bu yöntemler, video verilerinden çeşitli özellikler çıkararak davranışları analiz eder. Özellikler, piksel seviyesinde veya obje seviyesinde olabilir. Mekansal ve zamansal özelliklerin birleşimi, hareketin anlaşılmasında özellikle etkili olmuştur.
- Model Tabanlı Yaklaşımlar: Bu yöntemler, davranışları modellemek için istatistiksel ve makine öğrenimi tekniklerini kullanır. Gizli Markov modelleri (HMM'ler) ve derin öğrenme yöntemleri, anormal davranışları tespit etmek için uygulanmaktadır.



Şekil 3. 4. Tehlikeli ya da Şüpheli Hareket Algılama Sisteminin Detayları

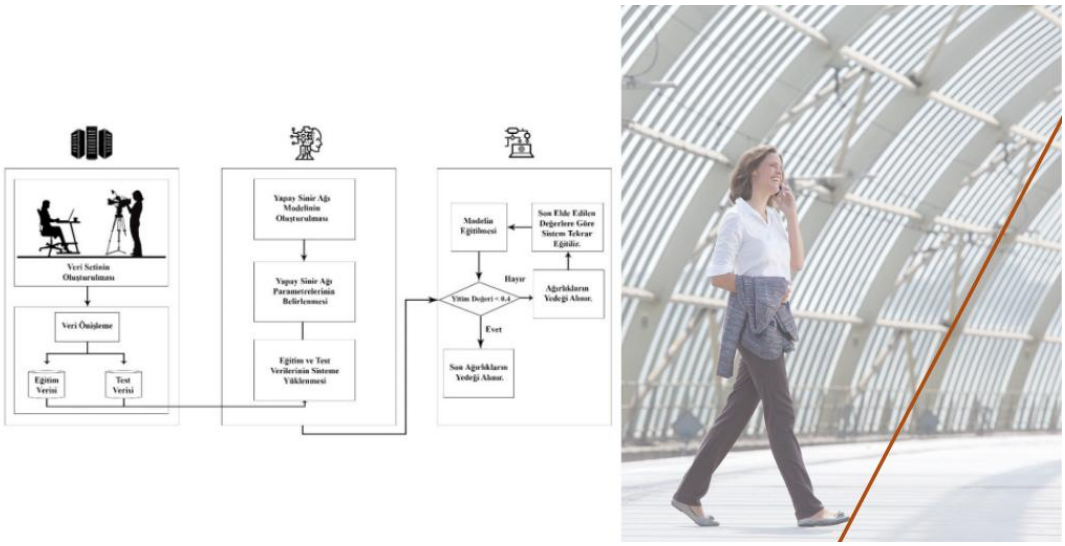
Kaynak: (T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2024)

Yukarıdaki yöntemlerle tespit edilen video tabanlı anormal insan davranışlarının tanınmasında karşılaşılan ana zorluklar üç başlık altında ele alınabilir. İlk olarak, veri çeşitliliği ve karmaşıklığı, farklı ortamlar, aydınlatma koşulları ve kamera açıları gibi faktörlerin, davranışların doğru bir şekilde modellenmesini zorlaştırdığını belirtmişlerdir. İkinci olarak, özellik seçimi ve temsili üzerinde durulmuştur; davranışları etkili bir şekilde temsil edecek uygun özelliklerin seçilmesinin, modelin başarısı açısından kritik bir öneme sahip olduğu vurgulanmıştır. Zaman ve mekan bağlamı, davranışların doğru bir şekilde anlaşılabilmesi için mekansal ve zamansal faktörlerin göz önünde bulundurulması gerektiği ifade edilmiştir. Bu zorluklar, anormal davranışların doğru tespiti için önemli engeller oluşturmaktadır (Popoola ve Wang, 2012).

Verimli bir analiz için öncelikle olayların meydana gelebileceği alanı tam olarak görebilen bir görüş açısı sağlanmalıdır. İşleme kapasitesinin yeterli olduğu durumlarda, daha fazla veri işlemek analizlerin başarısını artıracaktır. Video analiz yazılımları, merkezi sunucular üzerinde ya da kamera üzerinde bulunan işlemciler aracılığıyla çalıştırılabilir. Analizlerin kameralar üzerinde gerçekleştirilmesi, merkezi sunuculara iletilen veri miktarını azaltacaktır. Ancak analiz merkezi sunucularda yapıldığında kamera sayısının artmasıyla birlikte ihtiyaç duyulan işlem gücü ve bant genişliği de önemli ölçüde artabilir. Ağ trafiği ve depolama alanı ihtiyacını düşürmek için yazılım, yalnızca şüpheli olaylar sırasında veri iletecek şekilde yapılandırılabilir (Yaman ve Çakır, 2018). Sektörde sıkça tartışılan bir soru, video analizinin merkezi sunucularda mı yoksa kameralar üzerinde mi yapılması gerektiğidir. Her iki seçenek de kullanılabilir ancak yatırım kararı almadan önce sistemin denenmesi önerilmektedir. Video analiz başarısı, birçok farklı parametreye bağlıdır. Bu yüzden yatırım yapmadan önce kamera ve yazılımın bir demo sürümünün test edilmesi önemlidir. Bu testler sırasında, sistemin gerçek zamanlı görüntü ve olaylarda ne kadar başarılı olduğunu görmek, donanım ihtiyaçlarını belirlemeye ve yapılacak yatırımın getirilerini değerlendirmeye yardımcı olacaktır.

Tüm video analizlerinde benzer yöntemler uygulanır. İzlenmesi gereken olayın parametreleri belirlenir ve bir alarm durumu için uyarı mekanizması yapılandırılır. Belirlenen kriterlere uygun bir olay gerçekleştiğinde yazılım kullanıcıya alarm verir. Aşağıda yaygın olarak kullanılan bazı görüntülerden insan davranışı tespit türleri yer verilmiştir (Elektrik Tesisat Portalı, ET: 22.08.2024):

A) Sanal hat geçiş tespiti: Tanımlanmış bir sanal çizgiyi geçen nesneler tespit edilir ve nesnenin hangi yönde geçiş yaptığı belirlenir.



Şekil 3. 5. Sanal Hat Geçiş Tespiti ve Sistem Mimarisi

Kaynak: (Çalışkan ve Demir, 2022: 28-43)

B) Hareket algılama: Hareket, tüm sahnede veya belirlenmiş bir sanal bölgede tespit edilebilir.

Şekil 3. 6. Tehlikeli ya da Şüpheli Hareket Algılama

Kaynak: (Çalışkan ve Demir, 2022: 28-43)

C) Bırakılan nesne tespiti: Tanımlanmış bir bölgede belirli bir süre boyunca kalan nesneler algılanır.

Şekil 3. 7. Bırakılan Nesne Tespiti

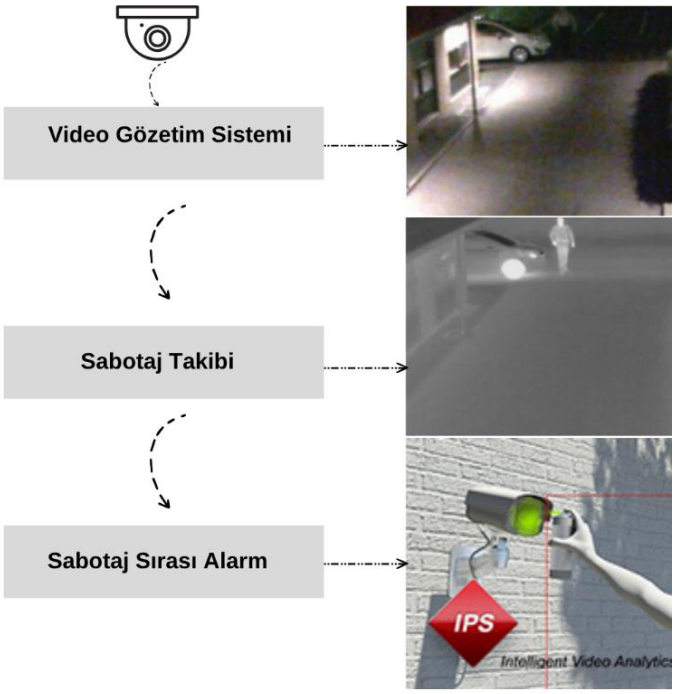
Kaynak: (Zhang vd., 2019: 122-129)

D) Alınan nesne tespiti: Tanımlanmış bir bölgeden kaybolan ve belirli bir süre sonra geri dönmeyen nesneler tespit edilir.

Şekil 3. 8. Alınan Nesne Takibi

Kaynak: (Gade vd., 2016: 291-308)

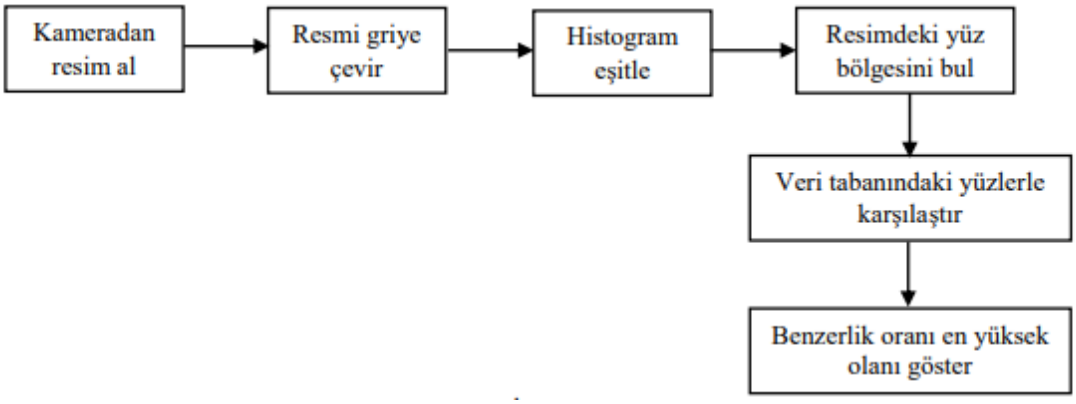
E) Kamera sabotaj alarmı: Kameranın görüş açısındaki ani değişiklikler algılanır. Kameranın açısının değiştirilmesi, görüşünün engellenmesi, üzerine sprey sıkılması ya da fokusun bozulması gibi durumlar bu alarmları tetikler.



Şekil 3. 9. Kamera Sabotaj Alarmı

Kaynak: (Gil-Jimenez vd., 2007: 222-231)

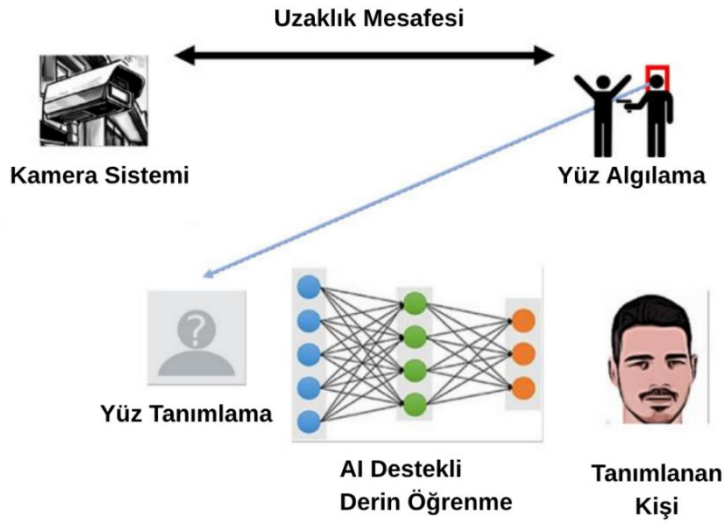
F) Yüz algılama: İnsan yüzünün temel özelliklerini tanıyarak yüz tespiti yapılır. Yüz algılama sistemlerinin genel olarak çalışma mekanizması vardır.



Şekil 3. 10. Yüz Algılama Sistemlerinin Çalışma Mekanizması

Kaynak: (Gil-Jimenez vd., 2007: 222-231)

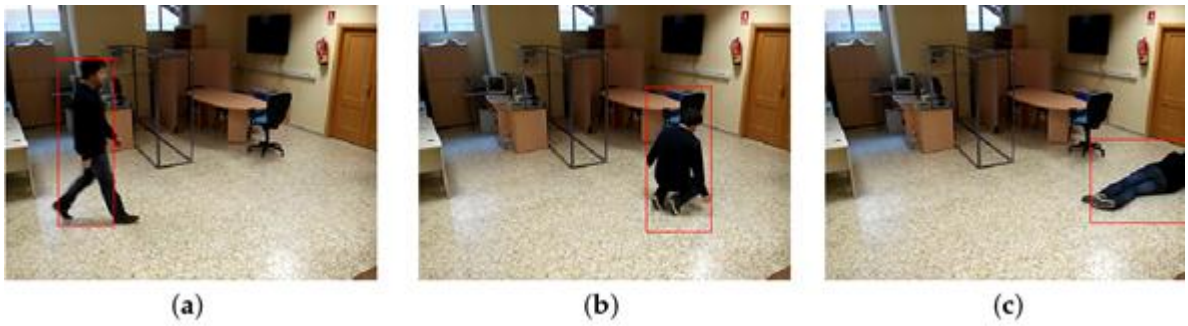
Bu çalışma mekanizmasına göre sistem, belirli yüzleri veri tabanıyla karşılaştırarak benzerlik oranı en yüksek olanı gösterir. Veri tabanına kayıtlı yüzleri ve resimleri kolaylıkla çıkarabilir. Şekil 3.10'de gösterilen işlem adımlarına göre sistem yüz algılama taramasına başlayarak aşağıdaki sonucu vermektedir.



Şekil 3. 11. Yüz Algılama

Kaynak: (Llauradó vd., 2023)

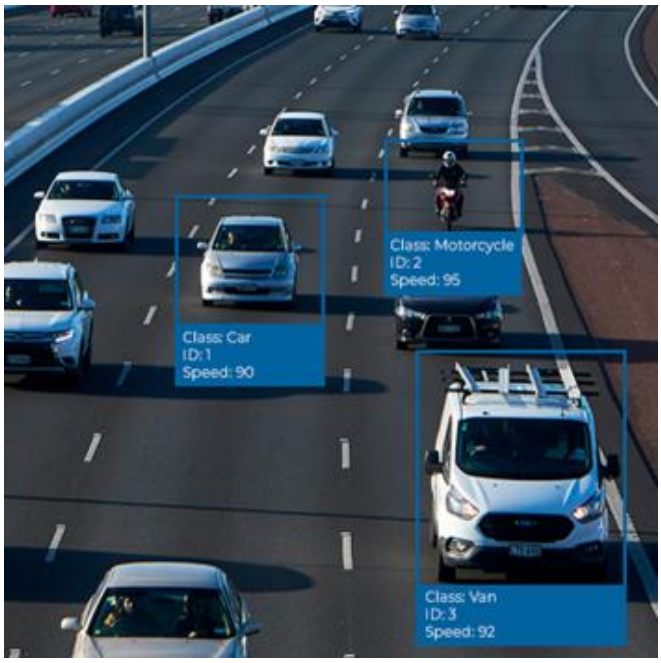
G) Düşme algılama: Belirlenen bir alanda bir insanın düştüğünü algılar ve alarm verir. Bu analiz aynı zamanda geçmiş kayıtlar üzerinden adli amaçlar için de kullanılabilir.



Şekil 3. 12. Düşme ya da Anormal Hareket Algılama

Kaynak: (Gil-Jimenez vd., 2007: 222-231)

Ğ) Aşırı hız tespiti: Bir kişi ya da araç, kameranın görüş açısında tanımlanmış hız sınırını aşarsa alarm oluşturur.



Şekil 3. 13. Aşırı Hız Tespiti

Kaynak: (Ilgaz ve Saltan, 2017)

H) Yüz tanıma alarmı: Kolluk kuvvetleri, saldırganları tanımlamak ve gerçek zamanlı uyarılar oluşturmak için yüz tanıma teknolojisini kullanır. Canlı video akışlarındaki yüz verileri, veri tabanındaki kayıtlarla karşılaştırılarak şüpheli kişilerin tespit edilmesi sağlanır.

Şekil 3. 14. Yüz Tanıma Alarm Sistemleri

Kaynak: (Llauradó vd., 2023)

İ) İş zekası analizleri: İnsan sayma, ısı haritaları ve sıra uzunluğu tespiti gibi analizlerle, müşteri davranışlarını anlamak ve deneyimi geliştirmek amacıyla kullanılır.

Şekil 3. 15. AI Destekli İş Zekası Analizi

Kaynak: (Gil-Jimenez vd., 2007: 222-231)

Bu analiz yöntemleri, güvenlik sistemlerinin etkinliğini artırmak ve olayları önceden tespit ederek hızlı müdahale olanağı sunmak amacıyla geniş bir yelpazede kullanılmaktadır. Bu teknoloji, güvenlik ve izleme sistemlerinin etkinliğini artıran önemli bir araç haline gelmiştir. Gerçek zamanlı olay algılama ve kayıt sonrası adli analiz imkânları, hem güvenlik güçleri hem de çeşitli sektörler için kritik avantajlar sunmaktadır. Farklı video kaynaklarından gelen verilerin analiz edilmesi, olayların erken tespitini ve müdahale sürecini hızlandırarak olası tehditlerin önlenmesine yardımcı olur. Video analiz teknolojisinin başarısı, kullanılan donanımın kapasitesi, analiz yapılan alanın görüş açısı ve yazılımın doğru yapılandırılmasına bağlıdır. Bu bağlamda, merkezi sunucu tabanlı sistemler ve kamera tabanlı analiz çözümleri arasında bir tercih yapılırken, sistemin uygulanacağı ortamın ihtiyaçlarına ve yatırımın getirisini maksimize etmeye yönelik detaylı bir değerlendirme yapılması gereklidir.

3.2.3.1. Biyometrik tabanlı video sistemleri

Biyometri, bireylerin ayırt edilebilirliğini sağlayan fiziksel ve davranışsal özelliklerin incelenmesiyle ilgilenen bir bilim dalıdır (Dede ve Sazlı, 2010). Yunanca kökenli olan biyometri terimi, yaşam anlamına gelen bios ve ölçüm anlamına gelen metron kelimelerinin birleşiminden türemiştir (Derya, 2011). Geleneksel yöntemlerle karşılaştırıldığında, biyometrik bilgilerin sahtesinin yapılması genellikle daha zordur. Normalde, kişisel biyometri fizyolojik özellikleri ve davranışsal özellikleri içerir (Liang vd., 2012). Biyometrik tanımlama sistemleri (BIS'ler), yani biyometrik özelliklere dayalı tanımlama, geleneksel tanımlamanın aksine, ne olduğumuza (kişinin bireysel özelliklerine) dayanır (De Luis-García vd., 2003).

Biyometrik sistemlerin basit formlarının kullanımı, aslında oldukça eski dönemlere dayanmaktadır. Binlerce yıl önce Nil Vadisi'nde, tarım sektörü ve bu sektöre bağlı hukuki işlemlerde, bireylerin tanımlanması için biyometrik veriler kullanılmıştır. O dönemde bireylerin yara izleri gibi ölçülebilir fiziksel özelliklerinin yanı sıra, ten rengi, göz rengi ve boy uzunluğu gibi kendilerine özgü fizyolojik niteliklere göre ayırt edildikleri belirtilmektedir (Tosun, 2009). 19. yüzyılda kriminoloji araştırmacıları, fiziksel özellikler ile suç eğilimleri arasında bir bağlantı olup olmadığını araştırmaya başlamıştır. Bu süreç biyometriye olan ilginin artmasına yol açmıştır. Araştırmalar sonucunda çeşitli ölçüm cihazları geliştirilmiş ve kapsamlı veri toplanmıştır. Elde edilen bulgular kesin olmasa da bireylerin fiziksel özelliklerinin ölçülmesi kabul görmüş ve parmak izi ile kimlik tespiti uluslararası düzeyde standart bir yöntem haline gelmiştir (Derya, 2011: 57; Tosun, 2009).

Kimlik tanımlama sürecinin otomatikleştirilmesi ise uzun yıllar boyunca askeri ve ticari alanlarda önemli bir gündem maddesi olmuştur. Biyometrik güvenlik sektöründeki firmaların sayısındaki artış, biyometri endüstrisinin büyümesini desteklemiş ve bu alandaki teknolojilerin gelişimini hızlandırmıştır. Biyometrik sistemler genel olarak fiziksel ve davranışsal olmak üzere iki ana kategoriye ayrılmaktadır (Nabiyev, 2009). Fiziksel biyometri, iris, yüz, parmak izi ve el tanıma gibi bireyin bedenine özgü özellikleri içerirken, davranışsal biyometri, ses ve el yazısı gibi bireyin davranışlarına dayalı tanımlamaları ele almaktadır. Bazı kaynaklar biyometrik özellikleri fizyolojik, biyokimyasal ve davranışsal olarak üç kategoriye ayırmaktadır. Fizyolojik biyometri, genellikle insan bedenine ait bir parçanın fiziksel özelliklerini ölçerek elde edilen verileri içerir ve yüz, iris, retina, el geometrisi, parmak izi, kulak yapısı gibi unsurları kapsamaktadır. Biyokimyasal biyometri ise, bedenin kimyasal yapısını ölçerek elde edilen verilerden oluşur. Örneğin vücut ısısı, kalp ritmi, DNA yapısı ve vücut kokusu bu kategoriye girer. Davranışsal biyometri ise yürüme tarzı, konuşma sesi, imza ve yazma ritmi gibi bireyin davranışsal karakteristiklerinden elde edilen verileri içerir. Literatürde, yalnızca tek bir biyometrik özelliğin kullanıldığı sistemler tekli model biyometrik sistemler olarak adlandırılırken birden fazla biyometrik özelliğin birlikte değerlendirildiği sistemler çoklu model biyometrik sistemler olarak tanımlanmaktadır. Ses ve yüz tanıma analizlerinin bir arada yapıldığı sistemler, çoklu model biyometrik sistemler olarak kabul edilir (Kaymaz, 2010).

Biyometrik tabanlı video sistemlerinin kullanım alanları şu şekilde sıralanabilir (Kaymaz, 2010; Nabiyev, 2009):

- Akıllı şehirler

- İnternet bankacılığında kullanıcı tanımlama
- Çağrı merkezlerinde kimlik tespiti
- Hastanelerde hasta takibi
- İş yerlerinde personel devam takibi
- ATM'lerde kullanıcı tanımlama
- Sigorta şirketlerinde kimlik tespiti
- Havaalanları giriş çıkış işlemleri
- Sınır kapılarında girişlerin kontrolü
- Kiralık kasalara erişim güvenliği
- Askeri kaynakların etkin takibi
- Kombine bilet uygulamaları
- Hastanelerde hasta takibi ve kimlik saptama
- Sigorta firmalarında kimlik saptama
- Masaüstü ve dizüstü bilgisayarlarda bilgi güvenliği
- E-ticaret işlemleri
- Yüksek güvenlik gerekli binaların giriş çıkış işlemleri
- Uzaktan eğitim sınav işlemleri
- Ulusal kimlik uygulamaları,
- Sürücü ehliyet ve pasaportlarda kimlik tespiti
- Fotoğraf makineleri
- Cep telefonları
- Akıllı ev sistemleri

Yukarıdaki kullanım alanlarına göre biyometrik video sistemlerinin genel çalışma mekanizması aşağıdaki sıralamada belirtilmiştir (Şamlı, 2009; Tosun, 2009):

- Veri toplama,
- Veri tabanına kaydetme,
- Veri iletimi,
- Modelleme ve ID kod oluşturma,
- Karşılaştırma,
- Sonuç iletimi.

Genel bir çalışma mekanizmasına sahip olan biyometrik video sistemleri, kullanım amaçlarına göre üç farklı kategoriye ayrılmaktadır. Bu kategorilerden ilki olan "bire çok

karşılaştırma" yöntemi, kimlik tanıma (identification) ya da algılama (recognition) süreci olarak tanımlanır. Bu yöntemde, sisteme giriş yapmaya çalışan kullanıcının biyometrik verisi, daha önce sisteme kayıtlı tüm kullanıcı verileriyle karşılaştırılır. Eğer eşleşme sağlanırsa, sistem kullanıcının girişine izin verir. İkinci yöntem, bire bir karşılaştırmadır ve veri doğrulama (verification) olarak adlandırılır. Kullanıcının sisteme sunduğu biyometrik veri, ikinci bir kimlik doğrulayıcı bilgi ile birlikte alınır. Sistemde kayıtlı olan biyometrik veri, bu ikinci kimlik doğrulayıcı bilgi ile ilişkilendirilmiş verilerle karşılaştırılır ve uygunluk durumunda sistem erişim izni verir. Bire çok karşılaştırma yönteminde, veri tabanındaki kayıt sayısının fazla olması, sistemin performansını olumsuz etkileyebilir. Bu, yöntemin temel dezavantajlarından biridir. Öte yandan, bire bir karşılaştırmada kullanılan ikinci kimlik doğrulayıcı bilgilerin unutulma veya kaybedilme riski bulunur. Üçüncü yani son yöntem ise sınıflandırma (classification) yöntemidir. Bu yöntemde, büyük veri tabanlarında biyometrik veriler benzer özelliklerine göre gruplandırılır. Bu sayede daha verimli bir karşılaştırma süreci sağlanır. Verilerin veri tabanlarında saklanması, çeşitli güvenlik problemlerini de beraberinde getirmektedir. Özellikle kişisel biyometrik verilerin çalınması durumu, sistem yöneticileri ve üreticiler açısından önemli bir sorun teşkil etmektedir. Bu sorunlara çözüm olarak biyometrik verilerin kullanıcının sahip olduğu taşınabilir bir cihazda saklanması önerilmektedir. Bu yöntemle, biyometrik veri taşınabilir cihazdan alınarak kullanıcıdan elde edilen güncel biyometrik veri ile karşılaştırılabilir (Şamlı, 2009).

Biyometrik sistemlerin yüksek hassasiyetle çalışması gerekmekle birlikte sistemlerin %100 doğrulukla sonuç üretmesi her zaman mümkün olmayabilir. Sistemin kullandığı cihazın kirlenmesi, ortamın nem oranı, biyometrik verinin elde edilmesi ya da iletilmesi sırasında meydana gelen dış etkenler, istenmeyen gürültülerin ortaya çıkmasına ve biyometrik kodların tam olarak aynı şekilde üretilmemesine neden olabilir. Biyometrik sistemlerin oluşturulabilmesi için belirli ölçütler kullanılmak zorundadır. Bu ölçütler, biyometrik ölçüler olarak adlandırılmaktadır (Özer, 2010). Biyometrik ölçülerin güvenli şekilde şifrelerde kullanılmasına yönelik olarak Uluslararası Bilgi Teknolojileri Standartları Komitesi (INCITS) tarafından geliştirilmiş uluslararası bir standart bulunmaktadır. Bu standart sayesinde, örneğin bir kişinin kendi ülkesinde biyometrik verisi ile erişim sağladığı banka hesabına, başka bir ülkedeki bankamatik üzerinden de güvenli bir şekilde ulaşabilmesi mümkün hale gelmektedir (Şamlı, 2009).

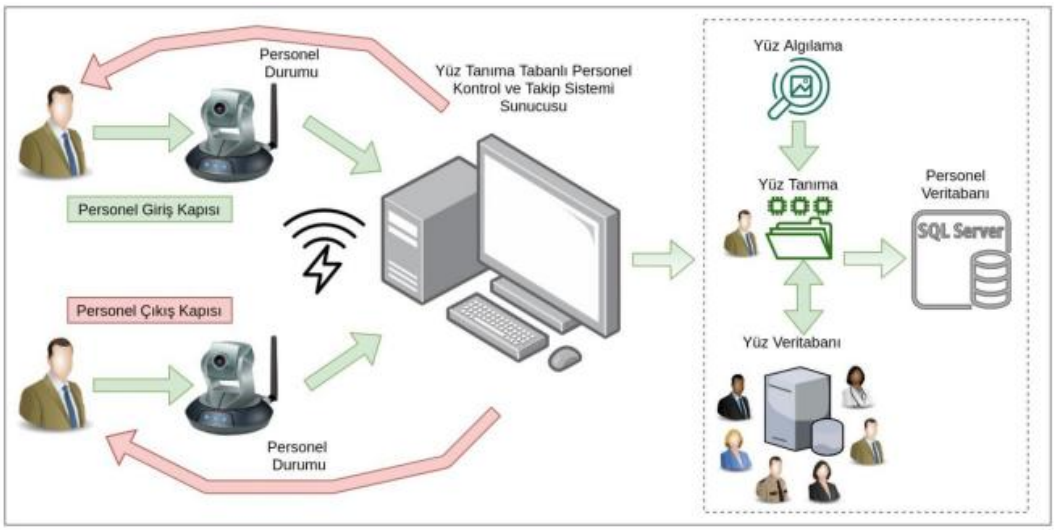
En yaygın kullanılan biyometrik sistemler arasında parmak izi, el geometrisi, yüz tanıma, iris ve retina taraması, ses tanıma ve imza doğrulama gibi yöntemler bulunmaktadır.

Bunun yanı sıra, damar tanıma, el yazısı analizi, yürüyüş tanıma, kulak biyometrisi ve tuş vuruşu analizi gibi daha birçok yöntem de biyometrik kimlik doğrulama sistemleri arasında yer almaktadır. Çalışma konusu gereği biyometrik tabanlı video sistemlerinde en çok tercih edilen yüz tanıma, iris tanıma, retina tanıma ve ses tanıma alanlarına daha yakından bakalım.

3.2.3.2. Yüz tanıma

Yüz biyometrik karakterleri, kişi tanıma süreçlerinde yaygın olarak kullanılan bir yöntemdir. Bu yöntem genellikle yüzün temel unsurları olan gözler, kaşlar, burun, dudaklar ve çene yapısı gibi anatomik özellikler ile bu unsurlar arasındaki ilişkiler üzerine kuruludur (Barbole ve Godase, 2012). Yüz tanıma sistemlerinin en önemli avantajlarından biri, görüntü yakalama cihazı ile çalışırken fiziksel temas gerektirmemesidir. Yüz tanıma teknolojisi birçok alanda kullanılmaktadır. Örneğin alzheimer hastalarının tanıdıkları kişileri hatırlamalarına yardımcı olmak amacıyla kullanılmaktadır. Bu amaçla, hastanın gözlüğüne yerleştirilen küçük bir kamera ve yüz tanıma yazılımı, karşılaşılan kişileri tanıyarak hastaya bilgi sağlar. Benzer biçimde, güvenlik güçleri tarafından suçlu tespiti ve takibi için de kullanılmaktadır.

