



T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI



DİJİTAL DÖNÜŞÜM SÜRECİNDE KENT GÜVENLİĞİ: KENT
GÜVENLİK YÖNETİM SİSTEMİ (KGYS) ÜZERİNE BİR ARAŞTIRMA

MUSTAFA AKARSU

YÜKSEK LİSANS TEZİ

DANIŞMAN
PROF. DR. MUSTAFA KOCAOĞLU

KONYA - 2025

BİLİMSEL ETİK SAYFASI

Öğrencinin	Adı Soyadı	MUSTAFA AKARSU		
	Numarası	22081031901		
	Ana Bilim / Bilim Dalı	Yönetim Bilişim Sistemleri		
	Programı	Tezli Yüksek Lisans	✓	
		Doktora		
Tezin Adı	Dijital Dönüşüm Sürecinde Kent Güvenliği: Kent Güvenlik Yönetim Sistemi (KGYS) Üzerine Bir Araştırma			

Bu tezin hazırlanmasında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Mustafa AKARSU

ÖZET

Bu çalışma, dijital dönüşüm sürecinin kent güvenliği üzerindeki yansımalarını, Kent Güvenlik Yönetim Sistemi (KGYS) örneği temelinde analiz etmeyi hedeflemektedir. Araştırmada, güvenlik hizmetlerinin dijitalleşme ile birlikte geçirdiği yapısal dönüşüm incelenmiş; bu teknolojik sistemlerin, toplumsal algı, tutum ve deneyimler bağlamında nasıl değerlendirildiği anlamlandırılmaya çalışılmıştır.

Verilerin toplanmasında nitel araştırma yaklaşımları benimsenmiş; saha çalışması kapsamında Kütahya il merkezinde görev yapan emniyet personeli ile birebir, derinlemesine görüşmeler gerçekleştirilmiştir. Bu görüşmelerde, katılımcıların KGYS'ye ilişkin deneyimleri, sistemin işlevselliğine dair gözlemleri ve dijital güvenlik teknolojilerine yönelik bireysel ve kurumsal yaklaşımları kapsamlı biçimde ele alınmıştır. Elde edilen veriler, içerik analizi tekniğiyle değerlendirilmiş; sistematik kodlama ve temalaştırma süreçleri MAXQDA yazılımı aracılığıyla yürütülmüştür.

Görüşmelerden elde edilen bulgular, KGYS'nin kent güvenliğine katkı sağladığı yönünde genel bir uzlaşma bulunduğuna işaret etmektedir. Suç önleme, olaylara hızlı müdahale imkânı ve koordinasyonun artırılmasına yönelik olumlu değerlendirmelerin öne çıktığı gözlemlenmiştir. Kamera sistemlerinin etkinliği, anlık izleme kapasitesi ve olay yönetiminde sağladığı destek, katılımcı söylemlerinde belirgin şekilde yer bulmuştur. Bu bağlamda, sistemin güvenlik operasyonlarında işlevsel bir araç olarak benimsendiği anlaşılmıştır.

Bununla birlikte, dijital güvenlik sistemlerinin mahremiyet, veri güvenliği ve etik sorumluluklar bağlamında çeşitli endişelere yol açtığı da belirlenmiştir. Katılımcıların bir kısmı, bu tür uygulamaların bireysel hak ve özgürlükleri sınırlayıcı etkiler doğurabileceğine ilişkin görüşlerini ifade etmiştir. Özellikle yüz tanıma sistemleri ve yapay zekâ tabanlı analiz araçlarının kullanımında, etik sınırların açık ve denetlenebilir biçimde tanımlanması gerektiği vurgulanmıştır. Görüşmeler sürecinde, gözetim uygulamalarının bireyler üzerinde yaratabileceği psikolojik etkilerin sıklıkla dile getirildiği ve bu etkilerin mahremiyet algısı ile doğrudan ilişkili olduğu gözlemlenmiştir. Ayrıca, KGYS ile doğrudan etkileşim içinde bulunan personelin belirli bir kullanıcı profiline sahip olması, deneyimlerin homojen olmayan bir yapı

içerisinde şekillendiğine ve sistemin algılanış biçiminde farklılaşmaların ortaya çıkabildiğine işaret etmektedir.

Sonuç olarak, araştırma kapsamında elde edilen bulgular, KGYS'nin teknik ve operasyonel düzeyde kent güvenliğine önemli katkılar sunduğunu ortaya koymaktadır. Ancak sistemin uzun vadeli başarısının, yalnızca teknolojik altyapıya değil; aynı zamanda toplumsal kabul, etik ilkeler, mahremiyet ve veri güvenliği gibi unsurların dikkate alınmasına bağlı olduğu anlaşılmaktadır. Bu yönüyle KGYS, yalnızca bir güvenlik aracı değil; aynı zamanda dijitalleşmenin toplumsal dönüşüm üzerindeki etkilerini somutlaştıran bir yapı olarak değerlendirilmektedir. Araştırma, bu çok katmanlı yapısıyla literatüre hem uygulamalı hem de eleştirel bir perspektif sunmaktadır.

Anahtar Kelimeler: Kent Güvenlik Yönetim Sistemi, dijital dönüşüm, kent güvenliği, mahremiyet, veri güvenliği, toplumsal algı

ABSTRACT

This study aims to analyze the reflections of the digital transformation process on urban security, based on the example of the Urban Security Management System (KGYS). The research examines the structural transformation that security services have undergone with digitalization, and it seeks to make sense of how these technological systems are evaluated in the context of societal perception, attitudes, and experiences.

Qualitative research approaches were adopted for data collection; in the scope of the fieldwork, one-on-one, in-depth interviews were conducted with police personnel working in the city center of Kütahya. In these interviews, participants' experiences with the KGYS, their observations regarding the system's functionality, and their individual and institutional approaches to digital security technologies were comprehensively addressed. The data obtained were evaluated using content analysis techniques, and the processes of systematic coding and thematization were carried out through the MAXQDA software.

The findings obtained from the interviews indicate a general consensus that the KGYS contributes to urban security. Positive evaluations focusing on crime prevention, the possibility of rapid response to incidents, and enhanced coordination were observed to stand out. The effectiveness of camera systems, their real-time monitoring capacity, and the support they provide in incident management were prominently reflected in participant statements. In this context, it is understood that the system is embraced as a functional tool in security operations.

However, it was also determined that digital security systems raise various concerns in terms of privacy, data security, and ethical responsibilities. Some participants expressed the view that such practices may have restrictive effects on individual rights and freedoms. In particular, the need for clear and monitorable definitions of ethical boundaries in the use of facial recognition systems and AI-based analytical tools was emphasized. Throughout the interviews, the potential psychological impacts of surveillance practices on individuals were frequently mentioned, and these effects were observed to be directly related to perceptions of privacy. Additionally, the fact that personnel who directly interact with the Urban

Security Management System possess a specific user profile suggests that experiences are shaped within a non-homogeneous structure, and differences may emerge in how the system is perceived.

In conclusion, the findings obtained within the scope of the research reveal that KGYS makes significant contributions to urban security at the technical and operational levels. However, it is understood that the long-term success of the system depends not only on its technological infrastructure but also on the consideration of elements