Aşağıdaki görselde farklı marka ve özelliklerdeki yüz tanıma sisteminin bir örneği verilmiştir. Sistemde çok sayıda özellik içermesi ve karşılaştırma yapılması nedeniyle eşleştirme sorunları ortaya çıkabilmektedir (Ariç, 2011).



Şekil 3. 16. Yüz Tanıma Kontrol ve Takip Sistemi

Kaynak: (Mamak vd., 2020: 497-504)

Ticari uygulamalarda da yüz tanıma yaygın bir şekilde kullanılmaktadır. Örneğin sosyal medya platformlarında ve fotoğraf düzenleme yazılımlarında, Microsoft Photo Gallery ve Google Picasa gibi uygulamalar aracılığıyla fotoğrafları etiketleme işlemleri yüz tanıma

teknolojisi ile yapılmaktadır. Halka açık alanlarda suçlu veya terörist tespitinde de bu teknoloji etkin bir şekilde kullanılmaktadır (Akçay ve Çetinkaya, 2011).

3.2.3.3. İris tanıma

İris, gözün iç kısmında yer alan dairesel ve renkli bölgedir ve bireyin yaşamı boyunca değişmeyen bu yapıya dayanan biyometrik tanıma sistemleri geliştirilmiştir. İris tabakası, her insanda benzersizdir ve hatta tek yumurta ikizleri aynı DNA'ya sahip olmalarına rağmen farklı iris desenlerine sahiptir. Aynı şekilde bir bireyin her iki gözündeki iris de farklılık göstermektedir. İris, doğumun 16. haftasından itibaren oluşur ve bireyin yaşamı süresince değişmez. Ölümden sonra ise göz, canlılığını en hızlı kaybeden organlardan biridir, bu süreç yaklaşık 3 saniye sürmektedir. Dış etkenlere karşı korunmuş bir yapıdadır ve cerrahi müdahalelerle değiştirilemez (Yıldız, 2010).

İris tanıma sistemlerinde birçok referans noktası kullanılmaktadır. Örneğin, parmak izi tabanlı biyometrik sistemlerde doğruluk sağlamak için 60 ila 70 referans noktası kullanılırken, iris tanımada yaklaşık 200 referans noktası bulunmaktadır. Bu durum iris tanıma sistemlerinin yüksek doğruluğa sahip olmasını sağlar. İris tanıma teknolojisi, bazı sınırlamalarla karşı karşıyadır (Bilgin, 2008). Örneğin görme engelli bireyler, Nistagmus hastalığı olan kişiler veya iris tabakasına sahip olmayan bireyler için bu sistemin kullanılması mümkün değildir. İris resmi alınırken göz kapakları veya kirpikler iris desenini bozabilir ve bu durum sistemin performansını olumsuz etkileyebilir. İris görüntüsünün alınması sırasında yayılmakta olan ışık da günlük yaşamda rahatsız edici olabilir (Barbole ve Godase, 2012).

3.2.3.4. Retina tanıma

Retina tanıma, insan göz bebeğinin arkasında yer alan damar tabakasının benzersiz yapısını tanıyan bir biyometrik yöntemdir. Bu sistem, her bireyin retina damar yapısının farklı olmasına dayanarak kimlik doğrulama işlemi yapar. Ancak retina damar yapısının bazı hastalıklardan dolayı kolayca etkilenip bozulabilmesi, bu yöntemin en önemli dezavantajlarından biridir. Özellikle diyabet veya hipertansiyon gibi hastalıklar retinanın yapısında değişikliklere yol açabilir. Sistemin doğruluk ve güvenilirliğini olumsuz etkileyebilir. Bu biyometrik yöntemin yüksek doğruluk sunmasına rağmen, sağlık durumu nedeniyle retina yapısında değişiklikler meydana gelebilecek kişilerde kullanılması sınırlıdır.

Aşağıda farklı marka ve özellikteki İris ve Retina tanıma sistemleri örnek olarak verilmiştir.

Şekil 3. 17. Yüz Tanıma Kontrol ve Takip Sistemi

Kaynak: (Gil-Jimenez vd., 2007: 222-231)

3.2.3.5. Ses tanıma

Davranışsal biyometrik sistemler arasında yer alan ses tanıma, kişinin anatomik, fizyolojik ve psikolojik yapısına bağlı olarak ses dalgalarının ayırt edici özelliklerini kullanır. Temel olarak bir ses sinyali, konuşmacının ağzından çıkarak dinleyicinin kulağına ulaşan bir hava basınç dalgası şeklinde iletilir. Bu dalga, kişinin benzersiz biyolojik yapısına göre farklılıklar gösterir ve tanımlamayı mümkün kılar (Meral, 2008).

Ses biyometrisi ses tanıma ve konuşmacı tanıma olmak üzere iki ana kategoriye ayrılmaktadır. Güvenlik açısından önemli olan konuşmacının kimliğini tanıma işlemleridir. Bu teknoloji, yalnızca belirli seslere yanıt veren cihazlar, güvenlik gerektiren binaların giriş sistemleri ya da güvenlik kuruluşlarında ses kaydına dayanarak konuşmacının kimliğini belirlemek amacıyla kullanılır. Konuşmacı tanıma, metin temelli ve metin bağımsız olmak üzere ikiye ayrılır. Metin temelli konuşmacı tanımada, belirli bir metin seslendirilir ve bu metin üzerinden tanıma gerçekleştirilir. Metin bağımsız konuşmacı tanımada ise herhangi bir metin zorunlu olmadan ses tanımlanır. Bu yöntemin dezavantajları, çoğunlukla çalışma koşullarının elverişsizliğinden kaynaklanmaktadır. Konuşma sinyalinin bozulmaması için ideal ortam sağlanmış olsa dahi, sistemin kullanıldığı farklı ortamlarda istenmeyen gürültüler veya sesin bozulması gibi etkenler, tanıma işlemini olumsuz etkileyebilir. Bireylerin farklı duygusal koşullar altında değişik ton ve vurgularla konuşması, hastalık ya da rahatsızlık durumlarında

sesin değişmesi gibi faktörler de bu biyometrik yöntemin doğruluğunu zayıflatabilir (Yalçın, 2006).

3.2.4. Kalabalıkların video ile izlenmesi

Yoğun insan trafiğinin bulunduğu alanlarda akıllı video izleme sistemleri, olası tehlikeleri hızlı ve anlık olarak tespit etmeye olanak tanır. Konser, stadyum veya geçici etkinliklerde kitle hareketlerinin izlenmesi bu sistemlerin kullanımına örnek olarak verilebilir. Güvenlik, acil durum yönetimi ve etkinlik organizasyonlarında önemli bir teknoloji haline gelmiştir. Bu akıllı video izleme sistemleri, kalabalık alanlarda hareketleri ve davranışları gerçek zamanlı olarak izleyebilir, analiz edebilir ve potansiyel tehlikeleri tespit edebilir. Şüpheli davranışların erken tespiti ve hızlı müdahale için kritik bir rol oynamaktadır (Londralife, 2018, ET: 21.11.2024).

Kalabalıkların video ile izlenmesi, genellikle akıllı video izleme sistemleri ve gelişmiş görüntü işleme algoritmaları kullanılarak yapılır. Bu teknolojiler, kalabalıkların yoğunluğunu, hareketlerini ve davranışlarını analiz etmek için video görüntülerini gerçek zamanlı olarak işler (Kızrak ve Bolat, 2018).

- Kalabalık Yoğunluğu İzleme: Akıllı video izleme sistemleri, bir alandaki kalabalığın yoğunluğunu izleyebilir. Eğer kalabalık yoğunluğu, belirli bir eşik değere ulaşırsa, sistem alarm verebilir. Bu özellik, kalabalığın fazla birikmesiyle ilgili olası tehlikeleri önceden tespit etmek için kullanılır ve acil çıkışların düzenli olarak denetlenmesine olanak tanır. Örneğin, etkinlik alanlarında fazla kalabalıklaşan bölgeler hızla tespit edilebilir.
- Davranışsal Analiz: Sistemdeki video analiz algoritmaları, kalabalıkların hareketlerini inceleyerek şüpheli davranışları tespit edebilir. Özellikle kaçma, koşma, hırsızlık, kavga gibi anormal davranışlar, gerçek zamanlı olarak izlenip alarm oluşturulabilir. Örneğin, bir kişi kalabalık içinde aniden koşmaya başladığında sistem hemen uyarı verebilir.
- Zaman ve Mekân Tabanlı İzleme: Bu sistemler, kalabalıkların hareketini izlerken zaman ve mekân bilgilerini de kullanarak tespit yapar. Örneğin, kalabalık bir alanın belirli bir noktada toplanması ya da dağılımı izlenebilir. Bu özellik, özellikle büyük etkinliklerde veya halka açık toplantılarda güvenliği artırmak için kullanılır.
- Yüz Tanıma ve Kimlik Tespiti: Akıllı video izleme sistemlerinde kullanılan yüz tanıma teknolojisi, kalabalık içerisindeki belirli kişileri tespit edebilir. Güvenlik için önemli bir kişi, aranan bir suçlu veya kaybolmuş bir kişi, kalabalık içinde bulunursa, sistem bu kişiyi tespit edip ilgili güvenlik birimlerine bildirebilir.

- Kalabalıkların Hareket Yönü ve Hızı: Kalabalıkların hareket yönü ve hızları izlenebilir. Bu tür veriler, kalabalığın içindeki bireylerin davranışlarını anlamak için çok faydalıdır. Örneğin, hızla hareket eden kalabalıklar, potansiyel bir kaos durumunun göstergesi olabilir ve sistem bu durumu önceden algılayıp acil müdahale için uyarı verebilir.

3.2.4.1. Akıllı video izleme sistemleri

Yoğun insan trafiğinin olduğu alanlarda akıllı video izleme sistemleri, olası tehlikeleri hızlı ve anlık olarak tespit etmeye yardımcı olur. Bu sistemler, kalabalık yönetimi, güvenlik tehditlerinin belirlenmesi ve ani olaylara hızlı müdahale açısından büyük önem taşır. Konserler, stadyumlar ve büyük organizasyonlarda kitlenin hareket dinamiklerini analiz ederek olası güvenlik tehditlerini önceden tespit edebilir. Kalabalık içinde meydana gelebilecek panik, izdiham veya şüpheli aktiviteler anında fark edilerek güvenlik güçlerinin müdahalesi sağlanır.

Bu sistemler güvenlik ve izleme alanlarında kullanılan, video kamera görüntülerini dijital ortamda analiz eden ve otomatik olarak olayları tespit edebilen ileri düzey bir teknolojidir. Bu sistemler, geleneksel video izleme sistemlerinin ötesinde, yapay zeka (AI) ve görüntü işleme algoritmalarını kullanarak daha akıllı, verimli ve etkili bir izleme çözümü sunar. Akıllı video izleme sistemleri, özellikle güvenlik, suç öncesi tespit, olay analizi ve otomatik raporlama gibi alanlarda pek çok fayda sağlar (Çakır ve Babacan, 2011):

- Kamera Donanımı: Akıllı video izleme sistemleri, yüksek çözünürlüklü kameralar kullanarak görüntü toplar. Bu kameralar, HD veya 4K çözünürlükte görüntüler sağlamakta ve bazıları gece görüşü, hareket algılama ve PTZ (pan-tilt-zoom) özelliklerine sahiptir. Ayrıca, bazı akıllı kameralar entegre yapay zeka özelliklerine sahip olup, gerçek zamanlı analiz yapabilme yeteneği sunar.
- Görüntü İşleme Yazılımı: Akıllı video izleme sistemlerinin kalbi, görüntü işleme ve analiz yazılımlarındadır. Bu yazılımlar, kameralar tarafından yakalanan video verilerini işler, analiz eder ve olayları otomatik olarak tespit eder. Görüntü işleme yazılımı, nesne tanıma, hareket algılama, yüz tanıma, plaka tanıma, davranış analizi gibi özellikler sunar.
- Veri Depolama ve Yönetimi: Akıllı video izleme sistemleri, topladıkları görüntü verilerini yüksek kapasiteli depolama alanlarında saklar. Bu veriler, genellikle bulut tabanlı sistemler veya yerel sunucularda depolanabilir. Verilerin şifrelenmesi ve güvenli bir şekilde saklanması, izleme sistemlerinin etkinliğini ve güvenliğini artırır.
- Alarm ve Bildirim Sistemleri: Akıllı video izleme sistemleri, analiz ettikleri görüntülerde belirli kriterlere göre anormallikler veya güvenlik tehditleri tespit ederse, ilgili

yetkililere bildirim gönderebilir. Bu bildirimler, anlık uyarılar, SMS, e-posta veya mobil uygulamalar üzerinden yapılabilir. Örneğin, bir kamerada izinsiz bir kişiyi veya şüpheli bir hareketi tespit ettiğinde, sistem hemen güvenlik ekibine alarm verir.

- Yapay Zeka ve Makine Öğrenimi: Akıllı video izleme sistemlerinin çoğu, makine öğrenimi ve yapay zeka teknolojilerini kullanarak zamanla daha verimli hale gelir. Sistemler, davranışsal analiz, kalabalık tespiti, takip edilen kişilerin veya araçların kimlik tespiti gibi yeteneklere sahip olabilir. Ayrıca, belirli bir bölgedeki anormal davranışlar tespit edilebilir.

3.2.4.2. Fiziksel kimlik ve erişim kontrol sistemleri (PIAM)

Fiziksel kimlik ve erişim kontrol sistemleri, her türlü fiziksel kimliğin yaşam döngüsünü, yetkilendirilmiş erişim süreçlerini ve güvenlik olayları ile olan ilişkisini yöneten standartlara uygun bütünleşik bir yapıdır. Bu sistemler, kurumsal tesisler, havaalanları, askeri bölgeler ve özel güvenlik gerektiren alanlarda giriş çıkışların düzenlenmesini sağlar. Ayrıca çalışanların ya da ziyaretçilerin belirlenen güvenlik protokollerine uygun şekilde yetkilendirilmesini ve izlenmesini mümkün kılar (Yalçın ve Gürbüz, 2015). Organizasyonların ve tesislerin güvenliğini sağlamak amacıyla, personel, ziyaretçiler, yükleme alanları, özel odalar ve hassas bölgelerdeki giriş-çıkış işlemlerini izler ve denetler. PIAM, organizasyonların fiziksel erişim kontrolünü dijitalleştirmek için güvenlik, verimlilik ve uyumluluk sağlamak amacıyla gelişmiş yazılım ve donanım çözümleri kullanır. Aşağıda PIAM sistemlerinin özellikleri ve bileşenlerine yer verilmiştir (Jain ve Sharath Pankanti, 2003; Erdinç, 2020)

- Kimlik Tanımlama Cihazları: PIAM sistemlerinde, bireylerin kimlik bilgilerini doğrulamak için çeşitli cihazlar kullanılır. Bunlar arasında kart okuyucular (RFID, manyetik, biyometrik), parmak izi tarayıcıları, yüz tanıma sistemleri ve iris tarayıcıları yer alır. Kimlik doğrulama işlemi, genellikle bir şifre, PIN veya biyometrik veri kullanılarak yapılır.
- Erişim Noktası Kontrol Cihazları: Bu cihazlar, fiziksel alanlara girişleri kontrol eder. Kapı kilitleri, turnikeler, biyometrik okuma makineleri, geçiş turnikeleri ve otomatik bariyerler gibi cihazlar, bireylerin doğrulandıktan sonra giriş yapmalarını sağlar.
- Merkezi Yönetim Yazılımı: PIAM sistemlerinin kalbi, merkezi yönetim yazılımıdır. Bu yazılım, tüm erişim noktalarını izler, kimlik verilerini saklar, kullanıcıların geçiş haklarını yönetir ve tüm erişim olaylarını kaydeder. Ayrıca, güvenlik protokollerine uyumu denetler, raporlar oluşturur ve güvenlik ihlalleri durumunda alarm verir.
- Entegrasyon Özellikleri: PIAM sistemleri, genellikle diğer güvenlik ve işletme sistemleriyle entegre çalışacak şekilde tasarlanır. Bu entegrasyonlar arasında CCTV (kapalı devre televizyon) sistemleri, yangın alarm sistemleri, bina yönetim sistemleri (BMS) ve insan

kaynakları yazılımları bulunabilir. Bu tür entegrasyonlar, daha kapsamlı bir güvenlik yönetimi ve kolay raporlama sağlar.

- Veritabanı ve Kayıt Tutma: PIAM sistemleri, kullanıcı bilgilerini ve erişim geçmişini kaydederek, güvenlik ihlalleri veya yetkisiz girişleri izleyebilir. Kayıtlar, herhangi bir şüpheli olayın analiz edilmesine veya gerektiğinde soruşturma yapılmasına olanak tanır.

3.2.4.3. Akustik ateşli silah algılama ve konum tespiti

Akustik ateşli silah algılama sistemi, bir dizi akustik sensör aracılığıyla silah seslerini tespit eder ve tehdidin kaynağını belirleyerek merkezi güvenlik sistemine iletir. Bu sistemler, hükümet binaları, askeri tesisler, müzeler ve yüksek güvenlik gerektiren bölgelerde kullanılarak, silahlı saldırılara karşı hızlı müdahale edilmesini sağlar. Ateş edilen konumun anında tespit edilmesiyle, güvenlik güçleri en kısa sürede olay yerine yönlendirilebilir ve olası tehlikeler minimize edilebilir. Akustik ateşli silah algılama sistemleri, ses algılayıcı mikrofonlar (sensörler) kullanarak, ateşli silahların patlama seslerini algılar ve bu ses dalgalarını dijital veriye dönüştürür. Patlama sesinin yayılması sırasında, sistem sesin kaynağını analiz ederek, ateş açılan yerin koordinatlarını tespit eder. Bu işlem, ses dalgalarının algılama noktalarına ulaşma süre farklarından yararlanarak gerçekleştirilir. Aşağıda akustik ateşli silah algılama ve konum tespiti yapan sistemlerin özelliklerine yer verilmiştir (Özuğur vd., 2014):

- Sensörler (Mikrofonlar): Sistemin en önemli bileşenleri sensörlerdir. Bu sensörler, geniş bir alanı kapsayan akustik algılama yapacak şekilde yerleştirilir. Çeşitli türdeki mikrofonlar kullanılarak, ateşli silah patlamalarının farklı frekanslarındaki sesler tespit edilebilir.
- Veri İşleme ve Analiz Yazılımı: Ses dalgaları sensörler tarafından algılandıktan sonra, bu veriler merkezi bir bilgisayar sistemine iletilir. Yazılım, sesin kaynağını tespit etmek için çeşitli algoritmalar kullanır. Akustik sinyaller, zaman farklarına göre analiz edilerek, en doğru konum belirlenmeye çalışılır.
- Konum Tespiti Teknolojisi: Sistemdeki sensörlerin, patlama sesini duyduğu zamana göre, ateş açılan yerin kesin koordinatları belirlenir. Bu teknoloji, geleneksel GPS veya diğer harita hizmetleriyle entegre edilebilir.
- İletişim ve Alarm Sistemi: Akustik ateşli silah algılama sistemi, tespit edilen bilgiyi gerçek zamanlı olarak yetkililere iletebilir. Bu genellikle bir alarm sistemi veya bir kontrol merkezine bildirilen uyarılar ile yapılır. Ayrıca, bu tür sistemler, anında sesli ve görüntülü iletişim sağlayarak, güvenlik görevlilerinin hızlı bir şekilde olay yerine yönlendirilmesine yardımcı olur.

3.2.4.4. Otomatik plaka tanıma sistemleri

Otomatik plaka tanıma sistemleri, kameralardan alınan araç görüntülerini analiz ederek plaka üzerindeki karakterleri ayrıştırır ve veri tabanıyla karşılaştırır. Bu sistemler, özellikle trafik yönetimi, suçluların takibi ve kaçak araçların tespitinde önemli bir rol oynar. Dubai polisi, devriye araçlarının ön ve yan taraflarına yerleştirdiği plaka tanıma kameraları ile trafiği gerçek zamanlı olarak takip etmekte ve şüpheli araçları tespit etmektedir. ANPR yani *Automatic Number Plate Recognition* bilinen bu sistem, araçların plakalarını hızlı ve doğru bir şekilde tanıyıp, bu bilgiyi dijital ortamda kaydeden teknolojilerdir. Bu sistemler, kamera ve yazılım kombinasyonu ile çalışarak, aracın plakasını okuyup, plakadaki harf ve rakamları dijital formata çevirir. ANPR sistemleri, genellikle güvenlik, trafik yönetimi, otopark yönetimi, geçiş kontrolü ve suç tespiti gibi çeşitli alanlarda kullanılır. Aşağıda bu sistemlerin temel özelliklerine yer verilmiştir (Bayram, 2020):

- Plaka Tanıma: ANPR sistemleri, araçların plakalarındaki harf ve rakamları tanıyabilen özel yazılımlarla çalışır. Sistemde yer alan kameralar, araçların plakalarını okur ve bu bilgiyi veri tabanına kaydeder.
- Yüksek Hızda Tanıma: Bu sistemler, yüksek hızla hareket eden araçların plakalarını bile hızlı bir şekilde tanıyabilir. Bu özellik, özellikle otoyol geçişlerinde ve yoğun trafik koşullarında kullanışlıdır.
- Gerçek Zamanlı İzleme: Otomatik plaka tanıma sistemleri, araç geçişlerini anlık olarak kaydederek ilgili veri tabanlarına işler; böylece trafik akışının eşzamanlı olarak izlenmesine ve etkin bir biçimde kontrol edilmesine olanak tanır.
- Entegre Sistemler: ANPR sistemleri, güvenlik kameraları ve diğer izleme cihazları ile entegre çalışabilir. Bu sayede plaka bilgileri, başka güvenlik önlemleriyle de ilişkilendirilebilir. Örneğin, bir araç arandığında, sistem plakayı tespit eder ve arama kaydıyla eşleştirir.
- Veri Kaydı ve Raporlama: Sistemde toplanan veriler genellikle bir veritabanında saklanır ve istenildiğinde raporlama yapılabilir. Bu raporlar, belirli bir zaman dilimindeki araç hareketlerini, sık kullanılan rotaları ve araçların sıklıkla girdiği alanları inceleme imkânı sağlar.
- Trafik Yönetimi: Otomatik plaka tanıma, trafik akışını düzenlemek ve trafik cezalarını yönetmek için kullanılır. Örneğin, bir araç hız sınırını ihlal ettiğinde veya yasaklı bölgelere girdiğinde sistem aracın plakasını tanır ve cezai işlem başlatılabilir.

3.2.4.5. Araç algılama sistemleri

Araç algılama sistemleri, yasak bölgelere izinsiz girişleri, trafik ihlallerini ve hız sınırı aşımlarını tespit etmek için kullanılır. Bu sistemler sayesinde, yasaklı bölgelere giren şüpheli araçlar otomatik olarak izleme listeleriyle eşleştirilebilir. Ayrıca birden fazla kamera ve konum bazlı takip teknolojileriyle araç hareketleri analiz edilerek anlık uyarılar oluşturulabilir. Olay yeri incelemelerinde, şüpheli araçların plakaları kaydedilerek adli soruşturmalarda delil olarak kullanılabilir (Bayram, 2020). Araç algılama veya takip sistemi, araçların anlık konumlarını izleyerek güvenliği artıran bir teknolojik çözümdür. Bu sistem, araçların rotalarını takip etmekle kalmaz, aynı zamanda önceden belirlenen güzergâhın dışına çıkılması durumunda merkezi uyarı sistemine bilgi gönderir. Ayrıca, araçların belirli hız limitlerinin üzerinde hız yapması durumunda da merkezi uyarı alır (Kocaman, 2020).

Acil durumlar için özel olarak tasarlanmış bir acil durum butonu sayesinde, şoförler olası tehlike anlarında bu butona basarak merkeze anında uyarı gönderir. Bu uyarı, sesli ve görüntülü iletişimle daha detaylı bilgi sağlanmasını mümkün kılar. Özellikle sürücünün tehlikede olduğu durumlarda, müdahale ekiplerinin hızlı bir şekilde yardıma ulaşmasına olanak tanır. Kaza ya da çarpışma gibi durumlar gerçekleştiğinde de araçtan otomatik olarak acil durum uyarısı merkeze gönderilir. Böylece herhangi bir kaza anında hızlıca yardım alınabilir (Bayram, 2020). Ayrıca araç içinde meydana gelen saldırı, hırsızlık veya taciz gibi olumsuz durumlar da acil durum butonuyla bildirilir ve yetkililere hemen haber verilerek güvenlik sağlanır (Akpulat, 2017). Bu sistem, tüm bu uyarıları anında merkeze ileterek, olaylara hızlı müdahale edilmesini sağlar.

3.2.4.6. Lte telsiz haberleşme sistemleri

Acil durumlarda LTE tabanlı telsiz sistemleri, hızlı ve güvenli iletişimi mümkün kılar. Bu sistemler ses, veri ve video akışlarını anlık olarak ileterek kolluk kuvvetleri ve acil durum ekiplerinin koordinasyonunu sağlar. Olay yerinde bulunan kolluk kuvvetlerinin HD video yayınları, merkezi operasyon birimine anında aktarılabilir ve durum değerlendirmesi yapılabilir (Ersoy ve Yiğit, 2017). Akıllı kent projelerinde park gibi açık hava mekanlarına özel projeler düşünülmektedir. Şehirlerdeki parklarda güvenliği artırmak amacıyla geliştirilen bir akıllı şehir uygulaması bulunmaktadır. Bu proje, parklarda gerçekleşebilecek çeşitli suçlar, kaybolan eşyalar, şüpheli paketler veya kaybolan çocuklar gibi olumsuz durumlara karşı etkili önlemler almak için entegre akıllı sistemler kullanmayı amaçlamaktadır. Güvenlik, telsiz haberleşme projesinin en temel unsurudur ve bu projeyle birlikte, parklarda görev yapan güvenlik

birimleriyle koordineli bir şekilde çalışan teknolojik sistemlerin kurulması sağlanmıştır (Dahlman vd., 2013). Böylece olası tehditler anında tespit edilip, müdahale edilebilir.

LTE tabanlı telsiz sistemleri parklarda kullanılacak çeşitli akıllı sistemler arasında akıllı video sistemi, akıllı operasyon merkezi takip sistemi ve LTE telsiz bildirim sistemi yer alır. Bu sistemler, parkların güvenliğini sağlamak amacıyla tasarlanmıştır. Kaybolan eşyaların veya şüpheli nesnelerin tespiti anında komuta merkezine bildirilecek şekilde bir altyapıya sahiptir. Ayrıca kaybolan çocuklar veya kara listede yer alan şüpheli şahıslar da bu sistemlerle tespit edilerek yetkililere bildirilir. Parklardaki güvenlik güçleri ile entegre çalışan bu sistemler, hızlı ve etkili bir müdahale imkanı sunar (Ersoy ve Yiğit, 2017). LTE telsiz bildirim sistemi, güvenlik güçlerinin kesintisiz iletişim kurabilmesini sağlayan bir altyapıdır. Bu teknoloji, parklar gibi geniş alanlarda çalışan güvenlik birimlerinin, acil durumlar, yangınlar, kazalar veya güvenlik tehditlerine karşı birbirleriyle hızlı bir şekilde iletişim kurmalarını mümkün kılar. LTE telsiz sistemleri sayesinde, güvenlik ekipleri sesli ve görüntülü iletişim kurabilirken ayrıca fotoğraf, video, belge ve diğer dosyalar da hızlıca paylaşılabilir (Klaue vd., 2003).

Bu akıllı sistemlerin avantajı, acil durumlarda şebeke kullanımı önceliklendirilerek kesintisiz bir iletişim sağlanmasıdır. 4G ve LTE teknolojilerinin kullanılması, güvenlik ekiplerinin her koşulda etkili bir şekilde haberleşmesini ve gerektiğinde hızlı bir şekilde müdahale etmelerini sağlar (Ersoy ve Yiğit, 2017). Bu sayede, güvenlik risklerinin minimize edilmesi ve olaylara hızlı bir şekilde tepki verilmesi mümkün olur.

3.2.4.7. Gerçek zamanlı istihbarat sistemleri

Gerçek zamanlı istihbarat sistemleri, sosyal medya, güvenlik kameraları, sensörler ve diğer kaynaklardan elde edilen verileri bir araya getirerek kolluk kuvvetlerine ve güvenlik birimlerine anlık bilgi akışı sağlar. Bu sistemler sayesinde; olay yerinden elde edilen canlı veriler, güvenlik tehditlerine karşı hızlı bir şekilde analiz edilebilir. Anlık saha bilgisi, alarm verileri ve performans göstergeleri, operatörler, mühendisler ve saha çalışanlarına mobil cihazlar aracılığıyla iletilerek etkili bir kriz yönetimi sağlanabilir (Kim vd., 2015).

Akıllı şehirler, teknolojiyi ve dijital altyapıyı kullanarak şehirlerin yönetimini daha verimli, sürdürülebilir ve güvenli hale getirmeyi amaçlayan modern bir şehirleşme anlayışıdır (Herzberg, 2017: 58). Bu sistemler, şehirlerin çeşitli hizmetlerini birbirine entegre ederek daha verimli çalışmasını sağlar. Akıllı şehir uygulamaları genellikle sensör ağları, veri toplama ve analiz sistemleri, yapay zeka ve nesnelerin interneti (IoT) gibi teknolojilerle desteklenir. Akıllı şehirlerin temel bileşenlerinden biri, şehrin farklı alanlarında veri toplayan sensörlerin

yerleştirilmesidir. Bu sensörler, ulaşım, enerji kullanımı, hava kalitesi, gürültü seviyesi gibi pek çok konuda anlık veriler sağlar. Toplanan bu veriler, şehir yöneticilerine şehirdeki durum hakkında gerçek zamanlı bilgi sunar ve bu sayede daha hızlı ve doğru kararlar alınabilir. Trafik yoğunluğuna göre ışıklandırma sistemleri otomatik olarak ayarlanabilir, hava kirliliği seviyeleri izlenerek gerekli önlemler alınabilir (Velibeyoğlu, 2019).

Bunun dışında, akıllı şehirlerde genellikle açık veri portalları bulunur. Bu portallar, halkın erişebileceği şekilde şehirle ilgili çeşitli verilerin paylaşılmasını sağlar. Bu sayede vatandaşlar, şehirdeki durum hakkında daha fazla bilgi sahibi olur ve şehir yönetimi ile daha etkili bir iletişim kurulabilir. Güvenlik de akıllı şehirlerin önemli bir parçasıdır. Şehirdeki güvenliği sağlamak amacıyla, gerçek zamanlı suç haritalama, kalabalık yönetimi, akıllı denetim sistemleri gibi teknolojiler kullanılmaktadır (Castells, 1996). Bu sistemler, suç oranlarını azaltmak ve acil durumlara hızlı bir şekilde müdahale etmek için veri analizini kullanır.

3.2.4.8. Olay yeri izleme ve kanıt toplama

Olay yeri izleme sistemleri, suç mahallindeki fiziksel delillerin analiz edilmesini ve suçun aydınlatılmasını kolaylaştırır. Bu sistemler, suç mahallinden alınan görüntü ve videoların dijital ortamda kaydedilmesini ve incelenmesini sağlar. Ayrıca olay mahallinin 3D modelleme yazılımlarıyla sanal olarak yeniden oluşturulması mümkün hale gelir. Böylece adli soruşturmalar için daha ayrıntılı ve doğru rekonstrüksiyonlar oluşturulabilir (Ersoy ve Yiğit, 2017). Olay yeri izleme, analiz ve müdahale destek sistemleri, özellikle güvenlik, acil durum yönetimi ve olay yönetimi alanlarında kritik öneme sahiptir. Bu sistemler, olayların hızla ve doğru bir şekilde izlenmesini, analiz edilmesini ve en uygun müdahale yöntemlerinin belirlenmesini sağlar (Velibeyoğlu, 2019). Olay yeri izleme sistemleri, çeşitli teknolojilerle donatılmıştır ve bu sayede olay yerinde meydana gelen tüm faaliyetler detaylı bir şekilde izlenebilir. Bu tür sistemler, görüntüleme cihazları, sensörler, GPS sistemleri ve diğer veri toplama araçlarını kullanarak olay yerinden gerçek zamanlı bilgi toplar. Elde edilen veriler, olayın büyüklüğüne ve ciddiyetine göre analiz edilerek, hızlı ve doğru müdahale yöntemlerinin belirlenmesine olanak tanır (Kim vd., 2015). Bu sistemlerin temel işlevleri arasında; gerçek zamanlı izleme, veri toplama, veri analizini yapma, müdahale stratejileri geliştirme ve operasyonel kararları destekleme yer alır. Olay yeri izleme ve müdahale destek sistemlerinin sunduğu avantajlar arasında, olay yerinde yapılan yanlış kararların önlenmesi, zaman kaybının önüne geçilmesi ve operasyonel verimliliğin artırılması sayılabilir. Bunlara ek olarak, bu tür sistemlerin özellikle kaza, yangın, doğal afet gibi durumlarda kritik önemi vardır. Polis, jandarma, sağlık ekipleri ve itfaiye gibi kurumlar arasında etkin bir koordinasyon sağlanmasına

yardımcı olur. Tehlikeli maddelerin taşınması veya potansiyel terör saldırıları gibi güvenlik tehditlerinin izlenmesinde de kullanılır (Ersoy ve Yiğit, 2017).

LTE telsiz haberleşme sistemi, mobil haberleşme teknolojisinin bir evrimidir ve yüksek hızlı veri iletimi sağlamak için kullanılır. Acil durumlar ve saha operasyonları için kritik öneme sahip bir iletişim altyapısı sunar. Yüksek veri hızları, düşük gecikme süreleri ve gelişmiş güvenlik özellikleri ile modern mobil iletişim sistemleri arasında yer alır (Ersoy ve Yiğit, 2017). Bu özellikler, güvenlik güçlerinin olay yerlerinde gerçek zamanlı iletişim kurmalarını sağlar. Acil servisler için geniş alanlarda kesintisiz iletişim olanağı sunar. Bu teknoloji, birden fazla cihaz ve sistem arasında hızlı ve güvenli veri aktarımına imkan tanıyarak, koordinasyonu artırır ve olaya hızlı müdahale edilmesini sağlar (Dalhman vd., 2013). Polis ve itfaiye ekipleri, LTE üzerinden anlık olarak olay yerindeki görüntüleri, sesli iletişimi ve diğer verileri birbirleriyle paylaşarak ortak bir strateji geliştirebilirler.

LTE sistemlerinin yüksek güvenilirlik ve yüksek bant genişliği özellikleri, özellikle olay yeri izleme ve analiz süreçlerinde önemli rol oynar. Olay yerinden gelen videolar, sesli iletişim ve veri analizleri, LTE üzerinden yüksek hızda aktarılabilir. Bu sayede, olayla ilgili tüm detaylar zaman kaybı olmadan merkeze iletilir ve ilgili kurumlar hızlıca müdahale eder.

3.2.4.9. Dron tabanlı güvenlik sistemleri

Dronlar, önceden belirlenen rotalarda otomatik olarak uçuş yaparak güvenlik tehditlerini tespit edebilir ve anlık olarak veri aktarımı gerçekleştirebilir. Bu sistemler, geniş ve engebeli arazilerin izlenmesini kolaylaştırır. Yapay zeka destekli analiz sistemleri sayesinde anormallikler tespit edilerek güvenlik ekiplerine anında bilgi verilir (Genç ve Erciyes, 2020). Sınır güvenliği, kaçakçılık ve doğal afet bölgelerinde dronlar, güvenlik operasyonlarını desteklemek için kullanılabilir. Günümüzde dronlar, çeşitli kötü amaçlar için kullanılabiliyor. Güvenlik ve emniyet açısından ciddi tehditler oluşturuyor. Özellikle terör bölgelerinde, savaş alanlarında, hapishanelerde ve bazı stratejik noktalarda dronların kötüye kullanımı büyük bir endişe kaynağıdır. Dronların sağladığı yüksek manevra kabiliyeti, uzun menzilli uçuşlar yapabilme kapasitesi ve düşük maliyetleri, onları çeşitli kötü amaçlı faaliyetler için cazip bir araç haline getirmiştir (Jian vd., 2018: 1150; Stasiak vd., 2018).

Dronların en yaygın kullanım alanlarından biri, istihbarat ve gözetim faaliyetleri çerçevesinde gerçekleştirilen casusluk amaçlı uygulamalardır. Dronlar, sahip oldukları yüksek çözünürlüklü kameralar ve ses kayıt sistemleri aracılığıyla gizli veri toplama kapasitesine sahiptir. Bu teknolojik yetenekler, devlet kurumları, özel sektör kuruluşları ve bireyler

açısından ciddi güvenlik açıkları doğurabilmektedir. Özellikle askeri üsler veya stratejik öneme sahip tesislerin çevresinde izinsiz olarak uçurulan dronlar, hem istihbarat toplama amacıyla kullanılabilir hem de savunmasız bölgelerdeki hedeflere odaklanarak düşman unsurlar tarafından tehdit unsuru hâline gelebilir. Bununla birlikte dronlar, terörist saldırılar için de bir araç haline gelebilir. Üzerlerine yerleştirilen patlayıcılarla birlikte, dronlar uzaktan kumanda ile istenilen hedefe yönlendirilip patlatılabilir (Genç ve Erciyes, 2020). Bu tür saldırı olasılıkları, hem sivil hem de askeri hedefler üzerinde ciddi güvenlik riskleri yaratabilir. Özellikle dronlar aracılığıyla taşınabilen patlayıcı materyaller, hem fiziksel güvenliği hem de kamu düzenini ve toplumsal istikrarı tehdit eden önemli unsurlar arasında yer almaktadır.

Bir diğer kötü kullanım senaryosu, hapishaneler gibi güvenlikli alanlara dışarıdan yasa dışı eşyaların taşınmasıdır. Dronlar, cezaevleri gibi kapalı alanlara yasadışı malzeme, silah veya uyuşturucu taşıyabilir. Cezaevlerinde güvenlik ihlalleri ve ciddi sorunlara yol açabilir. Bu tür tehditleri engellemek ve dronların kötü amaçlarla kullanımını önlemek amacıyla güvenlik güçleri tarafından çeşitli dron karşıtı sistemler geliştirilmektedir. Bu sistemler dronların sinyallerini tespit edebilecek radarlar, jamming (sinyal engelleme) cihazları veya etkisiz hale getirme teknolojileri ile donatılmıştır (Kumar, 2019). Ayrıca dronları tanıyıp izlemek için gelişmiş görüntü işleme ve yapay zeka teknolojileri de kullanılmaktadır.

Frekans izleme de, dronları kontrol eden sinyalleri tespit etmek için etkili bir yöntemdir. Özellikle 2.4 GHz ve 5 GHz bandındaki sinyallerin izlenmesi, izinsiz dronların tespit edilmesine olanak tanıyabilir. Bu tür sinyal tespiti ile, güvenlik güçleri, dronların kontrol merkezlerine müdahale edebilir veya dronları yönlendiren kişilere karşı etkili önlemler alabilir. Dronların kötü amaçlarla kullanımı ciddi güvenlik tehditlerine yol açmaktadır ve bu tehditlerin önüne geçmek için teknolojik, operasyonel ve yasal önlemler bir arada uygulanmalıdır. Gelişen teknolojilerin sağladığı fırsatlar, aynı zamanda yeni tehditler oluşturmakta; bu tehditlerle başa çıkabilmek için ise güvenlik alanında sürekli yenilikler ve iyileştirmeler yapılması gerekmektedir (Ersoy ve Yiğit, 2017).

3.2.4.10. Liman izleme ve deniz güvenliği sistemleri

Su altı sensör teknolojilerinin gelişimiyle birlikte, limanlar ve kıyı bölgelerinde bütüncül bir güvenlik altyapısının oluşturulması mümkün hâle gelmiş; bu sayede su altı ve su üstü tehditlerin erken tespiti ile güvenlik birimlerinin müdahale kapasitesi önemli ölçüde artmıştır. Bu sistemler, yasa dışı girişleri, kaçak avcılığı ve stratejik bölgelerde meydana gelebilecek tehditleri belirlemek için kullanılmaktadır. Özellikle, nükleer tesisler gibi kritik

altyapıların güvenliği açısından büyük önem taşır (Keskin ve Kum, 2012). Ulaştırma ve Altyapı Bakanlığı seyir emniyetini artırmak amacıyla, deniz kazalarının meydana gelme risklerini azaltmayı ve böylece can ve mal kayıplarını asgari düzeye indirmeyi hedeflemektedir. Bu doğrultuda, özellikle elektronik ve haberleşme teknolojilerindeki uluslararası gelişmelerden azami derecede faydalanarak, deniz trafiğinin etkin bir şekilde izlenmesini sağlayan sistemler kurulmuştur. Bu sistemler arasında, uluslararası denizcilik organizasyonları olan IMO (Uluslararası Denizcilik Örgütü) ve IALA (Uluslararası Deniz Fenerleri ve İşaretleme Birliği) tarafından onaylanmış olan Gemi Trafik Hizmetleri (GTH) Sistemi, Otomatik Tanımlama Sistemi (OTS) ve Uzak Mesafeden Gemilerin Tanımlanması ve İzlenmesi (LRIT) Sistemi gibi yenilikçi teknolojiler yer almaktadır (Demir, 2016).

Türkiye'nin stratejik öneme sahip Türk Boğazları bölgesi, İstanbul ve Çanakkale Boğazları ile Marmara Denizi'ni kapsayan bir alandır ve bu bölge, 164 deniz mili uzunluğunda olan ve alternatifleri bulunmayan, ulusal ve uluslararası deniz trafiğinin yoğun olduğu bir suyolu olarak tanımlanmaktadır. Coğrafi, morfolojik ve oşinografik yapısı itibariyle oldukça riskli bir bölge olan Türk Boğazları, hızı saatte 7-8 deniz miline ulaşan akıntılar, rüzgar, topuk ve adacıklar gibi zorlayıcı unsurlar barındırmaktadır. Emniyetli seyir için manevra yapmayı zorlaştırmaktadır. Bu yoğun deniz trafiği ve Türk Boğazları'nın riski göz önünde bulundurulduğunda, olası bir deniz kazasının sonuçlarının, İstanbul'da olabilecek büyük bir depremden farksız derecede tehlikeli olabileceği açıktır. Bu risklere örnek olarak, geçmişte İstanbul Boğazı'nda gerçekleşmiş olan INDEPENDENTA ve NASSIA kazalarında yaşanan büyük tehlikeler verilebilir (UEIM, 2020). Bu tür kazalar, yalnızca bölgenin tarihi ve doğal çevresini tahrip etmekle kalmayıp, aynı zamanda bölgesel güvenlik dinamiklerini de olumsuz yönde etkileyen çok boyutlu tehditler oluşturmaktadır.

Türk Boğazları'ndaki deniz trafiği, giderek artan gemi boyutları, karmaşık trafik yapısı, zorlu hava ve deniz koşulları ile iklim değişiklikleri gibi etmenlerle daha da karmaşık hale gelmektedir. Ayrıca, dar su geçitleri, liman yapıları, köprüler ve diğer altyapı unsurları da gemi trafiğinin güvenli bir şekilde yönetilmesini zorlaştıran unsurlar arasında yer almaktadır. Bu sebeplerle, Türk Boğazları'nda deniz trafiğini aktif olarak izleyebilecek modern bir Gemi Trafik Hizmetleri (GTH) Sistemi kurmak, hem ulusal hem de uluslararası düzeyde zorunlu hale gelmiştir. Bu sistem Türkiye'de 30 Aralık 2003 tarihinde faaliyete geçirilmiştir. İstanbul ve Çanakkale Boğazlarında olmak üzere iki merkez ve 16 Trafik Gözetleme İstasyonu'ndan oluşmakta olup, deniz trafiği ile ilgili çeşitli verileri toplayan, işleyen ve yayabilen bir altyapıya sahiptir. Bu sistemde, deniz trafiği radarlar, Otomatik Tanımlama Sistemi (OTS), kapalı devre

televizyon kameraları, elektronik haritalar ve telsiz sistemleri gibi çeşitli teknolojilerle izlenmektedir (UEIM, 2020).

TBGTH sistemi bilgi hizmeti, seyir yardımı hizmeti ve trafik organizasyon hizmeti olmak üzere üç ana hizmet sunmaktadır. Sistemin en temel görevi, GTH alanında bulunan gemilerin izlenmesi, gemilere ihtiyaç duydukları bilgilerin aktarılması ve tavsiyelerde bulunulmasıdır. Bu görev için radarlar ve diğer algılayıcılar ile gemilerin varlıkları, pozisyonları, kimlikleri gibi veriler toplanmakta ve aynı zamanda çevresel koşullar, meteorolojik ve hidrografik veriler de izlenmektedir. Elde edilen bu veriler, sistem operatörlerine iletilmekte ve arşivlenmektedir. TBGTH Sistemi'nin işleyişi, deniz trafiğini sürekli izlemeyi ve potansiyel tehlike oluşturan durumları tespit etmeyi amaçlamaktadır. Sistem operatörleri, gemilerle iletişime geçerek, gerekli bilgileri aktarmakta ve tavsiyelerde bulunarak gemilerin tehlikelere karşı önlem almasını sağlamaktadır (Balık vd., 2022). Bu sayede deniz kazalarının önlenmesi için etkin bir müdahale sağlanmakta ve gemi trafiği daha güvenli hale getirilmektedir.

3.2.5. Kamu güvenliğine yönelik teknolojik çözümler

1980'li yıllardan itibaren ulusal güvenliğin yanı sıra kamu güvenliği ve buna bağlı olarak şehir güvenliği kavramları, politika gündeminde önemli bir yer edinmiştir (Köseoğlu, 2019: 44). Geleneksel güvenlik anlayışı, ağırlıklı olarak devletin ve sınırların korunmasını temel alırken, modern güvenlik politikaları suç ve şiddetin önlenmesi, bireylerin güvenliğinin sağlanması ve kamu düzeninin korunması gibi unsurları da içerecek şekilde genişlemiştir. Şehir güvenliği, yalnızca terörizm, suç ve şiddet olaylarını değil, aynı zamanda kadına yönelik şiddet, organize suçlar, uyuşturucu kullanımı, kaçakçılık gibi farklı suç boyutlarını da kapsamaktadır (Yaman ve Çakır, 2018).

Bu bağlamda akıllı güvenlik teknolojileri şehirlerdeki güvenlik tehditlerine karşı hızlı müdahale imkânı sunarak kamu güvenliğinin artırılmasına katkı sağlamaktadır. Yapay zekâ destekli bu sistemler, olası kriz ve risklerin önceden tahmin edilmesine olanak tanımakta ve böylece yetkili birimlerin gerekli önlemleri zamanında almasını sağlamaktadır. Akıllı güvenlik teknolojilerinin temel bileşenlerinden biri olan görüntü tanıma sistemleri, suçluların tespiti ve suç olaylarının önlenmesi açısından kritik bir rol oynamaktadır. Görüntü tanımlama teknolojileri, yüz tanıma sistemleri, biyometrik analizler ve davranışsal izleme gibi unsurlarla desteklenerek, terörden sokak seviyesindeki suçlara kadar geniş bir yelpazede güvenlik tehditlerine karşı etkili çözümler sunmaktadır (Efe, 2021).

Bununla birlikte akıllı güvenlik sistemleri yalnızca suçla mücadelede değil, halk sağlığını tehdit eden unsurların tespitinde de önemli bir işlev görmektedir. Salgın hastalıklar ve biyolojik tehditler gibi ulusal güvenliği etkileyebilecek risk faktörleri, akıllı güvenlik sistemleri aracılığıyla erken aşamada tespit edilerek yayılmadan önce önlem alınmasını sağlamaktadır. Termal kameralar ve yapay zekâ destekli analizler, halk sağlığını tehdit eden enfeksiyonların yayılımını takip edebilir ve riskli bölgelerde karantina süreçlerinin daha etkin bir şekilde yönetilmesine yardımcı olabilir (Balık vd., 2022)

Akıllı güvenlik teknolojileri, hem bireysel hem de toplumsal güvenliğin sağlanması açısından giderek daha fazla önem kazanmaktadır. Kamu güvenliğinin korunması, suç oranlarının azaltılması ve kriz anlarında hızlı müdahale edilebilmesi için bu sistemlerin gelişimi ve entegrasyonu, günümüz şehir yönetiminde vazgeçilmez bir unsur haline gelmiştir.

3.2.5.1. Video gözetim sistemleri

Kapalı devre televizyon (CCTV), kameralar ve akıllı telefonlar gibi gözetim araçları, insan hareketlerini kayıt altına alarak bu verileri analiz edilebilir bilgilere dönüştürmektedir. Günümüzde en yaygın kullanılan gözetim araçları arasında video izleme sistemleri öne çıkmaktadır. Her yıl dünya genelinde yaklaşık 600 petabaytlık video verisinin toplandığı tahmin edilmektedir (Chui vd., 2019). Gözetim sistemlerinde verimliliğin artmasıyla birlikte geleneksel yöntemlerden akıllı sistemlere doğru bir geçiş yaşanmakta ve bu doğrultuda küresel gözetim pazarı hızla büyümektedir. 2019 yılında 42,94 milyar dolar seviyesinde olan video gözetim pazarının, 2027 yılında 144,84 milyar dolara ulaşması öngörülmektedir (Tewari, 2020).

Video analiz teknolojileri, kalabalık ortamlarda bireylerin hareketlerini takip ederek olağan dışı davranışları tespit edebilme kapasitesine sahiptir. Kalabalık hareket analizi, belirli bir alanda şüpheli hareketleri veya güvenlik risklerini tespit ederek ilgili birimlere anında bilgi aktarılmasını sağlar (NEC, 2020). Özellikle toplu etkinliklerde veya yoğun kullanılan alanlarda bu sistemler, insan akışını dengeleyerek güvenliği artırabilir. Şehirlerde yoğun insan hareketliliği, suç ve güvenlik risklerini beraberinde getirebilir. Bu tür riskleri en aza indirmek için geliştirilen akıllı güvenlik çözümleri, alan giriş-çıkış kontrolü, sıra dışı hareket analizi ve erken uyarı sistemleri ile güvenlik önlemlerinin etkinliğini artırmaktadır.

Büyük etkinlikler, toplu alanlarda güvenlik risklerini artırabileceği gibi bireysel tehditlere de zemin hazırlayabilir. Bu tür durumlarda gelişmiş güvenlik teknolojileri, kriz yönetimini destekleyerek olası tehlikelere karşı daha hızlı ve etkili müdahaleyi mümkün kılar

(NEC, 2020). Video gözetim sistemleri yalnızca suçların önlenmesi değil, aynı zamanda kazaların erken tespit edilmesi ve ilgili birimlerin zamanında müdahale etmesi açısından da kritik bir rol oynamaktadır. Birbirine entegre çalışan bu sistemler, anlık izleme ve bildirim mekanizmalarıyla güvenlik güçlerine eş zamanlı bilgi aktarımı yaparak şehir güvenliğine katkı sunmaktadır.

CCTV'ler veya video gözetim sistemleri, gerek kamusal gerek özel alanlarda temelde güvenliğin sağlanması amacıyla yaygın olarak kullanılmaktadır. Video gözetim sistemleri, veri akışının esas olarak kameradan kontrol merkezine doğru ulaştığı bir yapı olarak, izinsiz giriş dedektörü tarafından verilen alarmı kontrol etmek için devriye muhafızları veya polislerin yerini almak üzere güvenlik alanında fiziksel koruma sistemlerine dahil edilmiştir (Welsh ve Farrington, 2008).

Gözetim yapan video kayıt sistemleri, 2005 yılındaki Londra bombalamalarının soruşturma sürecinde şüphelileri tespit etmekte olduğu gibi, suç sonrasındaki süreçte önemli ipuçları sağlamıştır. Bu durum, hükümetlerin video gözetim sistemlerinin şehir yaşamının güvenliği ve kamusal güvenlik açısından kritik olduğunu düşünmesine neden olmuştur (Gill ve Spriggs, 2005). 13 Kasım 2022'de İstanbul İstiklal Caddesi'nde gerçekleşen bombalı saldırıyı gerçekleştiren kişinin de güvenlik kameraları sayesinde tespit edilmesi, CCTV'nin suç çözümündeki rolünü bir kez daha göstermiştir (İçişleri Bakanlığı, 2022).

Bir video gözetim sistemi, analog ve dijital cihazlar ile bir yazılımdan oluşur. Buradaki amaç, bir sahnenin görüntülerini yakalamak, görüntü işlemek ve bunları bir operatöre göstermek olarak özetlenebilir (Armitage, 2002: 173). Kapalı devre görüntü ve kayıt sistemleri (CCTV), bir veya birden fazla kamera kullanarak belirli bir alanın izlenmesini, bu görüntülerin kaydedilmesini ve gerektiğinde video şeklinde oynatılmasını sağlar (Armstrong ve Norris, 2020).

Teknolojik gelişmeler CCTV'lerin kurulum ve kullanım maliyetlerini düşürdüğünden, bu sistemler banka, kalabalık cadde ve sokaklar ile eğitim kurumları gibi kamusal alanlarda yaygın olarak kullanılmaya başlanmıştır. 2021 yılı itibarıyla dünya genelinde yaklaşık 1 milyar gözetim kamerasının kurulu olduğu tahmin edilmekte olup, bu sayı her sekiz kişiye bir kamera düşecek düzeye ulaşarak küresel ölçekte yaygın bir denetim mekanizmasının varlığına işaret etmektedir. (IHS Markit, 2021). Ancak CCTV yoğunluğu ülkeden ülkeye farklılık göstermektedir. 2021 yılı itibarıyla Çin ve ABD'de sırasıyla 4,1 ve 4,6 kişiye bir kamera düştüğü; en yüksek CCTV yoğunluğuna sahip 10 şehirden altısının Çin'de, üçünün ise

Hindistan'da olduğu belirtilmektedir. Asya dışındaki Londra, New York, İstanbul ve Paris gibi metropollerde de CCTV'ye sıkça başvurulmaktadır (Statista, 2021).

Suç oranları ve kişi başına düşen CCTV analizleri, güvenlik-gözetim-mahremiyet dengesi konusunda farklı ülkelerde tartışmalara yol açmaktadır. Suç endeksi 46,29 olarak hesaplanan New York'ta 1 km² başına 25,97 CCTV düşmekte ve toplam kamera sayısı 31.490 olarak ifade edilmektedir. Suç endeksi 47,85 olan İstanbul'da ise 1 km² başına 42,3 CCTV düşmekte ve toplam cihaz sayısının 109.000 olduğu belirtilmektedir. Paris için bu rakam 26.834, Bağdat için 120.000, Moskova için 193.000 ve Pekin için 1.150.000 olarak kaydedilmiştir (Numbeo, 2021). Ancak CCTV'lerin yalnızca suç oranlarına veya belirli bir alanın büyüklüğüne göre kurulup kurulmayacağı tartışmalı bir konudur.

CCTV, bir tür durumsal suç önleme stratejisi olarak suç fırsatlarının sayısını azaltmayı ve fiziksel çevrenin değiştirilmesi yoluyla algılanan suç işleme riskini artırmayı hedefler (Clarke, 1992: 178). CCTV'nin birincil amacı, suçluyu suçtan kaçınmaya yönlendirecek şekilde seçim yapılandırma mekanizmalarını devreye sokmaktır (Welsh ve Farrington, 2009: 179). Bununla birlikte, CCTV sistemlerinin kurulma ve kullanım amaçları genel olarak güvenlik, gözetleme ve denetleme şeklinde üç ana kategoride değerlendirilmektedir (Goold, 2004).

3.2.5.2. Trafik gözetimi

Dünya nüfusundaki hızlı artışa paralel olarak şehir içi motorlu taşıt sayısının da önemli ölçüde yükselmesi, özellikle metropol alanlarda trafik yoğunluğunu ciddi şekilde artırmakta; bu da mevcut ulaşım altyapılarının artan talep karşısında yetersiz kalmasına ve kent içi hareketliliğin sekteye uğramasına neden olmaktadır (Numbeo, 2021). Trafik yoğunluğunun artması, ulaşımda verimlilik kayıplarına, güvenlik tehditlerine ve çevresel olumsuzluklara yol açmaktadır. Bu bağlamda, şehirlerde ulaşım sistemlerinin yeniden yapılandırılması ve iyileştirilmesi gerektiği açıktır. Günümüzde trafik kazaları, küresel ölçekte önemli bir halk sağlığı sorunu olarak karşımıza çıkmaktadır. Her yıl dünya genelinde 1 milyondan fazla insan trafik kazaları nedeniyle hayatını kaybetmekte, 50 milyondan fazla kişi ise yaralanmaktadır (Chui vd., 2019). Trafik güvenliğini sağlamak ve trafik ihlallerini minimize etmek amacıyla video gözetim sistemleri giderek daha yaygın hale gelmiştir. Özellikle yoğun kullanılan bölgeler, kavşaklar ve yaya geçitleri gibi kritik noktalara yerleştirilen gözetim sistemleri, sürücü davranışlarını izleme ve ihlalleri tespit etme açısından önemli bir rol oynamaktadır.

Kapalı devre televizyon (CCTV) sistemleri, trafik izleme ve kontrol süreçlerinde merkezi bir yer tutmaktadır. Otomatik plaka tanıma, hız tespiti ve kural ihlallerinin belirlenmesi

gibi işlevlere sahip olan bu sistemler, trafik akışını düzenlemek ve kazaları önlemek amacıyla kullanılmaktadır. Kamera ve sensörler aracılığıyla trafik yoğunluğu analiz edilerek sürücülere alternatif güzergâh önerileri sunulmakta ve böylece ulaşım planlamasına katkı sağlanmaktadır. CCTV sistemleri, temel olarak analog ve dijital olmak üzere ikiye ayrılmaktadır. Geleneksel analog CCTV sistemleri, bir kayıt cihazı ve kameraların görüntülerini aktardığı bir monitörden oluşmaktadır. Analog sistemlerde görüntüler kablo aracılığıyla merkezi bir kayıt sistemine iletilmekte ve burada işlenmektedir (Zhang vd., 2017). Ancak teknolojik gelişmeler ile birlikte dijital video kayıt sistemlerinin yaygınlaşması, analog sistemlere olan ihtiyacı giderek azaltmaktadır.

Analog CCTV sistemleri, düşük maliyetli olmaları ve basit kurulum süreçleri nedeniyle tercih edilmektedir. Bununla birlikte analog sistemlerin sınırlı görüntü kalitesi, kablolama gereksinimi, sınırlı kapsama alanı ve güvenlik zafiyetleri gibi dezavantajları bulunmaktadır (Smith ve Brown, 2021). Dijital CCTV sistemleri ise yüksek çözünürlüklü görüntü kaydı yapabilme, geniş kapsama alanı sunma ve uzaktan erişim imkânı gibi avantajlara sahiptir. IP (Internet Protocol) destekli kameralar, ağ bağlantısı üzerinden çalışarak merkezi bir kayıt sistemine görüntüleri iletmekte ve böylece daha esnek bir yapı sunmaktadır (Jones, 2022). IP tabanlı CCTV sistemlerinin kurulumunda ayrı bir iletişim hattına ihtiyaç duyulmamaktadır. Bu sistemler, mevcut yerel ağlara entegre edilebildiği için ekstra kablolama gereksinimini ortadan kaldırmaktadır. Ayrıca, şifreleme ve veri güvenliği açısından daha gelişmiş koruma mekanizmalarına sahip oldukları için tercih edilmektedir (Garcia, 2023). Bununla birlikte, yüksek başlangıç maliyeti ve geniş bant genişliği ihtiyacı gibi dezavantajları da bulunmaktadır.

Ulaşımı daha güvenli, verimli ve sürdürülebilir hale getirmek için trafik yönetim birimlerinin, sürücülerin, yolcuların ve yayaların trafik ve yol koşulları hakkında sürekli bilgi edinmelerine olanak tanıyan bir teknolojik altyapının kurulması gerekmektedir. Bu altyapının sağlanabilmesi, hızla gelişen bilişim teknolojileri sayesinde mümkün hale gelmiştir. Bu bağlamda ulaşım sistemleri kavramları modern ulaşım problemlerini çözmeye yönelik önemli bir çözüm önerisi olarak öne çıkmaktadır. Trafik akışını düzenlemek, güvenliği artırmak ve çevresel etkileri minimize etmek amacıyla kullanılan gelişmiş bilgi ve iletişim teknolojilerine dayanan uygulamalardır (Aslan, 2024). Bu sistemler, trafik yönetimi, sürücüler, yolcular ve yayalar için gerçek zamanlı bilgi sağlayarak ulaşımın daha etkili hale gelmesini sağlar. Akıllı sistemler, sistem fonksiyonlarını belirleyen giriş ve durum değişkenlerinin gerçek zamanlı olarak ölçülmesi ve bu verilerin uygun şekilde işlenmesi ile çalışır (Yamin vd., 2021). Bu

sistemlerin etkin bir şekilde çalışabilmesi için sensörler, bilgisayar sistemleri ve iletişim altyapıları gerekmektedir.

Akıllı ulaşım sistemlerinin temeli, trafik verilerinin doğru bir şekilde toplanması ve işlenmesidir. Trafik akışını izlemek için kullanılan sensörler, yol durumu ve trafik yoğunluğuna dair verileri sürekli olarak toplar. Bu veriler, yüksek işlem gücüne sahip bilgisayar sistemlerinde işlenir ve ardından çıkış bilgileri, gerekli durumlarda uzak mesafelere iletilir. Bu sayede trafik yönetimi daha etkin hale gelir ve anında müdahale imkanı doğar. Ayrıca trafik akışını optimize etmek için kullanılan algoritmalar sayesinde, trafik ışıkları ve yönlendirme sistemleri akıllıca ayarlanabilir, böylece trafik sıkışıklığı minimize edilir (Aslan, 2024). Trafik güvenliğini artırmak için de önemli avantajlar sunar. Sistemler, trafik kazalarını önceden tespit edebilir ve kazaların gerçekleşmesinden önce sistem tarafından gerekli uyarılar yapılabilir. Bunun yanı sıra, kaza ve tıkanıklıkların hızlı bir şekilde tespit edilmesi ve anında müdahale edilmesi, yol güvenliğini artırır. Ayrıca, sistemler, çevresel faktörleri de göz önünde bulundurarak, yakıt tüketimini ve emisyonları azaltmaya yönelik çözümler sunulabilir.

Trafik kazalarının önlenmesi ve güvenli sürüş koşullarının sağlanması açısından video gözetim sistemleri kritik bir öneme sahiptir. Teknolojik ilerlemeler doğrultusunda IP tabanlı kameraların daha fazla benimsenmesi ve yapay zeka destekli analiz sistemlerinin entegrasyonu ile trafik yönetimi süreçleri daha etkin hale getirilebilecektir. Akıllı sistemlerin avantajı, ulaşım altyapısının daha verimli kullanılmasını sağlamasıdır. Trafik ışıklarının akışa göre ayarlanması, araçların daha hızlı bir şekilde ilerlemesini sağlayarak yolculuk sürelerini kısaltabilir. Hem ekonomik açıdan fayda sağlar hem de trafik sıkışıklığının önüne geçer (Yamin vd., 2021). Ayrıca sürdürülebilir ulaşım çözümleri üretme amacı güdülerek, çevresel etkiler en aza indirilebilir.

Bugün elektronik, bilgisayar ve haberleşme teknolojilerindeki hızlı gelişmeler, akıllı ulaşım sistemlerinin daha esnek ve etkili bir şekilde uygulanmasını sağlamaktadır. Bu teknolojik gelişmeler sayesinde, farklı şehirlerin ulaşım sistemleri de giderek daha entegre hale gelmektedir. Akıllı ulaşım çözümleri, sadece büyük şehirlerde değil, aynı zamanda daha küçük ölçekli yerleşim yerlerinde de uygulanabilir hale gelmektedir.

3.2.5.3. Akıllı sokak aydınlatması

Akıllı sokak aydınlatma sistemleri, yalnızca kamu alanlarında enerji verimliliğini artırmaz. Aynı zamanda suç tespiti, araç park alanı yönetimi, hava durumu takibi ve güvenlik algısının güçlendirilmesi gibi çok sayıda fonksiyonel avantaj sunar. Günümüzde dünya çapında

pek çok yol, eski teknolojilere dayalı sokak aydınlatma sistemleri ile aydınlatılmaya devam etmektedir. Bu eski tip sokak lambaları, şehirlerin elektrik tüketiminin yaklaşık %40'ını oluşturmaktadır (IoTUK, 2017). Ancak bu geleneksel sistemlerin verimliliği sınırlıdır ve çevresel etkileri göz önünde bulundurulduğunda, daha sürdürülebilir çözümler gereklidir.

Akıllı sokak aydınlatmaları, enerji verimliliğini sağlamak için ilk etapta LED tabanlı aydınlatma sistemlerini kullanır. LED'ler, daha düşük enerji tüketimi ve daha uzun ömürleri ile geleneksel ışık kaynaklarına kıyasla önemli avantajlar sunar. Bu lambaların birbirine bağlanarak merkezi bir yönetim sistemine entegre edilmesi, aydınlatma yönetimini daha esnek ve dinamik hale getirir. Ayrıca bu sistemler ses kaydedici sensörler, kameralar, partikül sayacı gibi ek ekipmanlarla donatılabilir. Böylece akıllı sokak aydınlatmaları, yalnızca ışıklandırma değil, aynı zamanda güvenlik, sağlık, enerji yönetimi ve çevre izleme gibi pek çok alanda da hizmet sunar (IoTUK, 2017).

Akıllı sokak aydınlatma sistemleri, internet hizmeti sağlama, çevre izleme, ulaşım ve park optimizasyonu, dijital tabelalar ve elektrikli araç şarj noktaları gibi fonksiyonları entegre edebilir. Ayrıca, akıllı video kameralar ve ses sensörleri gibi güvenlik özellikleri ile kamusal alanlarda güvenliği artırabilir ve vatandaşların güvenli bir şekilde sokaklarda gezinmelerini sağlayabilir. Bunun yanı sıra, bazı şirketler, trafik kazalarına veya suçlara tanıklık edilmesi durumunda acil çağrı düğmeleriyle vatandaşların hızlıca güvenlik güçlerine bildirimde bulunmalarını sağlar, böylece hızlı ve doğru lokasyon bilgileri ile müdahale süresi kısaltılır. Enerji santralleri ve rüzgar enerjisi santralleri gibi büyük ölçekli enerji üretim alanlarından, evlerde ve işyerlerinde kullanılan elektrik tüketim sistemlerine kadar akıllı aydınlatma teknolojileri geniş bir kullanım alanına sahiptir. Bu sistemler, enerji verimliliğini artırarak, enerji depolama teknolojileri ile entegrasyon sağlar ve tüketicilerin enerji kullanımını optimize eder. Özellikle enerji depolama teknolojileri, binalarda ısıtma, elektrikli araç şarjı gibi ihtiyaçların daha verimli bir şekilde karşılanmasını mümkün kılar ve enerji kullanıcılarının şebeke yönetimiyle entegre olarak enerji üreticisi ve tüketicisi rollerini üstlenmelerini sağlar. Enerji şebekesinin daha dinamik ve verimli çalışmasına katkıda bulunur (Smith ve Brown, 2021).

Akıllı sokak lambaları, anormal durumları ya da trafik desenlerini tespit eden sensörlerle donatılabilir ve bu sensörler, uzak mesafelerden izleme ve ayar yapabilme imkanı tanır. Bu lambalar aynı zamanda gelecekteki iletişim ağları için bir platform işlevi görebilir. Gerçekleştirilen enerji tasarrufları sayesinde, bu sistemler hızlı bir yatırım geri dönüşü (ROI) sağlar. Onları giderek daha popüler hale getirir. Akıllı aydınlatma sistemleri, akıllı şehirlerin en

yaygın kullanılan teknolojileri arasında yer alır. Kopenhag'daki Sustainia adlı düşünce kuruluşuna göre, 2010 ile 2025 yılları arasındaki karşılaştırmalarda, bina iyileştirmeleri sayesinde ısı tüketiminde %20, toplam enerji tüketiminde ise %30'dan fazla azalma sağlanmıştır. Bu tür iyileştirmeler, vatandaşların yaşam tarzlarını değiştirmeden enerji faturalarında önemli tasarruflar elde etmelerine olanak tanımaktadır (Jones, 2022).

3.2.5.4. Suç ve konum tespiti

Günümüz kentlerinde artan nüfus, ekonomik dönüşümler, yoğun kaynak tüketimi ve bu unsurlara bağlı olarak fiziksel altyapı ile temel yaşam kaynaklarına yönelik taleplerin yükselmesi, toplumsal yapıdaki sınıfsal farklılıklar ve mekânsal ayrışmalarla birleşerek güvenlik ihtiyaçlarını daha çok boyutlu ve karmaşık bir hale getirmektedir (Kaypak, 2024). Bu karmaşıklık, kentlerin farklı ekonomik, toplumsal ve siyasal ayrımlar nedeniyle suçun ve suçluların belirli bölgelerde yoğunlaşmasına yol açmaktadır. Suç ve suçluların bu şekilde sınıflanması, güvenlik meselelerinin çözülmesinde önemli bir zorluk yaratmaktadır (Karasu, 2012; Alacadağlı, 2020).

Akustik ateşli silah algılama ve konum tespiti sistemleri, çağdaş güvenlik teknolojilerinin önemli bir bileşeni olarak öne çıkmakta; bu sistemler, çevresel ses dalgalarını algılayan sensörler aracılığıyla silah seslerini tespit ederek, atışın gerçekleştiği konumu belirlemekte ve elde edilen verileri anlık olarak güvenlik birimlerine ileterek hızlı müdahaleyi mümkün kılmaktadır. Bu tür akustik sistemler, dünya genelinde birçok şehirde aktif olarak kullanılmaktadır. New York, Washington D.C. ve San Francisco başta olmak üzere doksandan fazla şehirde aktif olarak kullanılan akustik ateşli silah algılama sistemlerinin, suç oranları üzerindeki etkileri somut verilerle ortaya konmuştur. Örneğin, Las Vegas'ta genel suç oranlarında %25'lik bir azalma, Omaha'da silahlı saldırı mağdurlarında %56 oranında bir düşüş ve Greenville'de uygulamanın ilk yılında silahlı yaralanmalarda %29'luk bir azalma kaydedilmiş; bu bulgular, söz konusu teknolojilerin şehir güvenliğini artırma potansiyelini göstermektedir (Shotspotter, 2020).

Konum tespiti ve olay yeri incelemesi bağlamında öne çıkan bir diğer yenilikçi teknoloji ise dronlardır. Kriz anlarında ya da kriz öncesi süreçlerde, geniş alanların hızlı ve etkin bir biçimde taranması ile olay yerindeki kritik noktaların belirlenmesi genellikle insansız hava araçları (dronlar) aracılığıyla gerçekleştirilmektedir. Özellikle erişimi zor, dağlık veya afet bölgelerinde ve acil müdahale gerektiren durumlarda dronlar, güvenlik ve kurtarma operasyonlarında yüksek işlevsellik sunmaktadır. Bu cihazlar, müdahale ekiplerinin doğru

noktalarda toplanmasını ve en etkin şekilde müdahale etmesini sağlar (NEC, 2020). Bunun yanı sıra, kamusal alanlarda hizmet veren LinkNYC gibi sistemler, toplumsal güvenliği ve acil durum müdahale süreçlerini iyileştiren başka bir örnek teşkil etmektedir. Bu sistem, ankesörlü telefonlara eklenen acil durum düğmeleri ile, vatandaşların internet erişimi, telefon şarjı ve görüntülü görüşme gibi pek çok kamu hizmetine erişimini sağlar. Bu sistem acil durum anlarında vatandaşların eş zamanlı olarak güvenlik güçlerine hızlıca haber verebilmelerini sağlayarak kriz durumlarında müdahale süresinin kısalmasına olanak tanır. Bu tür entegre sistemler, güvenlik yönetiminde önemli bir rol oynayarak toplumsal güvenliği artırmada etkili bir araç olarak kullanılmaktadır.

Kent güvenliği, şehir yönetimleri tarafından suçun önlenmesine yönelik olarak geliştirilen önleyici güvenlik stratejilerinin uygulanması, suç olaylarının meydana gelmesi halinde faillerin etkin biçimde tespit edilerek adli makamlara sevk edilmesi ve nihayetinde kent sakinlerinin huzur ve güvenlik duygusunun sürdürülebilir şekilde korunması süreci olarak tanımlanabilir (Oğultürk ve Şahin, 2020). Bu süreçlerin, kent sakinlerinin temel hak ve özgürlüklerine zarar vermeden ve yaşamlarını tehdit etmeden uygulanması, modern devlet anlayışının bir gerekliliğidir (Payam, 2018; Alacadağlı, 2020). Kent sakinlerinin güvenli bir yaşam sürdürebilmeleri için hem can hem de mal güvenliğinin temin edilmesi büyük önem taşımaktadır. Kent güvenliği, bireylerin toplumsal yaşama aktif katılımını, ekonomik faaliyetlerini sürdürebilmelerini ve günlük yaşamın kesintisiz bir şekilde devamını mümkün kılacak istikrarlı ve korunaklı bir ortamın oluşturulmasını gerektirir (Payam, 2018).

Günümüz şehirlerinde, kent sakinlerinin suç ve saldırılara uğramadan yaşaması, temel bir hak olarak kabul edilmektedir (The CoE, 1992, ET: 09.12.2024). Bu bağlamda, kent güvenliği yalnızca belirli sınıflar veya mahalleler için güvenli alanlar yaratmakla sınırlı kalmamalı, tüm kentte herkes için güvenli yaşam koşullarının oluşturulması hedeflenmelidir (Karasu, 2012; Kaypak, 2024). Modern şehirlerde, insanların teknolojiye daha yatkın hale gelmesi, kentte suç işleme ve suçluları gizleme fırsatlarını artırabilmektedir. Bu, suçun daha kolay işlenmesini mümkün kılarken, aynı zamanda suçun önlenmesi için alınacak önlemleri daha da kritik hale getirmektedir. Bu konuda, ABD'deki Chicago Okulu'nun teorik çalışmaları, suç mekân ilişkisini ve toplumsal anomiyi inceleyerek, suçun şehirlerdeki yayılmasını engellemeye yönelik öneriler geliştirmiştir (Karasu, 2008).

Türkiye'de kentle ilgili politikalar, kalkınma planları çerçevesinde şekillendirilmiştir. Özellikle 1990'lı yıllardan itibaren küreselleşme etkisiyle, Türkiye'de kentlerin kalkınması ile güvenlik arasındaki ilişki daha fazla dikkate alınmaya başlanmıştır. Altıncı Beş Yıllık

Kalkınma Planı'ndan itibaren, sosyal güvenlik, kamu güvenliği, yönetişim ve teknoloji gibi unsurlar, kent güvenliği kavramıyla birlikte ele alınmaya başlanmıştır. 2000'li yıllardan itibaren yönetişim ilkesinin benimsenmesiyle birlikte, çevre, gıda ve siber güvenlik gibi yeni tematik güvenlik alanları kalkınma planlarında öncelikli başlıklar arasında yer almaya başlamış; bu doğrultuda, söz konusu alanlara yönelik kamu politikaları geliştirilmiş ve uygulamaya konulmuştur (Alacadağlı, 2020; Ijaz vd., 2016).

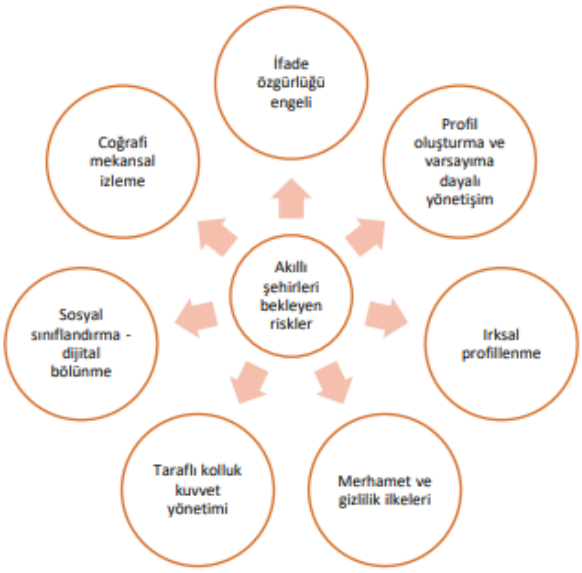
Güvenli kent yaklaşımı, yalnızca suç oranlarının azaltılmasını hedefleyen tedbirlerin ötesinde bir anlam taşır. Kent tasarımının, altyapı eksikliklerinin tamamlanmasının, trafik düzenlemelerinin ve sosyal huzursuzluk yaratan olguların azaltılmasının yanı sıra, kent sakinlerinin yaşam kalitesini artıran ve güvenli yaşam koşulları oluşturan daha geniş bir stratejiyi içerir. Suç oranlarının azaltılması ve çarpık kentleşmenin önlenmesi amacıyla bütüncül bir yaklaşım benimsenmekte; bu sayede, kent güvenliğinin artırılması ve kent sakinlerinin yaşam güvenliğinin sürdürülebilir şekilde temin edilmesi hedeflenmektedir (Karaman, 2019; Alacadağlı, 2020).

Avrupa'da, özellikle İngiltere ve Hollanda'da güvenli kent yaklaşımı, yönetim, hukuk, mimari ve kolluk hizmetlerini kapsayan bir bütünlük içerisinde, suçun önlenmesi amacıyla çevresel tasarım anlayışına dayanmaktadır. Bu yaklaşımda, kent sakinlerinin kent yönetimine katılımı önemli bir yer tutmaktadır. Sivil toplumun da bu sürece dâhil edilmesi, güvenli kentlerin inşasında kritik bir rol oynamaktadır. Birleşmiş Milletler tarafından başlatılan "Güvenli Kentler Programı" ise, suçun önlenmesi için çevresel tasarım odaklı çalışmaların örneklerini sunmuştur. Bu tür çalışmalar, güvenli kent anlayışının kurumsallaştırılması ve yaygınlaştırılması amacıyla yürütülmekte olup, zamanla Avrupa Birliği düzeyinde politika ve uygulamalara da entegre edilmiştir (Gündüzöz, 2016).

Türkiye'de güvenli kent yaklaşımının farkındalık seviyesinin henüz gelişim aşamasında olduğunu söylemek mümkündür. Türkiye'nin mevcut siyasal, ekonomik ve toplumsal koşulları göz önünde bulundurularak, güvenli kent anlayışının bir bütün olarak benimsenmesi ve kamu yönetimi ile politikaların bu yönde şekillendirilmesi gerekmektedir (Alacadağlı, 2020).

4. AKILLI ŞEHİRLERDE DİJİTAL GÜVENLİK TEKNOLOJİLERİNİN BİREYSEL HAK VE ÖZGÜRLÜKLER ÜZERİNDE YARATTIĞI TEHDİTLER

Günümüzde dijital teknolojilerin hızla gelişmesi ve bu teknolojilerin şehir yaşamının pek çok alanında kullanılmaya başlanması, kentlerin işleyişinde köklü dönüşümlere yol açmaktadır. Bu dönüşüm beraberinde, özellikle temel hak ve özgürlüklerin korunmasına ilişkin yeni tartışmaları da gündeme getirmiştir. Bu bağlamda yanıtı aranan önemli sorulardan biri, akıllı şehir uygulamalarının eşitlik, adalet ve katılım temelinde yurttaşların temel hak ve özgürlüklerini ne ölçüde güvence altına alabildiğidir. Mevcut şehir yönetimlerinde, yurttaşların –özellikle yaşlılar, engelliler, göçmenler veya sosyoekonomik açıdan dezavantajlı kişi veya grupların– kentsel gelişim, planlama ve karar alma süreçleri üzerinde etkisi oldukça sınırlıdır. Bu durum, şehirlerin yalnızca teknik olarak değil, aynı zamanda sosyal adalet açısından da kapsayıcı olup olmadığını sorgulamayı gerekli kılmaktadır (Düger, 2023).

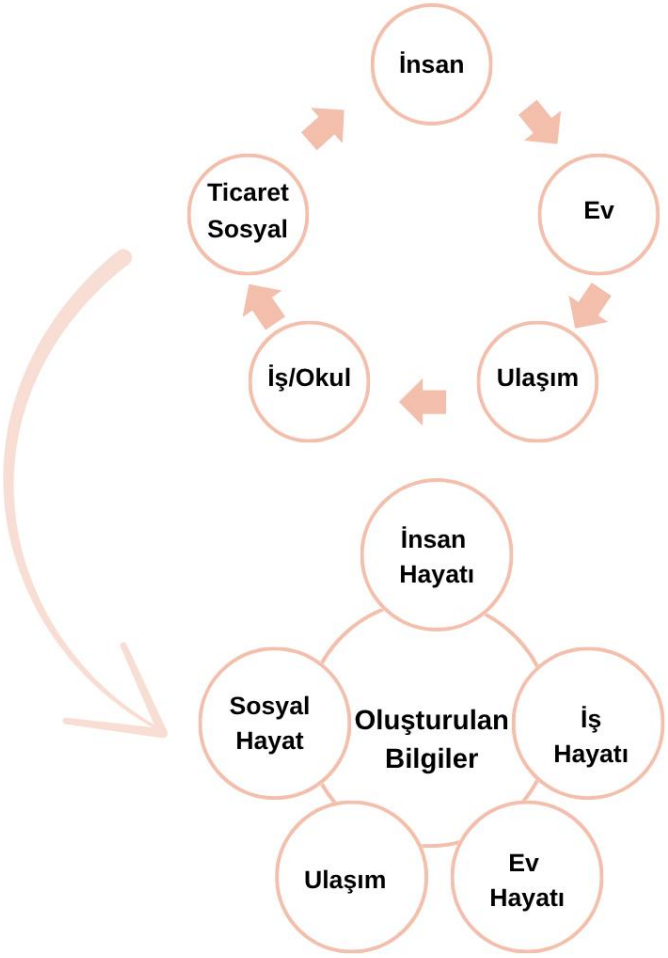


Şekil 4. 1. Hak ve Özgürlükler Açısından Akıllı Şehirleri Bekleyen Tehditler

Kaynak: (Reuter, 2020: 1-19)

Akıllı şehirler bağlamında kullanılan dijital ve gözetim teknolojileri, her zaman gizlilik ya da mahremiyet veya bireylerin diğer temel hak ve özgürlüklerinin ihlali anlamına gelmez. Daha önceki bölümlerde ifade edildiği gibi, bu teknolojiler, güvenlik, ulaşım, enerji verimliliği ve kamu hizmetlerinin etkinliği gibi alanlarda önemli faydalar sağlayabilir. Örneğin, trafik yoğunluğunu azaltmak için kullanılan sensörler veya acil durumlara daha hızlı müdahale

edilmesini sağlayan sistemler, toplumsal yaşamı kolaylaştırabilir. Dolayısıyla, bu tür teknolojilerin kullanımı, bireylerin mahremiyetine zarar vermeden de mümkün olabilir. Ancak bunun sağlanabilmesi için, veri toplama, işleme ve saklama süreçlerinde şeffaflık, denetim mekanizmaları ve etik ilkelerin gözetilmesi büyük önem taşır.



Şekil 4. 2. Veri Toplama, İşleme ve Saklama Süreçleri

Kaynak: (Elmaghraby ve Losavio, 2014: 491-497)

Öte yandan akıllı şehir yaklaşımı, şekil 4.2.'de gösterildiği üzere ortaya çıktığı ilk dönemlerden itibaren çeşitli eleştirilerin odağında yer almıştır. Bu eleştiriler arasında, kenti bir yaşam alanı olarak değil, işleyen bir sistemler ağı olarak tasarlamasıdır. Bu tasarım biçimi, sorunlara yalnızca teknoloji odaklı çözümler sunan indirgemeci bir yaklaşımı içermektedir. Bu yaklaşıma yöneltilen eleştirilerden biri de karar alma süreçlerinde teknokratik yönetişim modellerine öncelik verilmesi ve buna bağlı olarak yönetsel yapının yeniden biçimlendirilmesidir. Ayrıca, kamu hizmetlerinin şirketleştirilmesi ve özelleştirilmesi yönündeki eğilim, daha önce elde edilmiş sosyal hakların ve yatırımların önceliklendirilmesiyle birlikte, kentsel eşitsizlikleri artırma riskini beraberinde getirmektedir. Buna ek olarak, gözetim

pratikleri, tahmine dayalı profil oluşturma süreçleri, bireylerin sosyal olarak sınıflandırılması ve davranışsal yönlendirme tekniklerinin kullanılması gibi uygulamalar, etik açıdan ciddi kaygıların doğmasına yol açmaktadır. Dolayısıyla akıllı şehir teknolojileri, ürettikleri veriler ve onlara uygulanan analitikler, insanların günlük yaşamları üzerinde doğrudan ve dolaylı olarak önemli olumsuz etkileri doğurabilme potansiyeline sahiptir (Kitchin vd., 2019).

Nitekim akıllı şehirler bağlamında kullanılan bazı teknolojik sistemlerin, cinsiyet temelli ayrımcılığı ve toprak mülksüzleştirme gibi olumsuz yanları söz konusudur. Bu teknolojiler, kentsel mekânda kullanıldıklarında gözetimin yaygınlaşmasını kolaylaştırabilir ve bireylerin hareket, örgütlenme ile düşünce özgürlükleri üzerinde caydırıcı etkiler yaratma riski taşırlar. Kolluk kuvvetleri tarafından bu sistemlerin uygulanması, adil yargılanma hakkı ile masumiyet karinesine zarar verebilir. Özellikle azınlıkların ve marjinalleştirilmiş toplulukların polis tarafından ırksal gözetim yoluyla hedef alınması, ayrımcılık yapmama hakkının ihlal edilmesine neden olabilir. Akıllı şehir teknolojileri aynı zamanda vatandaşların kamu hizmetlerine ve mekânsal alanlara erişimini çeşitli biçimlerde sınırlayabilir. Örneğin gerek merkezi yönetimler gerekse yerel yönetimler sosyal yardımları dağıtmak ya da sosyal yardım dolandırıcılığını tespit etmek amacıyla algoritmik sistemler kullandıklarında, mahremiyet, veri koruma, ayrımcılıktan muafiyet, sosyal güvenlik, sağlık ve eğitim gibi temel hakların ihlal edilme riski ortaya çıkmaktadır (Wernick ve Artyushina, 2023). Ayrıca akıllı gözetim sistemleri gibi teknolojik uygulamalar her ne kadar başlangıçta gerçek ve siber ortamlardaki suç davranışlarını izlemek amacıyla geliştirilmiş olsa da, yerel sakinlerin günlük yaşamlarına, yaşam tarzlarına ve mahremiyetlerine ilişkin verileri de kaydedebilmektedir. Benzer biçimde, akıllı evler de hırsızlık ya da olağandışı durumları tespit etmek amacıyla gözetim kameraları kullanmaktadır. Ancak bu tür sistemler, izinsiz giriş gerçekleştiren saldırganların veya yabancı kişilerin evin özel alanına ilişkin mahrem bilgileri kolaylıkla elde etmelerine de zemin hazırlayabilmektedir (Zhang vd., 2017).

Mantelero ve Esposito'ya (2021) göre, akıllı şehir ortamı yalnızca tek bir cihazdan ibaret değildir, veriler ve algoritmalara dayalı çok bileşenli teknik çözümler bütününü içermektedir. Bu bileşenlerin entegre edilmesiyle ortaya çıkan kümülatif etki, parçaların toplamından daha büyük ve karmaşık bir sistemin oluşmasına neden olmaktadır. Bu durum, insan hakları ve özgürlüklerine yönelik potansiyel risklerin yalnızca her bir uygulamanın ayrı ayrı analiz edilmesiyle değerlendirilemeyeceğini ortaya koymaktadır. Bu nedenle, her bir bileşenin kendi başına yaratacağından daha geniş bir etkiye sahip olabilecek bir bütün olarak sistemin ve

bileşenleri arasındaki etkileşimin değerlendirilmesini esas alan entegre bir yaklaşım gerekmektedir (Mantelero ve Esposito, 2021).

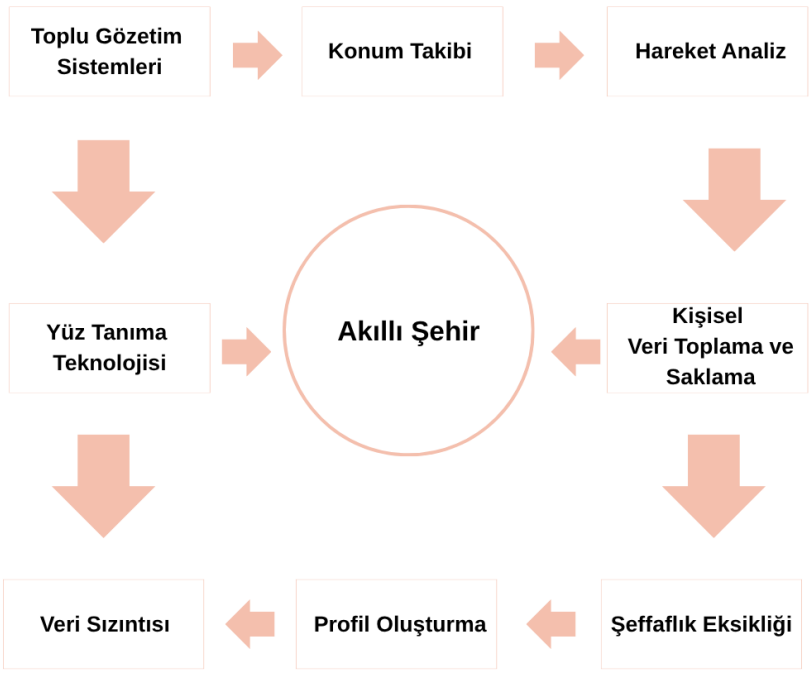
Ağ bağlantılı algılama sistemlerinin ve dijital altyapıların kentsel yaşamda giderek yaygınlaşmasıyla birlikte, akıllı şehir bağlamında şehir hakkına ilişkin sorular günümüzde daha görünür hale gelmektedir (Heitlinger ve Comber, 2018). Özellikle insan yaşamına doğrudan temas eden Nesnelerin İnterneti (IoT) uygulamaları, kişisel cihazlar, akıllı ev sistemleri, akıllı sağlık çözümleri ve akıllı şehir teknolojileri aracılığıyla bireylerin kişisel verilerine erişim sağlayabilmektedir. Bu tür uygulamalarda yer alan nesneler, büyük miktarda kişisel veriyi reklamcılık, dijital pazarlama, istatistiksel analiz ve profil oluşturma gibi farklı amaçlarla veri sağlayıcıları tarafından toplamak amacıyla kullanılmaktadır. Çoğu zaman açık rıza veya zorunlu kabul süreçleri olmaksızın gerçekleştirilen bu veri toplama faaliyetleri, bireylerin özel yaşamının gizliliğine yönelik evrensel insan hakkını ihlal edebilecek niteliktedir. Nesnelerin, bu kişisel verilerin toplanması, depolanması, işlenmesi ve birleştirilmesini kolaylaştırması, mahremiyetin zedelenmesine neden olabilmektedir (Berrehili ve Belmekki, 2016). Bunun yanı sıra her ne kadar akıllı şehir girişimleri yurttaşların yaşam standardını arttırma potansiyeline sahip olsa da mahremiyet, güvenlik ve ifade özgürlüğü gibi diğer insan haklarının ihlal edilmesi gibi durumları ortaya çıkarabilir. Bazı yurttaşlar kamu hizmetlerine eşit erişim imkânı bulamayacağından dolayı, bazı bireylerin internete taşınan kamu hizmetlerinden yararlanmak için gerekli teknolojik becerilere sahip olmaması nedeniyle akıllı bir şehirde kamu hizmetlerine eşit erişim hakkı konusunda zorlanmaktadır. Bu durum, uygun eğitimin verilmemesi veya geleneksel benzerlerinin ortadan kaldırılması durumunda vatandaşlar arasında dijital bir bölünmeye yol açabilir (Hansen ve Skaiaa, 2019). Ayrıca bilişim ve iletişim teknolojilerinin bu denli yaygınlaşması, bazı durumlarda kararları ve politikaları şekillendiren bilgi akışını etkileyebilmektedir. Üretilen ve toplanan verilerin etik dışı biçimlerde seçilmesi, eşitsizliği ve ayrımcılığı derinleştiren taraflı siyasi kararlara zemin hazırlayabilmektedir. Bu durum, toplumsal düzeyde olumsuz sonuçlara yol açma potansiyeli taşımaktadır. Akıllı şehir uygulamaları dünya genelinde yaygınlaştıkça, bu tür senaryoların gerçekleşme olasılığı artmakta ve ortaya çıkabilecek riskler daha tehlikeli boyutlara ulaşmaktadır (Fabregue ve Bogoni, 2023).

Kısacası veri kavramı izleme teknolojileriyle üretilen büyük sayıların ötesine uzanmaktadır. Bu bağlamda şehirlerin veri sistemlerinde kayıtlanan bilgiler, hükümet ya da şirket anketlerinden elde edilen veriler ve sosyal medya paylaşımlarından türetilen içerikleri de kapsamaktadır. Bu veriler, şehirlerin refahı, ekonomik canlılığı veya güvenliği gibi konulara

ilişkin ortak göstergeler üretmek amacıyla giderek daha fazla birleştirilmekte ve birbirine bağlanmaktadır. Yerel yönetimler, bu veri kümelerini giderek daha geniş bir kamuoyuyla paylaşma eğilimindedir. Ancak bu durum, kimin bu verilere meşru biçimde erişebileceği, hangi verilerin kamuya açık hale getirilebileceği ve farklı veri türlerinin nasıl bir gizlilik çerçevesi içinde ilişkilendirilebileceği gibi önemli sorunları gündeme getirmektedir. Bu bağlamda, akıllı şehirlerin siyasal ve kamusal düzeyde kabulü meselesi, bu tür 'verili' şehirlerdeki gündelik yaşam deneyimleri kadar önem arz etmektedir. Kimileri, büyük verinin şehirleri daha zengin, daha temiz ve daha verimli hale getireceğini ileri sürerken; kimileri de şehirlerin, yaratıcılığa ve farklılıklara yer bırakmayan, tamamen veri odaklı ve robotik alanlara dönüşeceği görüşündedir. Nitekim Kitchin (2014), bu tür 'şehir verisi politikaları' ile ilgili olarak, belirli veri toplama ve analiz yöntemlerinin doğurabileceği sosyal sorunlara yeterince dikkat gösterilmediğini belirtmektedir. Ayrıca, şehir süreçlerine dair her alanda veri toplanmasının, daha etkin yönetim biçimleri geliştirmeyi amaçlarken aynı zamanda gizlilik, mahremiyet ve ifade özgürlüğü gibi temel hakları tehdit edebilecek ‘panoptik’ şehirlerin oluşumuna da zemin hazırlayabileceğini vurgulamaktadır (Van Zoonen, 2016). Kitchin, “panoptik şehir” kavramıyla bireylerin sürekli izlendiğini hissettiği ama gözetleyiciyi göremediği bir denetim modelini kastetmektedir. Kitchin, modern akıllı şehirlerin buna benzer bir yapıya doğru evrildiğini savunur. Akıllı şehirlerde kurulan büyük veri merkezleri (örneğin Rio’daki Centro de Operações), trafik kameralarından sosyal medya paylaşımlarına, kamu hizmetlerinden güvenlik sistemlerine kadar çok farklı kaynaklardan veri toplar ve bu verileri birleştirir. Bu yapı, yalnızca fiziksel gözetim (kamera ile izleme) değil, aynı zamanda sayısal gözetim (veri analitiği, algoritmik analiz, veri kümelerinin karşılaştırılması) yoluyla da vatandaşların davranışlarını izlemeyi, tahmin etmeyi ve yönlendirmeyi mümkün kılar. Kitchin burada bir tehlikeye işaret eder: Bu kadar kapsamlı bir veri bütünleştirme ve gözetim ağı, yalnızca şehir yönetimini iyileştirmekle kalmaz; aynı zamanda bireylerin mahremiyetini, özerkliğini ve ifade özgürlüğünü tehdit eden bir gözetim toplumu yaratabilir. Böyle bir şehirde bireylerin hareketleri, tercihleri, alışkanlıkları hatta potansiyel davranışları bile sürekli olarak izlenebilir ve kayda alınabilir. “Hiçbir şeyin unutulmadığı bir dünya” ifadesiyle Kitchin, toplanan verilerin uzun süre saklanması, sürekli analiz edilmesi ve geçmiş davranışlara dayanarak bireylerin gelecekteki kararlarının bile şekillendirilmesi riskine dikkat çeker. Bu durum, kişisel geçmişin silinemezliği ve birey üzerindeki görünmez baskının kalıcılığı anlamına gelir (Kitchin, 2014).

4.1. Mahremiyet hakkının ihlali

Mahremiyet veya gizlilik, modern toplumlarda temel bir insan hakkı olarak kabul edilmektedir. Hukukun, bireylerin kişisel mahremiyetini ve konut dokunulmazlığını koruma altına almasının temelinde, bireyin özel yaşamını dış müdahalelerden uzak tutma gerekliliği yer almaktadır. Bu bağlamda mahremiyet –gizlilik–, kişilere kamusal denetimden ve üçüncü şahısların müdahalesinden arındırılmış özerk bir alan sunar (Bao ve Du, 2023). Bu bağlamda "mahremiyet hakkı, bireyin kendi yaşamını asgari düzeyde dış müdahaleyle, kendi istek ve arzuları doğrultusunda sürdürme, kendisiyle ilgili bilgileri kontrol etme ve özel alana yönelik müdahalelerden korunma hakkı olarak değerlendirilebilir" (Nässi, 2022). Naker ve Greenbaum'a göre ise, mahremiyet; "demokrasinin gelişimi ve özgürlüğün tesisi için temel bir ön koşuldur. Onlara göre, mahremiyetin bulunmadığı bir ortamda ifade özgürlüğü, din özgürlüğü ya da hareket özgürlüğünden söz etmek mümkün değildir" (Naker ve Greenbaum, 2017). Bunun yanı sıra Warren ve Brandeis, mahremiyet hakkını "yalnız bırakılma" hakkı olarak tanımlamış ve bunun gerekliliğini önemle vurgulamışlardır. Ancak modern girişimler –teknolojik gelişmeler–, mahremiyete yönelik müdahaleleriyle, bireyleri yalnızca bedensel zararların yol açabileceği acıdan değil, aynı zamanda çok daha derin zihinsel acı ve sıkıntılara da maruz bırakmaktadır (Warren ve Brandeis, 1989).

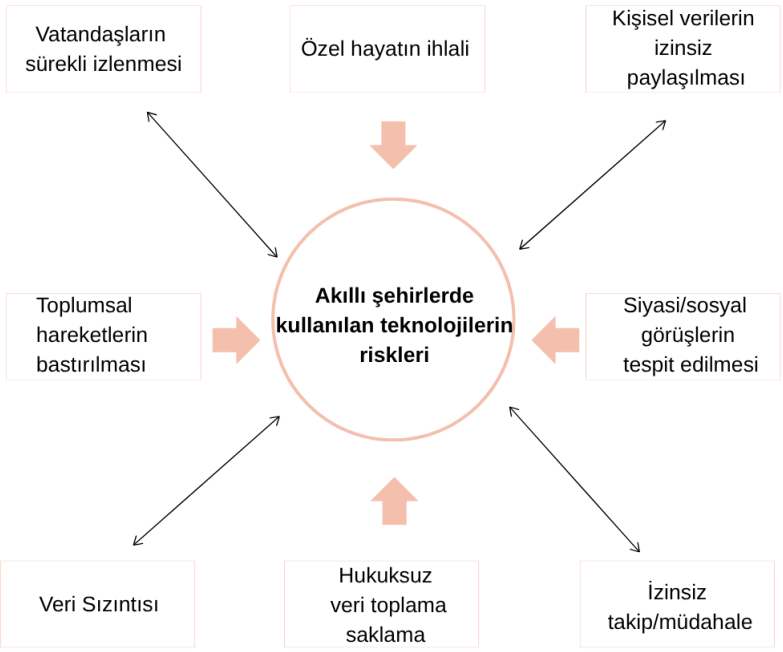


Şekil 4. 3. Akıllı Şehirlerde Mahremiyet Hakkının İhlalinde Başlıca Konular

Kaynak: (Thilakarathne ve Madhuka Priyashan, 2021: 21-44)

Mahremiyet hakkı ve bu hakkın ihlali, dijital teknolojilerin yaygınlaştığı ve kamusal alanların sayısallaştığı yeni kentsel yaşam alanlarında, özellikle de akıllı şehir uygulamaları bağlamında, yeniden tartışmaya açılmaktadır. Akıllı şehir uygulamaları, bireylerin yaşamlarının neredeyse tüm alanlarına nüfuz eden dijital sistemler içerdiğinden, bu ortamlarda yaşayan bireylerin mahremiyetinin pek çok yönü potansiyel olarak tehdit altındadır. Mahremiyet, temel bir insan hakkı olarak, genellikle "yalnız bırakılma hakkı" şeklinde tanımlanmaktadır. Ancak bu tanım, günümüzde büyük miktarda kişisel verinin sürekli olarak toplandığı, analiz edildiği ve depolandığı teknolojik yapılar karşısında yetersiz kalmaktadır. Mahremiyetin korunmasına dair bu klasik yaklaşım, akıllı şehirlerdeki veri yoğun sistemlerin doğasıyla çelişmektedir. Bu durum, bireysel özgürlükler açısından yeni hukuki ve etik tartışmaları beraberinde getirmektedir (Eckhoff ve Wagner, 2017).

Akıllı şehirlerin dünya genelinde büyük ilgi gören yönlerinden biri, bu şehirlerde kullanılan teknolojiler aracılığıyla toplanan büyük miktardaki verinin yetkililer tarafından toplumu gözetlemek amacıyla kullanılabilme riskidir (Atha vd., 2020). Bu risklerin bazıları şekil 4.4. üzerinde gösterilmiştir.



Şekil 4. 4. Akıllı Şehirlerde Mahremiyet Hakkının İhlalinde Başlıca Konular

Kaynak: (Thilakarathne ve Madhuka Priyashan, 2021: 21-44)

Mahremiyet ve akıllı şehir uygulamaları bağlamında ortaya çıkan sorunlar, bireylerin kişisel alanlarına yönelik özgürlüklerinin teknoloji temelli gözetim pratikleriyle sınırlandığı yönündeki kaygıları da beraberinde getirmektedir. Kişisel verilerin siber saldırılar veya veri ihlalleri yoluyla tehdit edilmesinden farklı olarak, gözetim riskleri doğrudan kamusal alanda bireylerle temas hâlindedir. Kent yönetimleri, suçların önlenmesi, kamu düzeninin sağlanması ve çeşitli aksaklıkların giderilmesi amacıyla gözetim kameraları, trafik kontrol sistemleri ve yüz tanıma teknolojileri gibi uygulamalara giderek daha fazla ağırlık vermektedir. Bu durum ise kent sakinlerinin mahremiyetini her geçen gün daha fazla tehdit eder hâle getirmektedir. Ayrıca bu tür teknolojilerin yaygınlaşması, yalnızca otoritenin gözetim yetkisini pekiştirmekle kalmayıp, kamusal alandaki insan davranışlarına dair toplumsal algıları da dönüştürmektedir. Bireylerin risk düzeyinin hesaplanmasında şeffaf olmayan algoritmaların kullanımı artarken, gözetim teknolojileri hükümetlerin hangi davranışların "kabul edilebilir" olduğunu hangisinin "kabul edilemez olduğunu" matematiksel sistemlerle belirlemesine olanak tanıyarak bazı davranışları norm haline getirmektedir (Martinus, 2022; Finn vd., 2012). Yeni teknolojilerin tehdit edebileceği yedi farklı gizlilik türünü özetlemektedir: bireyin kişisel mahremiyeti,

davranış ve alışkanlıklarına dair mahremiyet, iletişim içeriklerinin mahremiyeti, veri ve görsel kayıtların mahremiyeti, düşünce ve duyguların mahremiyeti, konum bilgisi ve fiziksel mekâna dair mahremiyet ile bireyin aidiyet ya da bağlılık ilişkilerinin mahremiyeti (Finn vd., 2012). Bu açıdan düşünüldüğünde, akıllı şehirlerde mahremiyetin korunmasına yönelik önlemler, yalnızca genel tehditlere karşı değil, farklı türden olası saldırganların niyet ve yöntemleri dikkate alınarak dikkatli bir biçimde planlanmalı ve uygulanmalıdır (Fabregue ve Bogoni, 2023).

Yukarıda belirtilen tanımlara göre, "kişisel mahremiyet" kavramı, bireyin bedensel işlevleriyle ilgili –genetik kodlar ve biyometri gibi gizli tutma hakkını– alanlara işaret etmektedir. "Davranışsal ve alışkanlık mahremiyeti", bireyin dini, siyasi ya da kişisel uğraşlarını kapsayan günlük yaşam pratiklerini içerir. "İletişim mahremiyeti", bireylerin elektronik mesajları, telefon görüşmeleri ve posta yoluyla gerçekleştirdiği tüm iletişim türlerinin gizliliğini ifade eder. "Veri ve görüntü mahremiyeti", bireyin kendisine ait kişisel bilgiler üzerinde tam denetim ve kontrol hakkına sahip olması gerektiği düşüncesine dayanır. "Özel düşünceler ve duygular" ise bireysel fikir ve bakış açılarına yönelik mahremiyet ihtiyacını tanımlar. "Konum ve mekân mahremiyeti", bireyin bulunduğu yerin veya alanın dış müdahalelerden izole edilmesi gerektiğini belirtir (Fabregue ve Bogoni, 2023). Konum ve mekân mahremiyeti anlayışına göre bireyler, kamusal ya da yarı kamusal alanlarda kimlikleri tespit edilmeden, izlenmeden ya da takip edilmeden hareket etme hakkına sahiptir. Bu mahremiyet anlayışı aynı zamanda yalnız kalma hakkını ve ev, araba, ofis gibi kişisel alanlarda özel yaşamın korunmasını da kapsar. Böylesi bir mahremiyet biçimi toplumsal açıdan da önem taşır. Vatandaşlar, kamusal alanlarda kimliklerinin teşhis edilmesi ya da gözetlenme korkusu olmadan özgürce hareket edebildiklerinde, demokratik bir düzende yaşadıklarını ve bireysel özgürlüklerini deneyimlediklerini hissederler. Bu öznel hissiyat hem sağlıklı işleyen bir demokrasinin güçlenmesine katkı sağlar hem de muhalefet hakkı ile toplanma özgürlüğü gibi temel demokratik ilkeleri destekler (Finn, vd., 2012). Son olarak, "meta veri", doğrudan verinin içeriğine değil, veriye eşlik eden ve onu çevreleyen tamamlayıcı bilgilere işaret eder (Fabregue ve Bogoni, 2023). Mahremiyetin bu türleri, bireylerin diğer mahremiyet alanlarıyla ve bazı temel hak ve özgürlükleriyle de doğrudan ya da dolaylı biçimde ilişki içerisindedir. Kişinin mahremiyetinin, bireysel özgürlük duygusuna katkı sağladığı ve sağlıklı, iyi uyumlanmış, demokratik bir toplumu desteklemeye yardımcı olduğu düşünülmektedir. Mahremiyetin bu yönü, davranış ve eylem mahremiyetiyle de doğrudan ilişkilidir. Bu kavram, bireylerin cinsel

tercihlerine ve alışkanlıklarına, siyasi faaliyetlerine ve dini uygulamalarına yönelik hassas konuları içermektedir (Finn vd., 2012).

Bu kapsamda, teknolojik gelişmelerin özellikle gözetim araçları üzerinden mahremiyet alanlarına nasıl müdahale ettiği sorusu daha da önem kazanmaktadır. Bu nedenle yüz tanıma ve gözetim teknolojilerinin kullanımı, bireylerin mahremiyetine dair ciddi endişeler yaratmaktadır. Bu teknolojilerle toplanan verilerin ne kadar kapsamlı olduğu, nasıl kullanıldığı ve kimler tarafından erişildiği çoğu zaman bireyler tarafından bilinmemektedir. Bu durum, gözetimin yalnızca teknik bir uygulama olmadığını, aynı zamanda toplumsal ve etik boyutları olan bir mesele haline geldiğini göstermektedir. Örneğin 2019 yılında teknoloji haber platformu TechCrunch tarafından ortaya çıkarılan bir olay, gözetim teknolojilerinin bireysel mahremiyet üzerindeki etkilerine dair çarpıcı bir örnek sunmuştur. Çin merkezli bir firma olan SenseNets'e ait yüz tanıma sistemine ilişkin büyük bir veri tabanının, herhangi bir şifre koruması olmaksızın internette erişime açık olduğu tespit edilmiştir. Bu veri tabanında yaklaşık 2,5 milyon kişiye ait kimlik bilgileri, yüz tanıma kayıtları ve bireylerin gün içinde nerelerde bulunduklarını gösteren zaman ve konum verileri yer almaktadır. Söz konusu bireylerin çoğunluğunu Çin'in Sincan bölgesinde yaşayan Uygur Müslümanlar oluşturmaktadır. Bu durum yalnızca teknik bir güvenlik zafiyeti olarak değerlendirilmemeli, aynı zamanda gözetim teknolojilerinin belirli topluluklara yönelik sistematik bir izleme aracı hâline gelebileceğini de göstermektedir. Verilerin herhangi bir koruma olmaksızın erişilebilir olması, yalnızca mahremiyetin ihlalini değil, aynı zamanda bu teknolojilerin siyasi ya da ideolojik amaçlarla kötüye kullanılma potansiyelini de gözler önüne sermektedir (Whittaker, 2021).

Gizli veya hassas nitelikteki kişisel bilgilerin rıza dışı ifşası, büyük veri çağında ön plana çıkan ciddi bir mahremiyet sorunu olmakla birlikte, bu risk yalnızca büyük veri analitiğine özgü değil, aynı zamanda kişisel verilerin toplanması ve işlenmesine dayalı sistemlerin yapısal bir niteliğidir. Öte yandan, büyük veriye özgü olarak ortaya çıkan bir diğer risk, bireyler hakkında yapılan değerlendirmelerin somut gerçekler yerine, nedensellikten yoksun çıkarımlar ya da istatistiksel korelasyonlara dayanmasıdır. Bu durum, literatürde "veri determinizmi" olarak tanımlanmaktadır. Bu tür "veri determinizmi" insanları yaptıklarına göre değil, gelecekte yapabileceklerine göre yargılar, profiller ve ele alır. Bireyler, doğrudan gerçekleştirdikleri eylemler nedeniyle değil, algoritmalar tarafından yapılan tahminler neticesinde düşük kredi puanı taşıma, sigorta riskinin yüksek görülmesi, işe alım süreçlerinde elenme ya da eğitim kurumlarına kabul edilmede olumsuz değerlendirilme gibi sonuçlarla karşı karşıya kalabilmektedir (Ramirez, 2013).

Dolayısıyla "Büyük Veri" uygulamaları hem bireyler hem de işletmeler için somut faydalar sunmaktadır. Ancak birçok şirket, büyük veriyi bireysel mahremiyeti etkileyebilecek biçimlerde kullanmaktadır. Toplanan veriler, bireylerin sağlık durumlarını, internet tarama geçmişlerini, satın alma alışkanlıklarını, sosyal ilişkilerini, dini ve siyasi eğilimlerini, finansal bilgilerini ve benzeri kişisel nitelikteki unsurları yansıtabilecek mahiyettedir (Ramirez, 2013). Başka bir deyişle, bireylerin çevrimiçi etkinliklerine ve tüketim alışkanlıklarına ilişkin verileri analiz eden algoritmalar ile coğrafi konum izleme teknolojileri, kişisel mahremiyetin ötesinde siyasi ve sosyal kimliklerin ifşası açısından da ciddi riskler barındırmaktadır. Bu teknolojiler aracılığıyla bir bireyin cinsel yönelimi, siyasi eğilimleri veya dini inançları gibi hassas bilgiler, farkında olunmaksızın devlet kurumlarına ya da üçüncü taraflara aktarılabilir. Bu tür bilgilerin açığa çıkması, bireyin hem kişisel yaşamında hem de siyasal alandaki güvenliğini tehdit edebilecek sonuçlar doğurabilir (Reuter, 2020). Büyük veri temelli uygulamaların yaygınlaşmasıyla birlikte bireylerin mahremiyetine yönelik tehditler giderek artmaktadır. Özellikle akıllı şehir bağlamında toplanan veriler, bireylerin yalnızca kamusal alanlardaki davranışlarını değil, aynı zamanda özel alanlara ilişkin eğilimlerini de izlenebilir hale getirmektedir. Martin (2020), bireylerin bu sistemler aracılığıyla sürekli bir denetim altında tutulmasının, kişisel özerkliği zayıflattığını ve bireylerin kendi davranışlarını özgürce yönlendirme yetilerini sınırladığını belirtmektedir. Çünkü dijital gözetim teknolojileri aracılığıyla bireylerin sürekli izlenmesi, yalnızca fiziksel mahremiyetin değil aynı zamanda bireyin kendine özgü bir kimlik geliştirme ve bu kimliği sürdürme hakkının da ihlaline neden olmaktadır. Kişisel alan, bireyin düşünsel ve davranışsal olarak özgürce hareket edebilmesi için gereklidir. Bu alanın gözetim yoluyla daraltılması, bireyin kendini ifade etmesini, karar alma süreçlerine katılımını ve sosyal ilişkiler kurma biçimlerini olumsuz yönde etkileyebilir. Sürekli gözlemlenme hissi bireyde içsel bir denetlenme kaygısı yaratır ve bu durum hem psikolojik bütünlüğü zedeler hem de bireysel özerkliği ciddi biçimde sınırlar (Martin, 2020).

Örneğin coğrafi konum izlemeye dayalı akıllı teknolojiler, bireylerin hareket mahremiyetini önemli ölçüde zayıflatmaktadır. Şehirlerde giderek yaygınlaşan, bireysel yayaları uzaktan izleyebilen dijital CCTV kameraları, yüz ve yürüyüş tanıma yazılımlarıyla desteklenmektedir.

Şekil 4. 5. Coğrafi Konum İzlemeye Dayalı Akıllı Teknolojilerin Bireysel Mahremiyete Etkisi

Kaynak: (Reuter, 2020: 1-19)

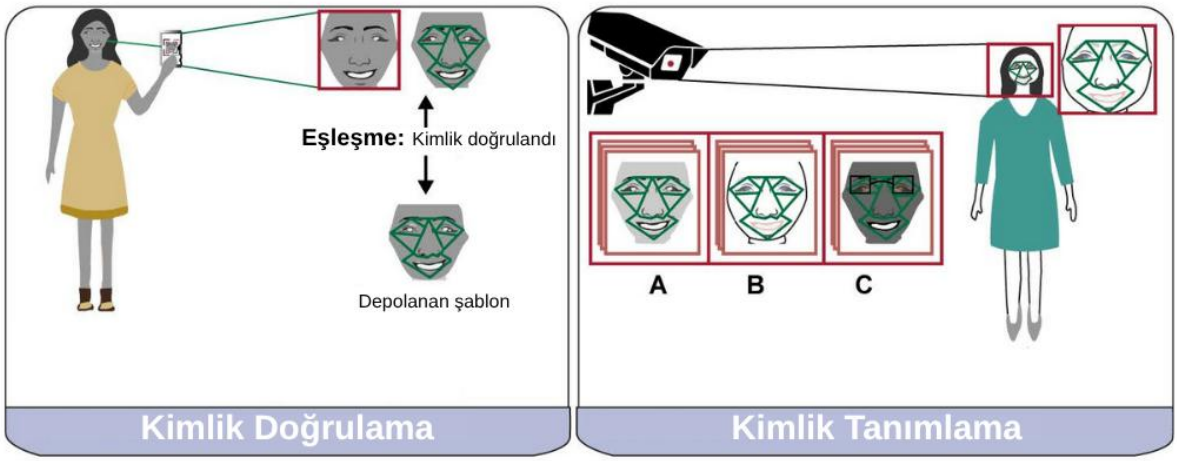
Bu sistemler aracılığıyla konum verileri üzerinden belirli tahmine dayalı gizlilik ihlalleri meydana gelebilir. Örneğin, bir kişinin düzenli olarak gey barlara gitmesi, bu kişinin gey olduğu yönünde bir çıkarıma neden olabilir ve bu bilginin paylaşılması kişisel zararlar doğurabilir. Benzer biçimde, başkalarıyla ortak yakınlık ya da eş zamanlı hareketlilik, bireyin siyasi, sosyal ya da dini aidiyetlerinin açığa çıkmasına yol açabilir. Bu tür çıkarımlar, zamanla bireyin kimliğine yapışan ve onun önüne geçen hatalı karakterizasyonlara dönüşebilir. Bu durum, yalnızca bireylerin geçmişte yaptıklarına dayalı olarak değil, aynı zamanda gelecekte yapabileceklerine dair varsayımlarla oluşturulan bir veri değerlendirme biçiminin ortaya çıkmasına neden olabilir. Böylece bireyler, henüz gerçekleştirmedikleri eylemler temelinde profil oluşturma, yargılanma ve muameleye tabi tutulma riskiyle karşı karşıya kalabilirler (Kitchin vd., 2019).

4.1.1. Yüz tanıma teknolojileri ve mahremiyet –gizlilik– sorunu

Günümüzde bireylerin yaşamın pek çok farklı yerlerinde karşısına çıkan yeni gözetim biçimi, bireylerin ve toplulukların son derece gelişmiş teknolojik araçlarla, daha önce benzeri görülmemiş bir yoğunlukta ve derinlikte izlenmesini ifade etmektedir. Bu bağlamda, bilgi elde etmek ve üretmek amacıyla kullanılan teknik araçlar, yalnızca duyularla algılanan ya da bireylerin gönüllü olarak paylaştığı verilerle sınırlı kalmayıp, bunun ötesine geçerek bireylerin

farkında olmadan paylaştığı ya da gizli kalması beklenen bilgilere de ulaşma kapasitesine sahiptir (de Oliveira Fornasier ve Borges, 2023). Ayrıca yüz tanımanın beraberinde getirdiği tek risk yaygın gözetim değildir. Bu teknoloji bireyleri tanımlamanın ötesinde, onların kişisel özelliklerini de belirleyebilmektedir. Çünkü bazı kişisel özellikler doğrudan yüz görünümüyle ilişkilidir. Tıpkı insanlar gibi, yüz tanıma algoritmaları da bir kişinin cinsiyetini, yaşını, etnik kökenini veya duygusal durumunu doğru bir şekilde tahmin edebilir. Ancak, yüzden elde edilebilecek kişisel özelliklerin listesi, bu birkaç açık örneğin çok daha ötesine uzanmaktadır (Kosinski, 2021).

Kamusal alanlarda giderek artan sayıda yüz tanıma teknolojisine dayalı uygulamalar kullanılmakta ve bu teknolojiler, güvenlik ve emniyeti sağlamaya yönelik daha geniş ve entegre gözetim sistemlerinin temel bir bileşeni olarak konumlanmaktadır. Bu bağlamda, dünya genelindeki (akıllı) şehirler, yüz tanıma teknolojilerinin kamusal alanların izlenmesi ve gözetlenmesinde bir araç olarak kullanıldığı, güvenlik süreçlerini destekleyen kritik mekânlara dönüşmektedir (Llauradó vd., 2023). Örneğin Çin hükümeti, 2005 yılında trafik şeritleri ve güvenlik kontrol noktaları gibi halka açık alanlara video gözetim ekipmanları yerleştirerek kentsel kamu güvenliği ihtiyaçlarını karşılamayı amaçlayan Skynet projesini başlatmıştır. Günümüzde Çin genelinde 200 milyondan fazla gözetim kamerası bulunmaktadır. 2015 yılından itibaren bu gözetim sistemi, Pekin, Şanghay ve Guangzhou şehirlerinde %100 kapsama alanına ulaşmıştır. Bu kameralar, yayaları gerçek zamanlı olarak algılayıp tanıyabilmekte; bireylerin yaşını, cinsiyetini ve kıyafetlerini tespit edebilmektedir. Aynı zamanda araçları tanıma kapasitesine de sahiptir. Ek olarak sistem, bir bireyin görüntüsünü veritabanında kayıtlı kişisel bilgilerle anlık olarak eşleştirme yeteneğine sahiptir (de Oliveira Fornasier ve Borges, 2023). Bu kişisel bilgilerle anlık eşleştirme, şekil 4.6. üzerinde gösterilmiştir.



Şekil 4. 6. Yüz Tanıma Teknolojilerinde Depolama ve Kayıt

Kaynak: (Xia vd., 2015: 241-250)

Bu biyometrik –izleme ve tanıma teknolojileri– sistemler ve özellikle yüz tanıma teknolojisi, suçların önlenmesi ve kayıp kişilerin bulunması gibi önemli faydalar sağlama potansiyeline sahip olmakla birlikte, bu tür faydaların, diğer temel haklara yönelik herhangi bir müdahaleyi meşru kılacak ölçüde güçlü ve haklı gerekçelere dayanması gerekmektedir. Tüm potansiyel faydalarının yanı sıra, yüz tanıma teknolojileri, mahremiyet –gizlilik– ve veri güvenliği hakkı için ciddi zorluklar da yaratabilir (Nässi, 2022). Naker ve Greenbaum'a göre, genel olarak yüz tanıma teknolojilerinin yaygın kullanımı, çeşitli evrensel etik kaygıları gündeme getirmektedir. En önemlisi, "bu teknolojilerle mahremiyet hakkı arasında ortaya çıkan gerilim, bir yandan yüz tanıma sistemlerinin uygulanmasıyla teşvik edilen ulusal güvenlik, kolluk kuvvetleri, ekonomik verimlilik veya halk sağlığı gibi hedeflerle bağlantılı diyalektiği öne çıkarırken; diğer yandan kişisel özerklik, anonimlik, unutulma hakkı, kişisel kimlik bilgilerini kontrol etme ve bireyin kendi bedeni üzerindeki haklarını koruma gibi temel ilkelerin toplumda orantısız bir şekilde ihlal edilme potansiyeline dair ciddi endişeleri beraberinde getirmektedir" (Naker ve Greenbaum, 2017). Yukarıda ifade edildiği üzere, mahremiyet hakkı, daha temel bir ahlaki değer olan özerklikle yakından ilişkilidir. Mahremiyet, genel anlamda, bilgiye ve gözleme dayalı olarak belirlenen bir "özel alanı" sınırlar. Buna karşılık özerklik hakkı, bireyin ne düşüneceğine ve ne yapacağına karar verme yetkisini, dolayısıyla bu özel alanı kontrol etme ve kimi dahil edip kimi dışlayacağına karar verme hakkını içerir. Bu çerçevede mahremiyet hakkı, kurumlar ve diğer bireyler açısından yalnızca kişisel bilgilere ve yüz görüntülerine erişimi değil, aynı zamanda gözlem ve izlemeye konu olan özel alanı da dışlamayı içeren bir özerklik hakkı ile bütünleşmektedir (Smith ve Miller, 2022). Üstelik

otomatik yüz tanıma teknolojisi, yalnızca bireylerin yüz görüntülerini ortaya koymakla kalmaz; aynı zamanda kişilerin siyasi eğilimleri, sosyal davranış biçimleri ve buna benzer birçok kişisel niteliği de açığa çıkarma potansiyeline sahiptir (Nässi, 2022).

Kısacası, yüz görüntülerinin kullanımı, bireylerin mahremiyeti üzerinde olumsuz etkilere yol açma potansiyeline sahiptir. Yapay zekâ sistemleri, özellikle yüz tanıma teknolojileri söz konusu olduğunda, bireylere yönelik önyargıları taşıma ve yeniden üretme riski taşımaktadır. Bu sistemlerde kullanılan algoritmalar teknik olarak ne kadar gelişmiş olursa olsun, eğitildikleri veri setleri homojen değilse ırk, cinsiyet gibi toplumsal kategorilere ilişkin önyargılar tekrar üretilmektedir. Nitekim Amerika Birleşik Devletleri'nde yaşanan bir olayda, Robert Williams adlı bir kişi, yüz tanıma teknolojisi tarafından başka bir siyah erkekle karıştırılarak haksız yere tutuklanmıştır. Williams'a gösterilen gözetim görüntüsü, kendisine benzememesine rağmen sistem tarafından şüpheli olarak eşleştirilmiş ve olay yerindeki polis memurları da bu eşleşmeye dayanarak işlem yapmıştır. Williams'ın bu duruma tepki olarak yönelttiği "Tüm siyahi erkeklerin birbirine benzediğini mi düşünüyorsunuz?" sorusu, yüz tanıma sistemlerinin ayrımcılık içeren yönlerini ortaya koyan çarpıcı bir örnek olmuştur. Bu örnek, söz konusu sistemlerin genellikle çoğunluğu beyaz yüzlerden oluşan veri setleriyle eğitildiğini ve bu nedenle siyah bireyler üzerinde hatalı sonuçlar üretebildiğini göstermektedir. Özellikle kolluk kuvvetleri tarafından kullanılan yüz tanıma teknolojilerinin toplumsal önyargıları pekiştirme riski taşıdığı, bu durumun ise ciddi mahremiyet ihlallerine ve ayrımcılığa yol açabileceği göz ardı edilmemelidir (Tao vd., 2022).

Öte yandan yüz tanıma teknolojilerinin, azınlıklar veya siyahi renkli insanlar açısından tehdit oluşturduğuna dair çeşitli göstergeler mevcuttur. Bu bağlamda Timnit Gebru , cinsiyet ve ırk temelli ayrımcılık ile azınlıklara yönelik önyargılı uygulamaları kapsamlı biçimde ele almaktadır (Nässi, 2022). Bu bağlamda Örneğin Çin'de hükümetin uygulamaya koyduğu "Sharp Eyes Projesi", ülke genelinde kapsamlı bir gözetim ağı oluşturmayı amaçlamaktadır. Bu program kapsamında hem kamuya açık alanlarda hem de özel mülkiyet sınırları içerisinde yer alan CCTV kameraları kullanılmakta ve bu kameralar aracılığıyla ülke çapında sürekli bir izleme sağlanmaktadır. Projenin dikkat çeken yönlerinden biri, sadece sabit gözetim kameralarıyla yetinilmemesi, aynı zamanda yerel halkın evlerine yerleştirilen özel TV kutuları ile bu gözetim sistemine dahil edilmesidir. Bu kutular sayesinde bireyler, kendi evlerinden canlı güvenlik görüntülerine erişebilmekte ve şüpheli bir durumla karşılaştıklarında tek bir tuşla güvenlik güçlerine haber verebilmektedir. Ayrıca, bu görüntülere akıllı telefonlar üzerinden de ulaşılabilmekte ve böylece vatandaşların sürekli gözetimi ve denetimi teşvik edilmektedir. Bu

uygulama, güvenliği artırma amacı taşısa da, toplumsal gözetimin sıradanlaşması ve mahremiyet hakkı üzerindeki olası etkileri bakımından ciddi etik tartışmaları da beraberinde getirmektedir (Gershgorn, 2021). Çin'de hayata geçirilen "Sharp Eyes Projesi" gibi yaygın gözetim sistemleri, kamu güvenliğini sağlama iddiasıyla geniş halk kesimlerinin günlük yaşamlarını sürekli denetim altına alırken, özellikle etnik ve dini azınlık gruplarına yönelik uygulamalar nedeniyle ciddi etik tartışmalara yol açmaktadır. Bu gözetim politikalarının en dikkat çekici yönlerinden biri, yüz tanıma teknolojilerinin etnik ayrımcılığa hizmet edebilecek biçimde kullanılmasıdır. Örneğin, Uygur Türkleri gibi azınlık gruplarını tespit ederek güvenlik birimlerine bildirmek üzere geliştirilen yüz tanıma sistemleri, Uygur nüfusu gibi azınlıklar arasında endişelere yol açma potansiyeli taşımaktadır (Bhuiyan, 2021). Bu durum, yüz tanıma teknolojilerinin yalnızca suçluları tespit etmeye yönelik bir araç olarak kullanılmadığını ve aynı zamanda farklı etnik kökenlere ve dini inançlara sahip bireylerin yaşamlarına doğrudan müdahale eden bir gözetim mekanizmasına dönüştüğünü ortaya koymaktadır (Nässi, 2022). Bu türden müdahaleler yalnızca etnik ya da dini kimliklerle sınırlı kalmamaktadır, aynı zamanda bireylerin siyasi yönelimleri gibi daha öznel ve mahrem sayılabilecek kişisel eğilimleri de teknolojik araçlarla analiz edilebilir hâle gelmektedir.

Nitekim Kosinski'nin (2021) çalışmasına göre, yüz görüntülerinden bireylerin siyasi yönelimlerini yüksek doğruluk oranıyla tahmin etmek mümkündür. Bu durum, muhafazakârlar ve liberaller arasında yüz ifadeleri ve duruş gibi çeşitli fiziksel özellikler bakımından belirgin farklar olabileceğini göstermektedir. Araştırmada, baş yönelimi, duygusal ifadeler, gözlük ve sakal gibi yorumlanabilir yüz özellikleriyle siyasi yönelim arasında bazı korelasyonlar bulunmuştur. Örneğin, liberallerin kameraya daha doğrudan baktığı ve şaşkınlık ifadesine daha yatkın olduğu; buna karşın iğrenme ifadesini daha az sergilediği saptanmıştır. Ancak bu yüz özellikleri bir araya getirildiğinde bile, siyasi yönelimi yalnızca %59 doğrulukla tahmin edebilmiştir. Buna karşılık, gelişmiş yüz tanıma algoritmaları aynı örneklemde %73 doğruluk sağlamıştır. Bu fark, algoritmaların çok daha fazla ve karmaşık özelliği analiz edebildiğini göstermektedir. Sakal, bakım, yüz ifadesi ve baş yönelimi gibi unsurlar sabitlenerek, standart koşullarda çekilen görüntüler üzerinden yürütülecek çalışmalar ise, yüz özellikleri ile siyasi yönelim arasındaki ilişkiyi daha net bir biçimde ortaya koyabilecek niteliktedir (Kosinski, 2021).

4.1.2. Duygu tanıma teknolojileri ve mahremiyet –gizlilik– sorunu

Vatandaşların şehirle kurduğu duygusal ve fiziksel etkileşimi anlamak, akıllı şehir tasarımı için büyük önem taşır. Geleneksel anketler ve simülasyonlar, çevresel deneyimin

karmaşıklığını tam yansıtamaz. Bireylerin şehirdeki davranışlarını etkileyen etkileşimler, motivasyonlar ve duygular, bu yöntemlerle tam olarak ölçülemez. Bu nedenle sanal gerçeklik ve biyometrik veriler gibi yeni teknolojiler, daha gerçekçi ve anlık değerlendirmeler sunar. Bu amaçla geliştirilen "Duygusal Haritalama" aracı, vatandaşların şehirdeki duygusal deneyimlerini gerçek zamanlı olarak izlemeyi hedefler (Jabbari vd., 2019).

Bununla birlikte, duygu tanıma teknolojilerinin şehir planlaması ve kamusal alan tasarımında kullanılması çeşitli sakıncaları da beraberinde getirme potansiyeline sahiptir. Öncelikle, biyometrik verilerin ve gerçek zamanlı duygusal tepkilerin toplanması, bireylerin mahremiyetini ciddi biçimde tehdit edebilecek niteliktedir. Toplanan verilerin kim tarafından, hangi amaçla ve ne süreyle saklanacağına dair belirsizlikler, yurttaşların kişisel bilgilerinin kötüye kullanım riskini artırmaktadır. Ayrıca, duygusal verilerin yorumlanmasında kullanılan algoritmaların tarafsızlığı ve doğruluğu da tartışmalıdır; yanlış veya eksik yorumlar hem bireyler hem de şehir politikaları açısından hatalı kararların alınmasına yol açabilir. Bu nedenle, söz konusu teknolojilerin uygulanmasında şeffaflık, veri güvenliği ve etik ilkelerin titizlikle gözetilmesi gerekmektedir.

4.1.3. Nesnelerin interneti'nin (Iot) gelişmesi ve mahremiyet ihlalleri

Nesnelerin İnterneti'nin (IoT) gelişimiyle birlikte akıllı şehir, her yerde algılama, heterojen ağ altyapısı ile akıllı bilgi işleme ve kontrol sistemlerinden oluşan yükselen bir paradigma haline gelmiştir. Akıllı şehir uygulamaları yalnızca insanlardan ve sosyal çevrelerinden çok çeşitli gizliliğe duyarlı bilgiler toplamakla kalmayıp aynı zamanda şehir tesislerini kontrol ederek insanların yaşamlarını etkilediğinden, güvenlik ve gizlilik endişeleri ortaya çıkmaktadır (Zhang vd., 2017).

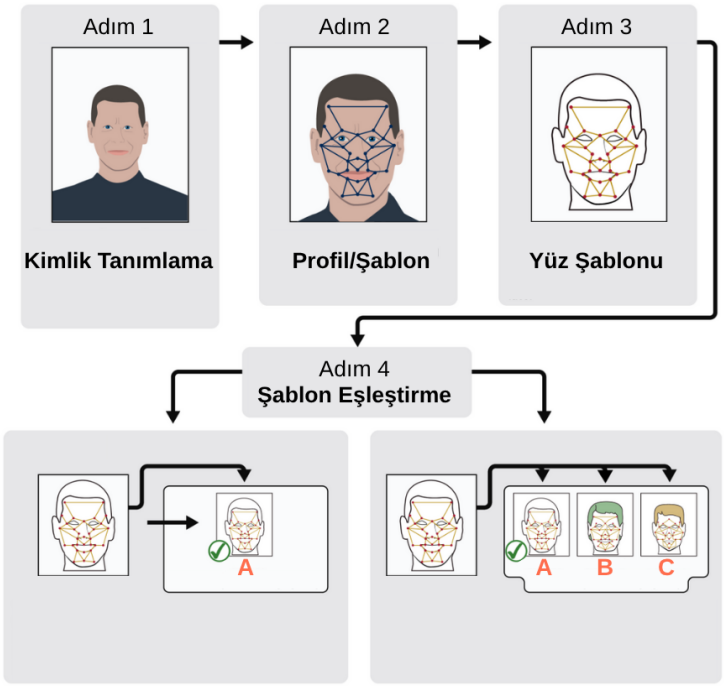
Nesnelerin İnterneti uygulamalarının şehir yaşamına entegre edilmesi, belirli bireyler ve gruplar açısından çeşitli olumsuz sonuçlar doğurabilmektedir. Örneğin, akıllı ev cihazları aracılığıyla toplanan enerji tüketim verileri, hane halkının günlük rutinlerini ortaya çıkararak hırsızlık gibi suçlara zemin hazırlayabilecek bilgiler sağlayabilir. Benzer şekilde, giyilebilir sağlık cihazlarından elde edilen biyometrik veriler, sigorta şirketleri veya işverenler tarafından erişildiğinde, bireylerin sağlık durumlarına göre ayrımcılığa uğramaları söz konusu olabilir. Toplu taşıma sistemlerinde kullanılan akıllı kart verilerinin analiz edilmesi, kişilerin günlük hareket güzergâhlarının izlenmesine imkân tanıyarak, özellikle hassas konumlarda bulunan aktivistlerin veya muhalif grupların hedef alınmasına neden olabilir. Bu örnekler, IoT tabanlı

sistemlerin yalnızca teknik güvenlik açıkları değil, aynı zamanda veri kullanımında etik ihlaller ve gözetim odaklı yaklaşımlar bakımından da ciddi riskler barındırdığını göstermektedir.

4.2. Demokratik katılım ve karar alma süreçlerinden dışlanma

Akıllı şehirler çoğunlukla demokratik yönetişim ilkelerinden ziyade kurumsal devlet bürokrasileri tarafından yönlendirilen yukarıdan aşağıya girişimler olarak şekillenmektedir. Bu bağlamda vatandaşlara ikincil bir rol verilmekte, en iyi ihtimalle tüketici ya da veri sağlayıcı olarak konumlandırılmakta ve en kötü ihtimalle engel teşkil eden, yetersiz görülen ve teknolojinin sağlayacağı faydalar konusunda ikna edilmesi gereken unsurlar olarak değerlendirilmektedir. Bu yaklaşım, vatandaşların kendi çıkarlarını belirleyemeyecekleri ve kentsel siyasette etkin bir rol üstlenemeyecekleri varsayımına dayanan bir yönetim kültürü ile desteklenmektedir. Bu anlayış, vatandaşları aktif ve bilinçli bir şekilde karar alma süreçlerine katılımı sağlamaktan ziyade sivil paternalist bir bakış açısını yansıtmaktadır. Bu çerçevede kent sakinleri karar alma süreçlerinden giderek dışlanmakta ve kentsel söylemin aktif katılımcıları olma niteliklerini kaybetmektedirler (Reuter, 2020).

Shelton ve Lodato'ya (2019) göre, vatandaşlar akıllı şehir stratejilerine ilişkin karar alma ve politika geliştirme süreçlerinden büyük ölçüde dışlanmış durumdadır. Vatandaşların katkı sunan bireyler olmaktan ziyade "veri noktaları" ya da "siber sistemin işleyen unsurları" olarak görülmesi oldukça yaygındır.



Şekil 4. 7. Akıllı Şehir Teknolojileriyle Demokratik Katılım ve Karar Alma Süreçlerinden Dışlanma

Kaynak: (Xia vd., 2015: 241-250)

Vatandaş-algılayıcı konumlandırması, vatandaşların rollerini ya da kentsel yönetişim süreçlerini temelden sorgulamalarını ya da değiştirmelerini dışlayan, son derece sınırlı rollerle tanımlanmaktadır. Şekil 4.7'de gösterildiği üzere, çeşitli görüşlere göre vatandaşları ayrıştırmak ve dışlamak bu konumlandırmaya uymaktadır. Bu bağlamda katılım, diyalog ve tartışma yoluyla gerçekleştirilen demokratik katılım yerine, bilgisayar aracılığıyla verilen yanıtlarla eş anlamlı hale gelmektedir (Shelton ve Lodato, 2019).

Akıllı şehir girişimleri kapsamında şehirdeki katılımı ve hizmet verimliliğini artırma amacıyla birçok kamu hizmeti dijital ortama taşınmaktadır. Ancak yaşlı bireyler ve göçmenler gibi kırılgan toplumsal gruplar, dijital topluma katılım için gerekli olan teknik bilgi ve dijital becerilerden yoksun kalabilmektedir. Hizmetlerin yalnızca çevrimiçi ortama taşınması, bu grupların kamu hizmetlerine erişimini sınırlandırarak eşitlik ilkesini zedeleyebilir. Bu durum yalnızca demokratik tartışmalara katılımı değil, aynı zamanda temel kamu hizmetlerine ulaşımı da etkileyen yapısal bir dışlanma riski doğurmaktadır (Hansen ve Skaiaa, 2019).

4.3. Kent hakkının ihlali

Kent hakkı, bireylerin kentsel yaşam üzerinde söz sahibi olma ve şehirden eşit şekilde yararlanma hakkıdır. Kent hakkı, yalnızca şehirde yaşama hakkı değil, aynı zamanda kent yaşamının şekillenmesinde söz sahibi olma, kamusal alanlara eşit erişim, katılım, özgürce hareket etme ve yaşam kalitesini belirleyen karar süreçlerine dahil olma hakkıdır. Dolayısıyla dijital teknolojilerin bu alanlarda sınırlayıcı veya dışlayıcı biçimde kullanılması, kent hakkının özünü zedeleyebilir. Örneğin Çin'de uygulanan Sosyal Kredi Sistemi (SCS) gibi gözetim temelli dijital uygulamaların kent hakkının ihlaliyle doğrudan ilişkisi vardır.

4.3.1. Sosyal kredi sistemi ve kent hakkının ihlali

Dijital teknolojilerin gelişimi, bireylerin bazı hak ve özgürlüklerinin sınırlandırılmasına neden olabilecek yeni uygulamaları da beraberinde getirmektedir. Bu uygulamalardan biri olan Sosyal Kredi Sistemi (SCS), bireylerin ve kuruluşların çeşitli davranışlarına göre puanlanmasını esas almaktadır. Söz konusu puanlar, hizmetlere, istihdam olanaklarına ve seyahat gibi temel haklara erişimi doğrudan etkileyebilmektedir. Bu sistem kapsamında finansal geçmiş, hukuki kayıtlar, sosyal medya kullanımı ve bireysel alışkanlıklar gibi pek çok veri toplanmakta ve analiz edilmektedir. Bu analiz sonucunda bireylere sosyal kredi puanları verilmekte, bu da ödül veya yaptırımlarla sonuçlanmaktadır. Yüksek puanlar, krediye, işe ve seyahate erişimde kolaylık sağlarken, düşük puanlar kara listeye alınma, seyahat kısıtlamaları ya da istihdamda dezavantaj yaşama gibi sonuçlar doğurabilmektedir. Bu yapı, bireylerin özel yaşamlarına müdahale edildiği, sürekli gözetim altında tutulduğu ve psikolojik baskı altında yaşamak zorunda kaldığı bir ortam yaratma potansiyeline sahiptir. Özellikle Çin'in Sincan Uygur Özerk Bölgesi'nde, bu sistemin gözetim devleti uygulamalarına dayanak oluşturduğu ve terörle mücadele gerekçesiyle kitlesel izleme ile toplama kamplarının meşrulaştırıldığı görülmektedir. Ancak mevcut bulgular, bu uygulamaların asıl amacının Uygur halkının kültürel ve dini kimliğini bastırmak olduğunu ortaya koymaktadır. Bu durum, dijital teknolojilerin yalnızca güvenlik değil, aynı zamanda politik ve ideolojik amaçlarla da kullanılabileceğini göstermektedir (Hickling, 2025). Sincan gibi azınlık bölgelerinde yaşanan baskıların ötesinde akıllı şehir girişimleri, sosyal kredi sistemleri gibi sosyal kontrol mekanizmalarının sistemli bir biçimde uygulanmasını kolaylaştıran dijital bir altyapı sunmaktadır. Çin'in azınlık nüfuslarını sıkı şekilde denetlediği Sincan ve Tibet gibi bölgelerde akıllı şehir teknolojileri, gözetim ve baskı politikalarının temel bir aracı haline gelmiştir. Bu bağlamda Çin'in Nesnelerin İnterneti, büyük veri, bulut bilişim ve uydu konumlandırma gibi kritik teknolojileri geliştirmesi ve

kullanıma sunması, diğer ülkelerdeki örneklerle karşılaştırıldığında çok daha ileri düzeyde mahremiyet ve insan hakları kaygılarına yol açmaktadır (Atha vd., 2020).

4.4. Dijital bölünme ve eşitsizliklerin derinleşmesi

Akıllı şehir teknolojileri, bilgiye erişimi kolaylaştırma ve vatandaşların karar alma süreçlerine katılımını teşvik etme açısından önemli fırsatlar sunmaktadır. Ancak bu fırsatların hayata geçirilebilmesi için bireylerin dijital okuryazarlık becerilerine sahip olması gerekmektedir. Nitekim akıllı şehirlerin etkili bir şekilde işlemesi, yalnızca teknik altyapıların değil, aynı zamanda bu sistemleri kullanabilen "daha akıllı vatandaşların" varlığını da gerekli kılmaktadır (Ramos, 2019). Bu bağlamda, özellikle teknolojik bilgiye erişimi sınırlı, düşük gelirli ya da eğitim olanaklarından yoksun bireylerin bu süreçlerin dışında kalma riski söz konusudur. Toriz Ramos (2019), halihazırda ciddi sosyal eşitsizliklerin ve gelir farklılıklarının bulunduğu şehirlerde, akıllı şehir uygulamalarının kapsayıcı olması hedeflense de bu yapısal eşitsizliklerin devam edebileceğini ifade etmektedir.

Akıllı kent uygulamalarının sunduğu olanaklardan yararlanmak çoğu zaman yüksek hızlı internet bağlantısına ve ileri düzey teknolojiye sahip algılama sistemlerine erişimi gerektirmektedir. Ancak bu tür altyapılara erişim imkânı, toplumun her kesimi için eşit düzeyde mevcut değildir. Özellikle teknolojik okuryazarlığı sınırlı olan bireyler ile düşük gelirli gruplar, yaşlılar ve engelli bireyler gibi kent planlama süreçlerinde tarihsel olarak yeterince temsil edilmeyen kesimler, bu dijital dönüşüm sürecinin dışında kalma riski taşımaktadır. Bu durum, kentsel hizmetlerin ve hakların paylaşımında yapısal eşitsizlikleri pekiştirme tehlikesi barındırmaktadır (Kempin Reuter, 2019). Shelton ve Lodato'ya (2019) göre, akıllı şehir çabaları, serbest piyasayı, teknoloji odaklı ve uzman temelli kentsel planlama ve yönetişim biçimlerini ayrıcalıklı hale getirerek, halihazırda mevcut olan kentsel sosyal ve mekânsal eşitsizlikleri yeniden üretmekte ve pekiştirmektedir (Shelton ve Lodato, 2019). Van Dijk'e (2012) göre dijital teknolojilerden dışlanmak, bireylerin bilgiye, iletişime ve çevrimiçi hizmetlere erişimini sınırlamakta ve bu durum toplumda "dijital uçurum" – dijital bölünme– olarak adlandırılan eşitsizliklerin derinleşmesine yol açmaktadır (Van Dijk, 2012).

Bu çerçevede, akıllı şehir uygulamalarının sunduğu olanakların tüm kent sakinleri için eşit biçimde erişilebilir olmaması, mevcut kentsel eşitsizliklerin derinleşmesine yol açabilir. Örneğin, akıllı altyapı yatırımlarıyla sağlanan yaşam kalitesi iyileştirmeleri —ısıtmalı kaldırımlar, akıllı aydınlatma sistemleri ya da çevresel izleme teknolojileri gibi— genellikle merkezi ve yüksek gelir gruplarının yaşadığı bölgelerde yoğunlaşmaktadır. Bu durum, kentlerin

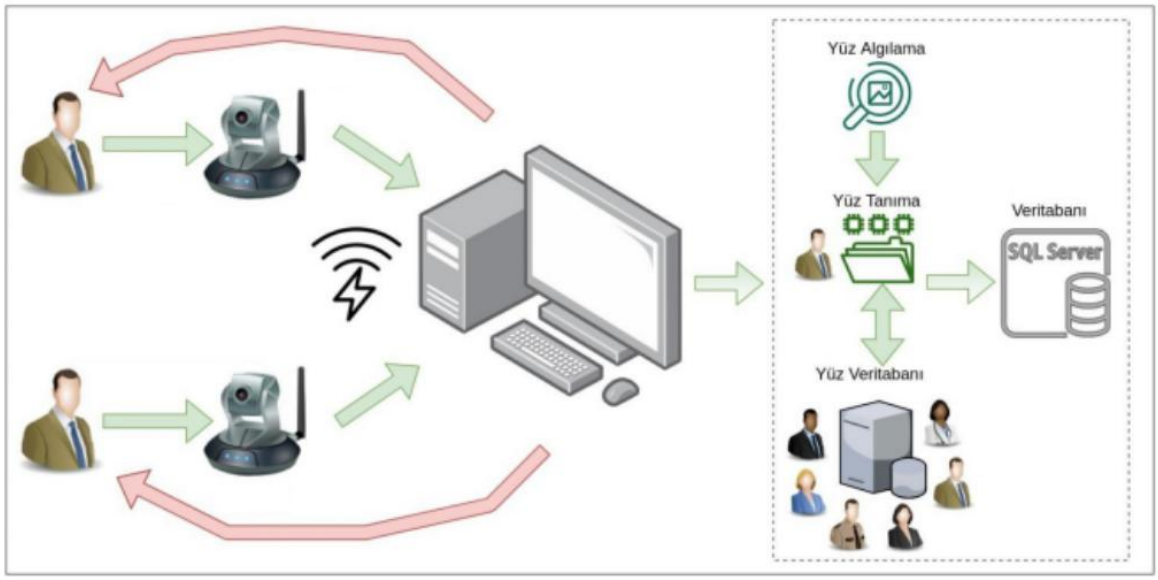
daha yoksul veya dezavantajlı bölgelerinde yaşayan bireylerin bu hizmetlerden yeterince faydalanamaması sonucunu doğurmakta ve teknolojik kalkınmanın toplumsal adalet açısından dengesiz bir biçimde ilerlemesine neden olabilmektedir (Flak ve Hofmann, 2020). Özellikle dijital uçurumu en çok deneyimleyen gruplar, tarihsel olarak dezavantajlı konumda bulunan topluluklardır. Her ne kadar her topluluğun koşulları farklılık gösterse de dijital uçurum; cinsiyet, yaş, ırk, gelir düzeyi ve engellilik gibi mevcut sosyal, ekonomik ve kültürel eşitsizlikleri yansıtmaya ve pekiştirmeye devam etmektedir. Bu durumdan orantısız biçimde etkilendiği bilinen topluluklar arasında kadınlar ve kız çocukları, yaşlı bireyler, yoksullar, dışlanmış ya da azınlık topluluklar, engelli bireyler veya mülteciler yer almaktadır (UN-Habitat, 2021).

Dolayısıyla Bilgi ve iletişim teknolojileri (BİT), bireylerin toplumsal hayata katılımını kolaylaştırma potansiyeli taşırken, aynı zamanda dijital eşitsizlikleri derinleştirme riskini de barındırmaktadır. Mevcut sosyal yapılar içinde BİT'lerin yaygınlaştırılması, kimi durumlarda toplumsal ayrışmaları ve mevcut güç ilişkilerini yeniden üretme işlevi görebilmektedir. Bu bağlamda, bireylerin BİT'lere erişimi yalnızca teknik bir mesele değil, aynı zamanda toplumsal eşitsizliklerin bir yansıması olarak değerlendirilmektedir. Sosyo-ekonomik statü, gelir düzeyi, eğitim geçmişi ve iş gücü piyasasına katılım gibi göstergeler, bireylerin dijital araçlara erişiminde belirleyici faktörler arasında yer almaktadır (Kempin Reuter, 2019). Teknolojiye erişim (geniş bant internet, yüksek kaliteli sensör cihazları) sosyal statü, gelir ve eğitimle doğrudan ilişkilidir, bu da dijital uçurumu derinleştirmektedir. Teknolojik olarak okuryazar olmayanlar, yoksullar, yaşlılar ve engelliler gibi geleneksel olarak marjinalize edilmiş gruplar dışarıda kalmaktadır. Akıllı kent planlamacıları genellikle homojen bir "genel vatandaş" profiline göre tasarım yapmakta, farklı değerlere, kimliklere ve deneyimlere sahip "eksik vatandaşları" göz ardı etmektedir (Reuter, 2020).

4.5. İfade özgürlüğü, örgütlenme ve siyasi katılımın kısıtlanması

Akıllı şehir uygulamaları, çevrimiçi katılım ve dijital iletişim araçlarının yaygınlaştırılması yoluyla ifade özgürlüğünü teşvik edebilecek bir potansiyel taşımaktadır. Belediyelerin karar alma süreçlerine dijital kanallar üzerinden erişimin kolaylaşması, vatandaşların görüşlerini dile getirme ve kamu politikalarına katkı sunma olanaklarını artırabilir. Ancak bu durumun yalnızca olumlu sonuçlar doğuracağı varsayımı her zaman geçerli değildir. Nitekim dijital platformların aynı zamanda gözetim mekanizmalarını güçlendirmesi, bireylerin kendilerini ifade ederken otosansür uygulamalarına yönelmesine neden olabilmektedir. Bu durum, ifade özgürlüğü açısından dikkatle değerlendirilmesi gereken

bir çelişki yaratmaktadır. Ayrıca, dijital katılımın gerektirdiği teknik bilgi düzeyine sahip olmayan bireyler için bu süreçler erişilebilir olmaktan uzak hale gelebilir. Özellikle yaşlılar ve göçmenler gibi grupların çevrimiçi hizmetleri etkin biçimde kullanmalarının önünde yapısal engeller bulunduğuna ilişkin kaygılar dile getirilmektedir. Bu durum, kamu hizmetlerine eşit erişim hakkının dijitalleşme sürecinde zedelenme riski taşıdığını ortaya koymaktadır (Flak ve Hofmann, 2020).



Şekil 4. 8. Kamu Personeli ve Vatandaşın İfade Özgürlüğü, Örgütlenme ve Siyasi Katılımın Takip Edilmesi

Kaynak: (Mamak vd., 2020: 497-504)

Bu açıdan bakıldığında gelişmiş gözetim teknolojilerinin bireyler üzerindeki etkileri tartışılırken, akla gelen önemli sorulardan biri şudur: Bu denetim ortamı, bireyleri normal davranışlarını değiştirmeye zorlayabilir mi? İnsanlar, yalnızca potansiyel sonuçlardan duydukları korku nedeniyle, farklı düşüncelere ilgi duymaktan, belirli kişilerle iletişim kurmaktan, protestolara katılmaktan ya da siyasi faaliyetlerde bulunmaktan kaçınabilir mi? Bu soruya kesin bir yanıt vermek güç olmakla birlikte, sosyal bilimlerde "soğutma etkisi" olarak bilinen olgunun varlığı, bu tür davranış değişimlerinin mümkün olduğunu göstermektedir. Soğutma etkisi, bireylerin veya grupların izlendiklerini bildikleri ya da düşündükleri durumlarda, karşılaşabilecekleri olumsuz sonuçlardan çekinerek ifade, örgütlenme ya da katılım gibi haklarını kullanmaktan geri durmaları şeklinde tanımlanmaktadır. Bu durum, gözetimin sadece fiziksel değil, aynı zamanda psikolojik ve siyasal bir baskı aracı olarak işlev gördüğünü ortaya koymaktadır (Murray vd., 2024). Nitekim bazı araştırmalar, dijitalleşmenin yalnızca teknik bir dönüşüm değil, aynı zamanda otoriter rejimlere vatandaşları izleme,

davranışları yönlendirme ve muhalefeti bastırma gibi yeni yönetim ve sosyal denetim araçları sunduğunu ortaya koymaktadır (Balayan ve Tomin, 2021).

(Murray vd., 2024) tarafından yapılan araştırmaya göre, gözetim bireylerin karar alma süreçleri, sosyal ilişkileri ve çevreleriyle kurdukları etkileşim üzerindeki etkilerini anlamada önemli bir araç olarak öne çıkmaktadır. Gözetim altında olduklarını düşünen ya da bu tür bir izlenim taşıyan bireylerle gerçekleştirilen görüşmelerde, katılımcıların ifade özgürlüğü ve toplanma özgürlüğü gibi temel haklarının nasıl sınırlandığı açıkça ortaya konmuştur. Söz konusu araştırmaya göre, bireylerin gözetlendiklerine yönelik inancı kendi ifadelerini gönüllü olarak sınırladıklarını ve bu durumun bir tür otosansür oluşturduğu görülmektedir. Ayrıca, bireylerin, gözetimle ilişkilendirilen kişi ya da kurumlarla temasta bulunmaktan çekindikleri, bunun kamu otoriteleri tarafından suç ortaklığı gibi yorumlanabileceği endişeleri taşıdıkları sonucuna ulaşılmıştır. Bu durum yalnızca bireysel ifade hakkını değil, aynı zamanda başkalarıyla ilişki kurma, sosyal ağ oluşturma ve siyasal anlamda örgütlenme gibi kolektif eylemleri de olumsuz yönde etkilemektedir. Söz konusu araştırmaya göre, gözetim uygulamaları bireyler arasında güven duygusunun zayıflamasına yol açarak, sosyal ilişkilerin sürdürülmesini ve kamusal alanda aktif yurttaş katılımını ciddi biçimde engellemektedir (Murray vd., 2024).

Bireylerin dijital araçlara sınırlı erişimi ve teknik yeterlilik eksikliği, kamusal yaşama katılım olanaklarını kısıtlarken, bazı rejimlerde dijital teknolojilerin bilinçli olarak baskı ve denetim aracı hâline getirilmesi, temel hak ve özgürlüklerin daha sistematik biçimde sınırlandığı bir yapıyı da beraberinde getirmektedir. Örneğin Çin'de uygulanan Sosyal Kredi Sistemi (SCS) ve buna bağlı gözetim temelli dijital uygulamalar, özellikle Sincan bölgesinde yaşayan Uygur Türkleri başta olmak üzere etnik ve dini azınlıklar üzerinde ciddi hak ihlallerine neden olmaktadır. Bu sistem kapsamında DNA örnekleri, yüz tanıma verileri, ses kayıtları gibi biyometrik bilgiler kitlesel biçimde toplanmakta; bireylerin günlük yaşamları, yüz tanıma teknolojileri ve yaygın kamera-sensör ağları ile sürekli olarak izlenmektedir. Ayrıca telefon görüşmeleri, kısa mesajlar ve internet kullanımı da denetim altındadır. Bu durum, hükümetin kimlikleri ve davranışları belirsiz kriterlerle değerlendirdiği bireyleri gözaltına almasına olanak tanımakta ve keyfi tutuklamalara zemin hazırlamaktadır. Bu gözetim mekanizması, ifade özgürlüğü açısından ciddi bir baskı ortamı yaratmakta, bireylerin düşüncelerini açıkça ifade etmelerini ve hükümete yönelik eleştirilerde bulunmalarını zorlaştırmaktadır. Aynı zamanda, örgütlenme ve toplanma özgürlüğü de tehdit altındadır. Çünkü kamuya açık toplantılar, gösteriler ve protestolar gözetim yoluyla izlenmekte ve çoğu zaman bastırılmaktadır. Seyahat

özgürlüğü, özellikle etnik azınlıklar için sosyal kredi sistemine dayalı olarak sınırlandırılmaktadır. Bu şekilde bireylerin şehir içinde ya da şehirler arası hareketliliği engellenebilmektedir (Hickling, 2025). Öte yandan, sosyal kredi sistemi aracılığıyla, anti-sosyal davranışlarla mücadele etmek ve sivil davranışları standartlaştırmak amacıyla giderek artan sayıda düzenleme hayata geçirilmektedir. Bu düzenlemeler, bireylerin günlük yaşamlarına doğrudan müdahale anlamına gelmekte ve ifade özgürlüğü ile örgütlenme hakkı gibi temel hakları sınırlandırma potansiyeli taşımaktadır. Ayrıca, devlet kurumlarının bu sistemi kötüye kullanarak bireyleri ilgisiz ya da keyfi gerekçelerle cezalandırması söz konusu olabilmektedir. Örneğin, İç Moğolistan'da çocuklarını zorunlu Mandarin eğitim müfredatı uygulayan okullardan alan velilerin kara listeye alınmakla tehdit edildiği bildirilmektedir. Bu tür uygulamalar, bireylerin karar alma özgürlüklerini zedelemekte ve kamusal alanlarda özgürce düşünce beyan etme ya da alternatif görüşleri savunma imkanlarını daraltmaktadır. Tüm bu uygulamalar, sadece bireysel hakları değil, aynı zamanda yurttaşların siyasi katılım hakkını da zayıflatmakta ve demokratik işleyişi tehdit eden bir gözetim rejimi ortaya çıkarmaktadır (Hickling, 2025).

Gözetim verilerinin kötüye kullanımı ve yanlış kullanımı, yalnızca otoriter rejimlerle sınırlı bir tehdit değildir. Liberal demokrasilerde de güvenlik, terörle mücadele ve kamu düzenini sağlama gerekçeleriyle yüz tanıma sistemleri, biyometrik kimlik doğrulama teknolojileri ve öngörücü polislik uygulamaları giderek daha yaygın hâle gelmektedir. Bu tür teknolojiler, başlangıçta kamu güvenliğini artırma amacıyla kullanılsa da, zamanla denetim mekanizmalarının yetersizliği nedeniyle bireysel özgürlükleri tehdit edecek biçimde istismar edilebilmektedir. Nitekim bazı demokratik ülkelerde, muhalefet liderlerine, gazetecilere veya insan hakları savunucularına yönelik casus yazılım kullanımı gibi vakalar, bu teknolojilerin siyasi çıkarlar doğrultusunda araçsallaştırılabileceğini göstermektedir (Hickling, 2025).

4.6. İnsan onuru ve bireysel özerkliğin zayıflaması

Akıllı şehirlerde kullanılan dijital ve gözetleme teknolojileri, bireylerin özerkliğini ve karar alma süreçlerini dolaylı yollardan etkileyebilecek yeni kontrol biçimlerini gündeme getirmektedir. Güvenlik yöntemi olarak izlemeyle ilişkili temel gizlilik riski, manipülatif dürtme uygulamaları ve bunun, bireylerin gizliliğe değer vermesinin temel gerekçelerinden biri olan özerklik üzerindeki etkisidir. Akıllı şehirler, birey davranışlarının öngörülebilir ve dışarıdan denetlenebilir hale getirilmesinin esas kaygı haline geldiği devasa laboratuvarlara dönüşmektedir. Bu bağlamda teknoloji, bir yeri daha güvenli ve cazip hale getirmek amacıyla ziyaretçi davranışlarını inceleyen ve yönlendiren, çevreyi kontrol eden bir araç olarak

kullanılmaktadır. Bu gelişme biçimi çoğu zaman "dürtme" olarak adlandırılır. Dürtme, bireylerin davranışlarını ekonomik teşvikleri önemli ölçüde değiştirmeksizin ve seçeneklerini doğrudan sınırlamadan öngörülebilir biçimde etkileyen seçim mimarisi unsurlarını tanımlar. Bu kavram, karar alma süreçlerinin çoğunlukla bilinçli ve aktif değil, bilinçaltı, pasif ve düşüncesiz biçimde gerçekleştiği varsayımına dayanır. Bu nedenle çevre, insan kararlarını belirli yönlere yönlendirmek amacıyla sistematik olarak şekillendirilebilir. Sonuç olarak dürtmeler, bireyin özerk biçimde karar almasını engelleyebilecek manipülatif etkileri nedeniyle, bireysel özerkliğe yönelik bir tehdit olarak karşımıza çıkmaktadır. Nitekim bu tip sistemler insani bir amaca sahip değilse, bilgi başlı başına bir amaç haline gelir ve bu da gerçeği çarpıtabilir. Daha da vahim bir durum ise, uygulama aşamalarını belirli kuruluşların hedeflerine hizmet edecek şekilde yönlendirerek gerçekliğin kasıtlı olarak manipüle edilmesidir (Fabregue ve Bogoni, 2023).

4.7. Algoritmik ayrımcılık, profilleme ve şeffaflık eksikliği

Akıllı şehir teknolojilerinin ayrımcı sonuçlar doğurması ya da mevcut eşitsizlik yapılarını derinleştirmesi yönündeki risk dikkate değer bir öneme sahiptir. Nitekim, yüz tanıma teknolojilerinin akıllı şehir bağlamında yaygınlaştırılması, bu teknolojilerin ırksallaştırılmış bireyleri tespit etmede daha düşük doğruluk oranlarına sahip olması nedeniyle hatalı soruşturmalara, gözaltılara veya tutuklamalara yol açabilmektedir (Qarri ve Gill, 2022). Bu nedenle, şehir yönetimleri açısından sorumluluk her ne kadar vatandaşlara ait olsa da, vatandaşlar yekpare bir grup değildir; gerçek hesap verebilirlik, sınıfa, ırka, cinsiyete, yaşa ve engelliliğe göre ayrıştırılmış eşitlik arayışındaki grupların farklı ihtiyaçlarının ele alınmasını zorunlu kılmaktadır (Sengupta ve Sengupta, 2022).

Öte yandan veri analitiğine dayalı karar alma süreçleri, bireylerin davranışlarına ilişkin öngörülerde bulunmak amacıyla geliştirilen algoritmalar aracılığıyla yürütülmektedir. Ancak bu süreçler, zaman zaman bireylerin yanlış sınıflandırılmasına neden olabilmekte ve bu durum, ilgili kişilerin yaşamlarında doğrudan ve ciddi sonuçlar doğurabilmektedir. Uçuşa yasak listelerine alınmak, istihdam olanaklarına erişememek ya da belirli hizmetlerden dışlanmak gibi sonuçlar, bu tür algoritmik hataların doğrudan ve somut etkileri arasında yer almaktadır. Bu bağlamda, veri determinizmine dayalı tahmin modelleri, özellikle öngörüye dayalı kolluk faaliyetleri gibi ileri yönetişim uygulamalarında daha da sorunlu hale gelmektedir. Bu tür uygulamalar, bireylerin yalnızca olası davranışlarına ilişkin tahminler üzerinden değerlendirilmeleri nedeniyle hem hak ihlallerine hem de sosyal dışlanmaya zemin hazırlayabilmektedir (Reuter, 2020).

Akıllı kent uygulamaları kapsamında geliştirilen öngörücü polislik yazılımları, belirli coğrafi alanlarda işlenen suçlara ilişkin verileri analiz ederek geleceğe dönük suç örüntülerini tespit etme amacı taşımaktadır. Gelişmiş algoritmalar aracılığıyla çalışan bu sistemler, yüksek suç oranlarının yoğunlaştığı bölgeleri suç türüne göre kategorize edebilmekte ve bu doğrultuda kolluk kuvvetlerinin müdahale stratejilerini yönlendirmektedir. Özellikle Amerika Birleşik Devletleri'nde çeşitli şehirlerde yaygın olarak kullanılmaya başlanan bu teknolojiler, yerel düzeyde olası suç davranışlarını henüz gerçekleşmeden tahmin etme iddiası taşımaktadır (Koss, 2015). Algoritmaların ve dijital öğrenme sistemlerinin polislik faaliyetlerinde kullanımı, ırk temelli ayrımcılık biçimlerini ortadan kaldırmak yerine, mevcut önyargıları pekiştirme riskini beraberinde getirmektedir. Bu tür teknolojiler, bireylerin ırklarına dayalı olarak hedef alınmasını kolaylaştırmakta ve bu süreçte ırksal önyargılar içeren algoritmaların üretilmesine neden olmaktadır. Bunun sonucunda, özellikle dini, etnik ve ırksal azınlık gruplarının gözetim altında tutulması kurumsal bir nitelik kazanmaktadır. Polis uygulamalarında tarafsızlık ve eşitlik sağlama iddiasıyla geliştirilen bu sistemler, ırksal profilleme gibi halihazırda sorunlu olan uygulamaların dijital araçlarla yeniden üretilmesine hizmet etmektedir. Ayrıca bu teknolojilerin kullanımı, polis ile toplum arasındaki güven ilişkisini zedeleyen yapısal sorunlara ya da ırksal önyargıların ortadan kaldırılmasına yönelik herhangi bir katkı sunmamaktadır (Reuter, 2020). Kısacası "veri determinizmi" olarak adlandırılan bu yaklaşım, bireyleri geçmişte gerçekleştirdikleri eylemlerden ziyade, gelecekte gerçekleştirme ihtimali bulunan davranışlara göre değerlendirmektedir. Bu yaklaşım, bireylerin profillenmesine ve bu profillere göre muamele görmesine neden olmaktadır. Özellikle tahmine dayalı polislik uygulamaları, ırk temelinde hedef alma ve ırksal önyargılarla şekillenen algoritmalar üretme riski taşıyarak, etnik ve dini azınlıkların baskı altına alınmasına yol açabilmektedir. Bu durum, ifade özgürlüğü ve toplanma özgürlüğü gibi temel hak ve özgürlüklerin ihlal edilmesi tehlikesini de beraberinde getirmektedir (Reuter, 2020).

4.8. Türkiye’de akıllı kent ve verilerin kötüye kullanımı

Veri, gözleme dayalı olarak elde edilen ve genellikle sayısal biçimde ifade edilen bilgi birimleridir. Daha teknik bir ifadeyle veri; bir ya da birden fazla birey ya da nesneye ait niteliksel veya niceliksel değişkenlerin çeşitli değerlerinden oluşur; tek bir değişkenin tek bir gözlemine ait bilgi ise "veri" olarak adlandırılır. "Veri" (data) kavramının İngilizce'deki ilk kullanımı 1640’lı yıllara dayanmakta olup, 1946 yılı itibarıyla “aktarılabilir ve depolanabilir bilgisayar bilgisi” anlamını kazanmıştır. “Veri işleme” terimi ise ilk kez 1954 yılında literatürde yer bulmuştur (Garfinkel, 2000). Veriler, yalnızca bilimsel araştırmalarda değil aynı zamanda

insan etkinliklerinin neredeyse tüm alanlarında başvurulan temel bilgi kaynaklarıdır. Veriler ölçülmekte, toplanmakta, raporlanmakta ve analiz edilmektedir. Elde edilen bulgular, grafikler, görseller veya çeşitli analiz araçları aracılığıyla görselleştirilerek daha anlaşılır hale getirilmektedir.

Büyük veri, geleneksel veri işleme yöntemlerinin yetersiz kaldığı, yüksek hacimli ve karmaşık veri kümelerini ifade eder. Bu veriler, çözümü zor olan sorunların analizinde önemli fırsatlar sunmaktadır. Büyük veri; hacim (volume), hız (velocity) ve çeşitlilik (variety) gibi temel özelliklerle tanımlanır. Geçmişte kentsel araştırmalar daha çok toplu istatistikler ve sınırlı ölçekli anketlere dayanırken, günümüzde dijital kayıtlar, sensör teknolojileri ve bilgisayarlaştırılmış toplum yapısı sayesinde detaylı, zaman ve mekâna duyarlı şehir verileri üretilmektedir. Bu gelişme, büyük verinin kent bilimine katkı sağlamasını mümkün kılmaktadır. Algoritmalarla desteklenen büyük veri, daha önce ölçülmemiş toplumsal dinamikleri anlamada yeni olanaklar sunar. Kentsel büyümenin etkilerini analiz etmek ve sosyal politikaların değerlendirilmesini sağlamak gibi klasik sosyal bilim sorularına yanıt üretmede, dışsal varyasyonlarla birleştirilen büyük veri güçlü bir araç haline gelmektedir (Greenstone vd., 2010).

Açık veri, herhangi bir telif veya erişim kısıtlaması olmadan kamuya sunulan ve serbestçe kullanılabilen veri setlerini ifade eder. Bu yaklaşım, yalnızca kamusal erişimi kolaylaştırmakla kalmaz; aynı zamanda bireylerin ve kurumların veri süreçlerine aktif biçimde katılımını da mümkün kılar. Böylece çok aktörlü ve katılımcı bir gelişim modeli teşvik edilir. Açık verinin temel avantajı, toplum genelinde bireysel ve kolektif gelişimi desteklemesidir. Bunun yanı sıra, yönetişimde şeffaflık ve hesap verebilirlik ilkelerini güçlendirerek kamu yönetiminde güveni artırır. Özellikle yazılım geliştirme alanında önemli fırsatlar sunan açık veri sayesinde bireyler, kamu kurumları veya özel sektör tarafından üretilen verilere erişebilir, bu veriler üzerine yeni uygulamalar geliştirerek inovasyonu destekleyebilir (Lim vd., 2018).

Türkiye'de kişisel verilerin korunmasına ilişkin yasal çerçeve başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 5237 sayılı Türk Ceza Kanunu (TCK) ve Anayasa ile çizilmiştir. TCK, "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü veriyi" kişisel veri olarak tanımlamaktadır (Gürler, 2025). Bu bağlamda veri güvenliği, verinin doğruluğunun korunmasını; gizlilik ise veriye izinsiz erişimlerin engellenmesini ifade eder. Her iki unsur da gerek teknolojik açıklar, gerekse idari ihmaller nedeniyle risk altına girebilmektedir. Kişisel verilerin korunmasına dair uluslararası alandaki ilk kapsamlı düzenleme, OECD tarafından 1980 yılında yayımlanan "Mahremiyetin ve Kişisel Verilerin

Sınırlar Arası Aktarımının Korunması" Rehber İlkeleridir. Bu ilkeler sekiz temel başlıkta toplanmıştır: sınırlı veri toplama, veri kalitesi, amaç belirliği, sınırlı kullanım, veri güvenliği, açıklık, bireysel katılım ve hesap verebilirlik (Akıncı, 2019). Bu ilkeler, verilerin yalnızca belirli amaçlar doğrultusunda toplanmasını, sınırlı biçimde kullanılmasını ve sürece bireylerin dâhil olmasını esas alır. Ayrıca, veriyi işleyen kişi veya kurumların hesap verebilirliğini zorunlu kılar.

Avrupa Birliği düzeyinde ise 1995'te yürürlüğe giren Veri Koruma Direktifi, kişisel verilerin işlenmesine yönelik ilk hukuki metindir. Ancak asıl dönüm noktası, 2016 yılında kabul edilen ve doğrudan tüm üye ülkelerde geçerli olan Genel Veri Koruma Tüzüğü (GDPR) olmuştur. GDPR; hukukilik, dürüstlük, şeffaflık, amaçla sınırlılık, doğruluk, veri minimizasyonu, saklama süresi sınırı, bütünlük, gizlilik ve eşit sorumluluk ilkeleriyle kişisel verilerin korunmasına yönelik daha güçlü ve kapsamlı bir yapı sunmaktadır. Kişisel verilerin korunması, özel hayatın gizliliği ilkesi çerçevesinde birçok ulusal ve uluslararası düzenlemede güvence altına alınmıştır. Türkiye Cumhuriyeti Anayasası'nın 20. maddesi, bireylerin özel ve aile hayatına saygı gösterilmesini isteme hakkını tanımakta; bu alanların gizliliğine dokunulamayacağını açıkça belirtmektedir. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi de benzer şekilde özel yaşam, konut ve yazışma mahremiyetini koruma altına almaktadır. Türk Ceza Kanunu'nun 9. bölümü ise "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında bu alandaki ihlallere ilişkin cezai yaptırımları düzenlemektedir. Türkiye'de kişisel verilerin korunmasına yönelik ilk resmi girişim Sekizinci Kalkınma Planı ile başlatılmış; ancak bu alandaki temel yasal dayanak, Onuncu Kalkınma Planı kapsamında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu olmuştur (mevzuat.gov.tr, ET: 07.06.2025).

5. TARTIŞMA, SONUÇ VE ÖNERİLER

Bu çalışmada, akıllı şehirlerin güvenlik teknolojileri bağlamında çok boyutlu bir analizi gerçekleştirilmiş, bu teknolojilerin sunduğu fırsatlar ile bireysel hak ve özgürlükler üzerinde yarattığı tehditler kapsamlı biçimde değerlendirilmiştir. Araştırmanın bulguları, akıllı şehir teknolojilerinin kentsel yaşam kalitesini artırma potansiyeli ile demokratik değerler arasında hassas bir denge kurulması gerektiğini ortaya koymaktadır.

5.1. Öneriler ve yol haritası

Araştırmanın bulguları ışığında, Türkiye'de akıllı şehir güvenlik teknolojilerinin etik ve sürdürülebilir kullanımı için kapsamlı bir yol haritası önerilmektedir:

1. Yasal ve Düzenleyici Çerçeve:

KVKK'nın akıllı şehir teknolojilerini kapsayacak şekilde güncellenmesi gerekmektedir. Özellikle biyometrik veri kullanımı, algoritmik karar verme süreçleri ve büyük veri analitiği konularında spesifik düzenlemeler yapılmalıdır. AB'nin GDPR'ı model alınarak, veri minimizasyonu, amaç sınırlılığı ve hesap verebilirlik ilkeleri güçlendirilmelidir. Yüz tanıma ve davranış analizi gibi invazif teknolojilerin kullanımı için açık yasal sınırlar belirlenmeli, bu teknolojilerin kullanımı bağımsız denetim mekanizmalarına tabi tutulmalıdır.

2. Etik Kurallar ve Standartlar:

Ulusal Akıllı Şehir Etik Kurulu kurularak, teknoloji kullanımında etik ilkelerin belirlenmesi ve uygulanması sağlanmalıdır. ISO/TC 268 Sürdürülebilir Şehirler ve Topluluklar standartlarına uyum zorunlu hale getirilmelidir. Algoritmik şeffaflık ilkesi benimsenerek, karar verme süreçlerinin denetlenebilir olması sağlanmalıdır. Özellikle kolluk kuvvetlerinin kullandığı sistemlerde algoritmik önyargı testleri zorunlu tutulmalıdır.

3. Vatandaş Katılımı ve Demokratik Denetim:

Akıllı şehir projelerinde vatandaş katılımı mekanizmaları güçlendirilmelidir. Barcelona'nın katılımcı bütçe modeli örnek alınarak, teknoloji yatırımlarında vatandaş görüşü alınmalıdır. Dijital platformlar üzerinden şeffaf geri bildirim sistemleri kurulmalıdır. Sivil toplum örgütlerinin denetim süreçlerine aktif katılımı sağlanmalıdır. Teknoloji etki değerlendirme raporları kamuoyuyla paylaşılmalıdır.

4. Dijital Kapsayıcılık:

Dijital uçurumu kapatmak için ulusal bir strateji geliştirilmelidir. Yaşlılar, engelliler ve göçmenler için özel dijital okuryazarlık programları düzenlenmelidir. Kamu hizmetlerinde dijital ve geleneksel yöntemlerin birlikte sunulması sağlanmalıdır. Düşük gelirli bölgelerde ücretsiz internet erişim noktaları artırılmalıdır. Dijital hizmetlerde evrensel tasarım ilkeleri uygulanmalıdır.

5. Veri Güvenliği ve Mahremiyet:

Güçlü şifreleme ve anonimleştirme teknikleri zorunlu hale getirilmelidir. Veri saklama süreleri minimize edilmeli, gereksiz veriler otomatik olarak silinmelidir. Bireysel veri erişim ve silme hakları güçlendirilmelidir. Veri ihlali durumunda zorunlu bildirim mekanizmaları oluşturulmalıdır. Hassas verilerin işlenmesi için açık rıza şartı katı biçimde uygulanmalıdır.

6. Teknolojik Egemenlik:

Yerli teknoloji üretimi teşvik edilmelidir. Açık kaynak kodlu sistemlerin kullanımı önceliklendirilmelidir. Kritik altyapılarda yabancı teknolojilere bağımlılık azaltılmalıdır. Üniversite-sanayi işbirliği güçlendirilerek, yerli çözümler geliştirilmelidir. Teknoloji transfer mekanizmaları iyileştirilmelidir.

7. Kapasite Geliştirme:

Yerel yönetim personeline akıllı şehir teknolojileri eğitimi verilmelidir. Üniversitelerde disiplinlerarası akıllı şehir programları açılmalıdır. Kamu çalışanları için veri güvenliği ve etik konularında zorunlu eğitimler düzenlenmelidir. Uluslararası deneyim paylaşımı programları geliştirilmelidir.

8. İzleme ve Değerlendirme:

Akıllı şehir projelerinin sosyal etki değerlendirmeleri yapılmalıdır. Performans göstergeleri belirlenerek düzenli raporlama sağlanmalıdır. Bağımsız denetim mekanizmaları kurulmalıdır. Vatandaş memnuniyet anketleri düzenli olarak yapılmalıdır. Başarısız projelerin nedenleri analiz edilerek dersler çıkarılmalıdır.

9. Finansman Modelleri:

Sürdürülebilir finansman modelleri geliştirilmelidir. Kamu-özel işbirliği mekanizmaları etik ilkeler çerçevesinde düzenlenmelidir. AB fonları ve uluslararası finansman kaynaklarından yararlanma kapasitesi artırılmalıdır. Yerel yönetimlere teknik destek fonları oluşturulmalıdır.

10. Pilot Uygulamalar ve Ölçeklendirme:

Living lab yaklaşımıyla pilot bölgeler oluşturulmalıdır. Başarılı uygulamaların diğer şehirlere transferi için mekanizmalar geliştirilmelidir. Başarısızlık toleransı olan deneysel alanlar yaratılmalıdır. En iyi uygulama örnekleri dokümante edilerek paylaşılmalıdır.

5.2. Sonuç

Bu çalışma, akıllı şehirlerde güvenlik teknolojilerinin sunduğu fırsatlar ile yarattığı risklerin dengeli bir analizini sunmuştur. Bulgularımız, teknolojinin kendisinin nötr olduğunu, ancak kullanım biçimi ve yönetişim modelinin belirleyici olduğunu ortaya koymaktadır. Türkiye'nin akıllı şehir yolculuğunda, teknolojik determinizmden kaçınarak, insan merkezli, katılımcı ve etik ilkelere dayalı bir yaklaşım benimsenmesi kritik öneme sahiptir.

Akıllı şehir teknolojileri, kentsel sorunlara çözüm potansiyeli taşırken, aynı zamanda yeni güvenlik açıkları, mahremiyet ihlalleri ve demokratik değerlere yönelik tehditler yaratmaktadır. Bu ikili doğanın farkında olarak, teknolojinin toplumsal faydayı maksimize edecek ve riskleri minimize edecek şekilde kullanılması gerekmektedir.

Önerilen yol haritası, yalnızca teknik çözümleri değil, aynı zamanda yasal, etik, sosyal ve ekonomik boyutları da kapsayan bütüncül bir yaklaşım sunmaktadır. Bu yaklaşımın başarısı, tüm paydaşların – merkezi ve yerel yönetimler, özel sektör, akademi, sivil toplum ve vatandaşlar – aktif katılımı ve işbirliğine bağlıdır.

Gelecek araştırmalar için öneriler arasında, Türkiye'deki akıllı şehir uygulamalarının uzun vadeli etkilerinin ampirik olarak değerlendirilmesi, vatandaş algı ve deneyimlerinin derinlemesine incelenmesi, farklı şehir modellerinin karşılaştırmalı analizi ve teknoloji-insan etkileşiminin psikolojik ve sosyolojik boyutlarının araştırılması yer almaktadır.

Sonuç olarak, akıllı şehirler çağında güvenlik ve özgürlük arasındaki dengenin kurulması, 21. yüzyılın en önemli toplumsal meydan okumalarından biridir. Bu dengenin başarıyla kurulması, yalnızca teknolojik yenilik değil, aynı zamanda demokratik değerlere bağlılık, etik duyarlılık ve toplumsal adalet perspektifi gerektirmektedir. Türkiye'nin bu yolculukta başarılı olması, küresel akıllı şehir deneyimlerinden öğrenmesi, yerel bağlamı gözetmesi ve insan onurunu merkeze alan politikalar geliştirmesi ile mümkün olacaktır.

KAYNAKÇA

Aebi, M. F. (2004). Crime trends in Western Europe from 1990 to 2000. *European journal on criminal policy and research*, *10*(2), 163-186.

Ahvenniemi, H. vd. (2017). What are the differences between sustainable and smart cities?. *Cities*, *60*, 234-245.

Ak, T. (2024). Kentlerde Suç ve Akıllı Kentler Yaklaşımı Ekseninde Türkiye'de Kentleşme ve Kent Güvenliği. *Kent Akademisi*, *17*(3), 1005-1029.

Akçay, M., & Çetinkaya, H. H. (2011). Kampüslerde uygulanan yeni biyometrik sistemler. *Akademik Bilişim*, *11*.

Akdamar, E. (2017). Akıllı Kent İdealine Ulaşmada Büyük Verinin Rolü. Kent Akademisi, 10(30), 200-215.

Akgül, H. (2013). Türkiye'de Akıllı Kent Proje Örnekleri. *Avrupa Birliği Akıllı Kent Uygulamaları ve Türkiye'deki Yansımaları*, 1789-*1795*.

Akıllı Şehirler Portalı (2023). *Akıllı Şehir Bileşenleri.* [Erişim: 05.08.2025, https://www.akillisehir.com/idet/77/989/akilli-sehir-bilesenleri]

Akıncı, A. N. (2019). *Büyük veri uygulamalarında kişisel veri mahremiyeti*. TC Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

Akpınar, M. T. (2019). Smart city applications in digital age: State-of-art review and critique. *Journal of Information Systems and Management Research*, *1*(1), 37-42.

Akpulat, O. (2017). Sürdürülebilir Şehirlerde Atık Yönetimi. *TSE Standard Ekonomik ve Teknik Dergi*, 32-37.

Alacadağlı, E. (2020). Güvenli kent ve kent güvenliği üzerine bir irdeleme. *Giresun Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *6*(2), 152-167.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of urban technology*, *22*(1), 3-21.

Alp, Ö. (2018). *Akıllı şehirlerde siber güvenlik.* (Yayınlanmış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Altınışık, H. U. (2018). Srategıes and polıcıes for the smart cıtıes ın Turkey/Türkiye'de akıllı kentlere yönelik stratejiler ve politikalar. *Tourısm human rıghts & sustaınable envıronment*, 135-159.

Amoozadeh, M. vd. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*(6), 126-132.

Amrutha, C. V., Jyotsna, C., & Amudha, J. (2020). Deep learning approach for suspicious activity detection from surveillance video. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (335-339). IEEE.

Ariç, H. (2011). *Bulanık kümelemeli yapay sinir ağları ile biyometrik tanıma.* (Yayınlanmış Yüksek Lisans Tezi). Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Armstrong, G., & Norris, C. (2020). *The maximum surveillance society: The rise of CCTV*. Routledge.

Arslan, G. Y. (2014). Kentsel dönüşümün sürdürülebilirlik boyutu: Hammarby (İsveç) ve Fener-Balat örneklerinin incelenmesi. *Artium*, *2*(2), 180-190.

Aslan, M. M. (2018). *Akıllı kent uygulamaları üzerine bir inceleme: Kahramanmaraş örneği*. (Yayınlanmış Yüksek Lisans Tezi). Mustafa Kemal Üniversitesi, Sosyal Bilimler Enstitüsü, Hatay.

Aslan, M. M., & Bulut, Y. (2019). Akıllı kent uygulamalarının kentsel güvenlik açısından önemi. *ASSAM Uluslararası Hakemli Dergi*, 52-60.

Aslan, M. M. (2024). Akıllı Kent Uygulamalarının Kentlerde Yaşanan Trafik Sorununun ve Ulaşıma Bağlı Olarak Ortaya Çıkan Çevre Kirliliğinin Azaltılmasına Etkisi: Akıllı Ulaşım Uygulamaları. *JOEEP: Journal of Emerging Economies and Policy*, *9*(2), 388-399.

Ateş, M., & Önder, D. E. (2019). 'Akıllı Şehir' Kavramı ve Dönüşen Anlamı Bağlamında Eleştiriler. *Megaron*, *14*(1).

Atha, K. vd. (2020). *China's smart cities development*. SOS International LLC, Intelligence Solutions Group. Prepared for the U.S.-China Economic and Security Review Commission. Retrieved from https://www.uscc.gov/research/chinas-smart-cities-development

Axxon Intellect Enterprise (2024). Entegre güvenlik çözümleri: Yüz tanıma ve arama işlemleri. [Erişim:21.08.2024, https://www.axxonsoft.com/integrated_security_solutions/face_recognition/]

Aydınbaş, G. (2023). Akıllı turizm (turizm 4.0) teknolojileri üzerine iktisadi bir yaklaşım: Türkiye örneği. *Journal of Tourism Intelligence and Smartness*, *6*(1), 26-44.

Bakıcı, T., Almirall, E., & Wareham, J. (2012). The underlying mechanisms of online open innovation intermediaries. *Copia elettronica scaricata da: http://ssrn. com/abstract*, *2141908*.

Balayan, A. A., & Tomin, L. V. (2021). Surveillance City. Digital Transformation of Urban Governance in Autocratic Regimes. In *2021 Communication Strategies in Digital Society Seminar (ComSDS)* (196-200). IEEE.

Balık, İ., Aydın, S. Z., & Bitiktaş, F. (2022). Türk Boğazları trafik yoğunluğu, bekleme süreleri ve deniz kazaları. *Kent Akademisi*, *15*(1), 262-276.

Bao, Y., & Du, Z. (2023). Face Recognition Technology Risks and Regulatory Issues. 10.2991/978-94-6463-040-4_99.

Barbole, A. N., & Godase, M. (2012). *Biometric Security Systems: A Comparative Review*. *Indian Streams Research Journal*.

Bayram, F. (2020). Derin öğrenme tabanlı otomatik plaka tanıma. *Politeknik Dergisi*, *23*(4), 955-960.

Berrehili, F. Z., & Belmekki, A. (2016). Privacy preservation in the Internet of Things. In *International symposium on ubiquitous networking* (163-175). Singapore: Springer Nature Singapore.

Bhuiyan, J. (2021). Major camera company can sort people by race, alert police when it spots Uighurs. [Erişim: 21.06.2025, https://ethicsatwork.nd.edu/resources/major-camera-company-can-sort-people-by-race-alert-police-when-it-spots-uighurs/]

Bibri, S. E., & Krogstie, J. (2017). Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustainable cities and society*, *31*, 183-212.

Bilici, Z., & Babahanoğlu, V. (2018). Akıllı kent uygulamaları ve Konya örneği. *Akademik Yaklaşımlar Dergisi*, *9*(2), 124-139.

Bilgin, M. (2008). *Biyometrik Seçim Sistemi Tasarımı ve Gerçekleştirilmesi.* (Yayınlanmış Yüksek Lisans Tezi). Selçuk Üniversitesi, Konya.

Boz, Y., & Çay, T. (2019). Şehri akıllı yapan özellikler ve dünyada öne çıkan akıllı şehirler. *TMMOB Harita ve Kadastro Mühendisleri Odası*, *6*, 23-25.

Bulkeley, H., & Betsill, M. (2005). Rethinking sustainable cities: Multilevel governance and the'urban'politics of climate change. *Environmental politics*, *14*(1), 42-63.

Bulkeley, H., & Betsill, M. M. (2013). Revisiting the urban politics of climate change. *Environmental politics*, *22*(1), 136-154.

Canpolat, B. Y. (2024). *Geleceğin Mimarisinde Kentsel Dönüşüm: Akıllı Şehirler*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul Aydın Üniversitesi, İstanbul.

Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell Publishers.

Clarke, R. V. G. (1992). Situational crime prevention: Successful case studies.

Cohen, B. (2018). *Blockchain cities and the Smart Cities Wheel*. *Medium*. [Erişim:20.08.2024, https://medium.com/iomob/blockchain-cities-and-the-smart-cities-wheel-9f65c2f32c36]

Czupich, Mariusz. (2019). *The Role of ICT in the Smart City Concept*. *Olsztyn Economic Journal, 14*(1), 63-74.

Çakır, H., & Babacan, H. K. (2011). Hareketi Algılayan Kamera Destekli Güvenlik Programı. *International journal of informatics technologies*, *4*.

Çalışkan, D., & Demir, Ö. (2022). Derin Öğrenme Yöntemleri ile Şüpheli Davraniş Tespiti. *International Periodical Of Recent Technologies İn Applied Engineering*, *3*(1), 28-43.

Çetin, D., Kara, Y., & Correia, Z. C. H. (2020). Sürdürülebilir ve akıllı kentler: Marmara depremi. *İdealkent*, *11*(31), 1933-1958.

Çetin, M., & Çiftçi, Ç. (2019). Literatüre göre dünya ve ülkemizden örneklerle akıllı kent kavramının irdelenmesi. *Ulusal Çevre Bilimleri Araştırma Dergisi*, *2*(3), 134-143.

Çevre, Şehircilik ve İklim Değişikliği Bakanlığı. (2019). *Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı (2020-2023)*. Ankara: ÇŞİB. [Erişim: 14.05.2025, https://cevresehiriklimkutuphanesi.csb.gov.tr/ShowPDF/dc6191d5-aa39-4bd2-b679-9ca2d44752a5]

Çodur, M. Y., & Topdağı, S. (2018). Akıllı ulaşım sistemlerinin kent içi toplu taşımaya etkisi: Erzurum ili örneği. *Erzincan University Journal of Science and Technology*, *11*(3), 576-586.

Dahlman, E., Parkvall, S., & Skold, J. (2013). *4G: LTE/LTE-advanced for mobile broadband*. Academic press.

Dameri, R. P. (2013). Searching for smart city definition: a comprehensive proposal. *International Journal of computers & technology*, *11*(5), 2544-2551.

Dede, G., & Sazlı, M. H. (2010). Biyometrik sistemlerin örüntü tanıma perspektifinden incelenmesi ve ses tanıma modülü simülasyonu. *EEBM Ulusal Kongresi*, 1-5.

Deloitte. (2016). *Delivering the Digital City: Best-in-class Customer Experience in Smart Cities*. [Erişim: 14.07.2025, https://www.deloitte.com/global/en/Industries/government-public/perspectives/gx-delivering-digital-city-customer-experience-smart-cities.html]

Demir, İ. (2016). Deniz kazalarını ve olaylarını araştırma ve inceleme yönetmeliği üzerine değerlendirmeler. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, *22*(3), 879-904.

de Luis-García, R. vd. (2003). Biometric identification systems. *Signal processing*, *83*(12), 2539-2557.

de Oliveira Fornasier, M., & Borges, G. S. (2023). The Chinese´ sharp eyes´ system in the era of hypervigilance: between state use and risks to privacy. *Revista Brasileira de Políticas Públicas*, *13*(1).

Düger, Y. (2023). Akıllı Şehirleri Bekleyen Temel Hak ve Özgürlük İhlalleri. Urban 21 Journal Yıl: 2023, Cilt: 1, Sayı 1. 1-15.

Eckhoff, D., & Wagner, I. (2017). Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), 489-516.

Efe, A. (2021). Yapay zekâ odaklı siber risk ve güvenlik yönetimi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, *5*(2), 144-165.

Elassy, M. vd. (2024). Intelligent transportation systems for sustainable smart cities. *Transportation Engineering*, *16*, 100252.

Elektrik Tesisat Portalı, Video Analiz CCTV 'nin Geleceği mi?,

[Erişim: 22.08.2024 https://www.elektriktesisatportali.com/video-analiz-cctv-nin-gelecegi-mi.html]

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), 491-497.

Erdinç, G. H. (2020). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. *Kişisel Verileri Koruma Dergisi*, *2*(1), 1-19.

Erkek, S. (2017). 'Akıllı şehircilik'anlayışı ve belediyelerin inovatif uygulamaları. *Medeniyet ve Toplum dergisi*, *1*(1), 55-72.

Ersoy, M., & Yiğit, T. (2017). Lte teknolojilerinde gerçek zamanlı ve yüksek çözünürlüklü video aktarımlarının performans analizleri. *Mühendislik Bilimleri ve Tasarım Dergisi*, *5*(1), 351-363.

Fabrègue, B. F., & Bogoni, A. (2023). Privacy and security concerns in the smart city. *Smart Cities*, *6*(1), 586-613.

Finn, R. L., Wright, D., & Friedewald, M. (2012). Seven types of privacy. In *European data protection: coming of age* (3-32). Dordrecht: Springer Netherlands.

Flak, L. S., & Hofmann, S. (2020). The Impact of Smart City Initiatives on Human Rights. In *EGOV-CeDEM-ePart-** (165-174).

Fraiji, Y. vd. (2018). Cyber security issues of Internet of electric vehicles. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (1-6). IEEE.

Gade, R. vd. (2016). Thermal imaging systems for real-time applications in smart cities. *International Journal of Computer Applications in Technology*, *53*(4), 291-308.

Gaffney, C., & Robertson, C. (2018). Smarter than smart: Rio de Janeiro's flawed emergence as a smart city. *Journal of Urban Technology*, *25*(3), 47-64.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. " O'Reilly Media, Inc.".

Genç, Y., & Erciyes, E. (2020). İnsansız hava araçları (İHA) tehditleri ve güvenlik yönetimi. *Türkiye insansız hava araçları dergisi*, *2*(2), 36-42.

Gershgorn, D. (2021). China´s „Sharp Eyes“ Program Aims to Surveil 100% of Public Space. Retrieved from https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015, (27.07.2025).

Giffinger, R. vd. (2007). Smart cities. Ranking of European medium-sized cities. Final report.

Gil-Jiménez, P. vd. (2007). Automatic control of video surveillance camera sabotage. In *International work-conference on the interplay between natural and artificial computation* (222-231). Berlin, Heidelberg: Springer Berlin Heidelberg.

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV* (Vol. 292). London: Home Office Research, Development and Statistics Directorate.

Goold, B. J. (2004). *CCTV and policing: Public area surveillance and police practices in Britain*. OUP Oxford.

Greenstone, M., Hornbeck, R., & Moretti, E. (2010). Identifying agglomeration spillovers: Evidence from winners and losers of large plant openings. *Journal of political economy*, *118*(3), 536-598.

Gürler, M. (2025). Türk Ceza Kanunu'ndaki Kişisel Verilerin Korunmasına İlişkin Suçlar Bakımından Hukuka Uygunluk Sebepleri. Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 11(2), 979-1008. https://doi.org/10.54699/andhd.1678041

Gürsoy, O. (2019). *Akıllı Kent Yaklaşımı ve Türkiye'deki Büyükşehirler İçin Uygulama İmkânları*. (Yayınlanmış Yüksek Lisans Tezi). Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Kamu Yönetimi Bilim Dalı, , Ankara.

Güvendik, A. (2016). Akıllı şehirler için akıllı teknolojiler. *Uluslararası Sürdürülebilir Yapılı Çevre Konferansı*, 13-15.

Hansen, J. L., & Skaiaa, A. (2019). The impact of smart city initiatives on human rights. *A Qualitative Research Study. University of Agder*.

Harrison, C., & Donnelly, I. A. (2011). A theory of smart cities. In *Proceedings of the 55th Annual Meeting of the ISSS-2011, Hull, UK*.

Heitlinger, S., & Comber, R. (2018). Design for the right to the smart city in more-than-human worlds. *arXiv preprint arXiv:1803.10530*.

Herzberg, C. (2017). Akıllı Şehirler Dijital Ülkeler (Çev. Nadir Özata), İnfoloji-Optimist Yayın Dağıtım, İstanbul.

Hickling, C. (2025). Surveillance technologies and human rights. [Erişim: 18.06.2025, https://www.startts.org.au/media/Surveillance-technology-and-human-rights.pdf]

Hunt, D. (2014). Smart cities: Contradicting definitions and unclear measures. In *Proceedings of the 4th world sustainability forum*.

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *computers & security*, *25*(7), 498-506.

Ilgaz, A., & Saltan, M. (2017). Ortalama hız uygulamasının verimliliğini etkileyen durumlar: sürücülerin hız davranışı üzerine bir çalışma. *Uluslararası Teknolojik Bilimler Dergisi*, *9*(2), 23-38.

İçişleri Bakanlığı (2022). "İstanbul İstiklal Caddesi Terör Saldırısı Resmi Açıklaması".

Jabbari J. vd. (2019). Citizens as real-time emotional sensors in smart cities. In *International conference on smart infrastructure and construction 2019 (ICSIC) driving data-informed decision-making* (571-576). ICE Publishing. Jian, M., Lu, Z., & Chen, V. C. (2018). Drone detection and tracking based on phase-interferometric Doppler radar. 2018 IEEE Radar Conf, 1146–1149.

Jain, A. L., & Sharath Pankanti, H. (2003). Biometric identification systems, signal processing. *ACM*, *83*(12), 2539-2557.

Jan, M. A. vd. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems*, *80*, 613-626.

Kalbo, N. vd. (2020). *The Security of IP-Based Video Surveillance Systems. Sensors, 20(17), 4806.* doi:10.3390/s20174806

Karasu, M. A. (2008). Türkiye'de kentleşme dinamiklerinin suça etkisi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, *57*(4), 255-281.

Karasu, M. A. (2012). Kent ve suç üzerine kavramsal bir çerçeve. *Cumhuriyet University Journal of Economics & Administrative Sciences/Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *13*(2).

Kaymaz, S. (2010). *Çevrimdışı İmza Tanıma.* (Yayınlanmış Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.

Kaypak, Ş. (2024). Kentsel bir sorun olarak kentsel güvenlik. *The Journal of Academic Social Science*, *33*(33), 35-50.

Kempin Reuter, T. (2019). Human rights and the city: Including marginalized communities in urban development and smart cities. *Journal of Human Rights*, *18*(4), 382-402.

Keskin, H. İ., & Kum, S. (2012). Deniz Emniyet ve Güvenliğinde Lrit Sistemi. *Dokuz Eylül Üniversitesi Denizcilik Fakültesi Dergisi*, *4*(2), 47-57.

Kızrak, M. A., & Bolat, B. (2018). Derin öğrenme ile kalabalık analizi üzerine detaylı bir araştırma. *Bilişim Teknolojileri Dergisi*, *11*(3), 263-286.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1-14.

Kitchin, R. (2016). "Getting smarter about smart cities: Improving Data Privacy and Data Security." Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Kitchin, R., Cardullo, P., & Di Feliciantonio, C. (2019). Citizenship, justice, and the right to the smart city. In *The right to the smart city* (pp. 1-24). Emerald Publishing Limited.

Kocaman, E. G. (2020). Akıllı ve sakin şehirler için enerji çözümleri. *İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *2*(2), 40-47.

Komninos, N. (2008). *Intelligent cities and globalisation of innovation networks*. Routledge.

Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific reports*, *11*(1), 100.

Koss, K. K. (2015). Leveraging predictive policing algorithms to restore fourth amendment protections in high-crime areas in a post-Wardlow world. *Chi.-Kent L. Rev.*, *90*, 301.

Kumar, N. (2019). *Saudi Arabia Drone Attack: Sign of Changing Character of Hybrid War*.

Liang, Z., Tan, F., & Chi, Z. (2012). Video-based biometric identification using eye tracking technique. In *2012 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2012)* (728-733). IEEE.

Lim, C., Kim, K. J., & Maglio, P. P. (2018). Smart cities with big data: Reference models, challenges, and considerations. *Cities*, *82*, 86-99.

Llauradó, J. M. vd. (2023). Study of image sensors for enhanced face recognition at a distance in the Smart City context. *Scientific Reports, 13*(1), 14713. https://doi.org/10.1038/s41598-023-40110-y

Lugaric, L., Krajcar, S., & Simic, Z. (2010). Smart city—Platform for emergent phenomena power system testbed simulator. *In 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe)* (1-7). IEEE.

Mamak, U. vd. (2020). Gerçek zamanlı yüz tanıma tabanlı personel kontrol ve takip sistemi tasarımı. *Avrupa Bilim ve Teknoloji Dergisi*, (19), 497-504.

Mantelero, A., & Esposito, M. S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, 105561.

Martin, K. E. (2020). Ethical issues in the big data industry. In *Strategic information management* (450-471). Routledge.

Martinus, M. (2022). Smart city and privacy concerns during COVID-19: Lessons from Singapore, Malaysia, and Indonesia. In *Smart Cities in Asia: Regulations, Problems, and Development* (33-47). Singapore: Springer Nature Singapore.

McBride, K., Hammerschmid, G., & Cingolani, L. (2022). Policy Brief: Human Centric Smart Cities-Redefining the smart city. *Hertie School Centre for Digital Governance*, 1-19.

Meral, O. (2008). *Doğrusal Öngörülü Kodlama ve Adaptif Algoritma Tabanlı Konuşmacı Tanıma*. (Yayınlanmış Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Murray, D. vd. (2024). The chilling effects of surveillance and human rights: insights from qualitative research in Uganda and Zimbabwe. *Journal of Human Rights Practice*, *16*(1), 397-412.

Nabiyev, V. (2009). Kulak Biyometrisine Göre Kimlik Tespiti, 2. Mühendislik ve Teknoloji Sempozyumu, Ankara.

Naker, S., & Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *BUJ Sci. & Tech. L.*, *23*, 88.

Nässi, T. (2022). Facial Recognition–Technology for a Safer Future or Violation of the Right to Privacy.

Netser Grup (2024). Video yönetim yazılımı ve önemli VM özellikleri nelerdir. [Erişim: 21.08.2024, https://www.netser.com.tr/tr/blog/video-yonetim-yazilimi-ve-onemli-vmsozellikleri-nelerdir]

Nevin, R. (2007). Understanding international crime trends: the legacy of preschool lead exposure. *Environmental research*, *104*(3), 315-336.

Oğultürk, M. C., & Şahin, G. (2020). Eleştirel jeopolitik çerçevesinde akıllı şehirler ve şehir jeopolitiği. *Karadeniz Sosyal Bilimler Dergisi*, *12*(23), 417-433.

Örselli, E., & Akbay, C. (2019). Teknoloji ve kent yaşamında dönüşüm: akıllı kentler. *Uluslararası Yönetim Akademisi Dergisi*, *2*(1), 228-241.

Öz, K., & Görgünoğlu, S. (2016). Video gözetim sistemlerinde anomali tespiti üzerine bir derleme. *El-Cezeri*, *3*(3).

Özer, D.S. (2010). İristen kimlik tanıma, Yüksek Lisans Tezi, Kocaeli Üniversitesi, Kocaeli-Türkiye,

Payam, M. M. (2018). Emniyet, güvenlik, kent emniyeti ve kent güvenliği: Kavramsal bir analiz. *Avrasya Terim Dergisi*, *6*(1), 15-25.

Pierce, P., & Andersson, B. (2017). Challenges with smart cities initiatives–A municipal decision makers' perspective. *Proceedings of the 50th Hawaii International Conference on System Science.* 2804-2813.

Popoola, O. P., & Wang, K. (2012). Video-based abnormal human behavior recognition—A review. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *42*(6), 865-878.

Qarri, A., & Gill, L. (2022). Smart cities and human rights. *Future Cities Canada. Available online at: https://futurecitiescanada. ca/portal/resources/smartcities-and-human-rights/(accessed July 18, 2022)*.

Ramaswami, A., Baidwan, N.K., & Nagpure, A.S. (2016). Exploring social and infrastructural factors affecting open burning of municipal solid waste (MSW) in Indian cities: A comparative case study of three neighborhoods of Delhi. *Waste Management & Research,* 34(11).

Ramirez, E. (2013). *The privacy challenges of big data: a view from the lifeguard's chair*. US FTC.

Ramos, C. T. (2019). Democracy and governance in the smart city. In *Smart Cities: Issues and Challenges* (17-30). Elsevier.

Reuter, T. K. (2020). Smart city visions and human rights: Do they go together. *Carr Center for Human Rights Policy Harvard Kennedy School*, *6*, 1-19.

Selvi, E. vd. (2022). Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video, MDPI, 11, 4210.

Sengupta, U., & Sengupta, U. (2022). Why government supported smart city initiatives fail: Examining community risk and benefit agreements as a missing link to accountability for equity-seeking groups. *Frontiers in Sustainable Cities*, *4*, 960400.

Shelton, T., & Lodato, T. (2019). Actually existing smart citizens: Expertise and (non) participation in the making of the smart city. *City*, *23*(1), 35-52.

Sınmaz, S. (2013). Yeni gelişen planlama yaklaşımları çerçevesinde akıllı yerleşme kavramı ve temel ilkeleri. *Megaron*, *8*(2), 76.

Singh, B. (2015). Smart city-smart life-Dubai Expo 2020. *An Experience of Bangladeshi Garment Industry*.

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *Ai & Society*, *37*(1), 167-175.

Stasiak, K. vd. (2018). A study on using different kinds of continuous-wave radars operating in C-Band for drone detection. 22nd Int. Microwave Radar Conf. (MIKON), 521–526

Süleymanlı, H. (2019). *Sürdürülebilir Kent Yönetimi ve Akıllı Kent Uygulamaları*. (Yayınlanmış Yüksek Lisans Tezi). Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Şengül, R., & Altıntaş, H. Y. (2020). Akıllı kentin bir bileşeni olarak akıllı ulaşım uygulamalarının incelenmesi: Kocaeli büyükşehir belediyesi örneği. *Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi*, *6*(2), 487-502.

T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı (2024). Akıllı Şehir Rehberlik Uygulamaları Projesi, Görüntü İşlemeye Dayalı Güvenlik Sistemleri Uygulaması. [Erişim: 05.08.2025, https://www.akillisehirler.gov.tr/wp-content/uploads/fizibilite-rapor/12-G%C3%B6r%C3%BCnt%C3%BC%20%C4%B0%C5%9Flemeye%20Dayal%C4%B1%20G%C3%BCvenlik%20Sistemleri.pdf]

Tao, M., Jiang, R., & Downs, C. (2022). Ethics of Face Recognition in Smart Cities Toward Trustworthy AI. In *Big Data Privacy and Security in Smart Cities* (23-52). Cham: Springer International Publishing.

Townsend, A. M. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*. WW Norton & Company.

Thilakarathne, N. N., & Madhuka Priyashan, W. D. (2021). An overview of security and privacy in smart cities. *IoT and IoE Driven Smart Cities*, 21-44.

Tosun, M. B. (2009). *Akıllı Kart ve Parmak İzi Kullanan Geliştirilmiş Güvenlik Sistemi Tasarımı*. (Yayınlanmış Yüksek Lisans Tezi). Hacettepe Üniversitesi, Ankara.

Tozkoparan, İ. B. (2019). Değişen Güvenlik Anlayışında Geleceğin Akıllı Kentleri. *ASSAM Uluslararası Hakemli Dergi*, *13*, 417-427.

Uçar, A., Negiz, N., & Şemşit, S. (2017). Avrupa Birliği Akilli Kent Uygulamalari ve Türkiye'deki Yansimalari. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *22*(Kayfor 15 Özel Sayısı), 1785-1798.

United Nations Human Settlements Programme (UN-Habitat) (2021). Addressing the Digital Divide, Taking Action towards Digital Inclusion. [Erişim: 04.08.2025, https://unhabitat.org/sites/default/files/2021/11/addressing_the_digital_divide.pdf]

Van Dijk, J. A. (2012). The evolution of the digital divide-the digital divide turns to inequality of skills and usage. In *Digital enlightenment yearbook 2012* (57-75). IOS Press.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

Velibeyoğlu, K. (2019). Akıllı kentler: vaatler ve ötesi. *Yenilikçi Sürdürülebilir Gelişme Stratejileri Bağlamında Türkiye Ekonomisinin Geleceğine Yönelik Çözüm Arayışları (Ed. S. Şanlısoy), İlkim Ofset, İzmir*.

Xia, L. M., Yang, B. J., & Tu, H. B. (2015). Recognition of suspicious behavior using case-based reasoning. *Journal of Central South University*, *22*(1), 241-250.

Warren, S., & Brandeis, L. (1989). The right to privacy. In *Killing the messenger: 100 Years of media criticism* (1-21). Columbia University Press.

Welsh, B. C., & Farrington, D. P. (2008). Effects of closed circuit television surveillance on crime. *Campbell systematic reviews*, 4(1), 1-73.

Welsh, B. C., & Farrington, D. P. (2009). *Making public places safer: Surveillance and crime prevention*. Oxford University Press.

Wernick, A., & Artyushina, A. (2023). Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies. *Internet policy review*, *12*(1), 1-26.

Whittaker, Z. (2021). *When surveillance meets incompetence*. TechCrunch. [Erişim: 17.04.2025, https://techcrunch.com/2019/02/19/when-surveillance-meets-incompetence/]

Yalçın, N., & Gürbüz, F. (2015). Biyometrik güvenlik sistemlerinin incelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *3*(2), 398-413.

Yalçın, N. (2006). *Konuşmacı Tanıma Teknolojisi Yardımıyla İlköğretim Birinci Sınıf Öğrencilerine İlkokuma Yazma Öğretimi için Bir Yazılım Geliştirme*. (Doktora Tezi). Gazi Üniversitesi, Ankara.

Yaman, M., & Çakır, E. (2018). Dijitalleşen dünyada akıllı afet ve acil durum uygulamaları. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, *7*(2), 1124-1138.

Yamin, M. M. vd. (2021). Weaponized AI for cyberattacks, Journal of Information Security and Applications, Volume 57, 102722.

Yapraklı, Ş., & Noksan, E. (2021). Kentsel Dönüşüm Hizmetlerinin Kentsel Yaşam Kalitesi Algısı Üzerindeki Etkisinin İncelenmesi: Erzurum Kent Merkezinde Yaşayanlar Üzerinde Bir Uygulama. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *11*(1), 69-93.

Yıldız, A., & Baz, İ. (2021). Bütüncül planlama anlayışının kentsel dönüşüm üzerindeki etkisi: tuzla örneği. *İstanbul Ticaret Üniversitesi Teknoloji Ve Uygulamalı Bilimler Dergisi*, *3*(2), 137-150.

Zhang, K. vd. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications. Volume:55. 122-129.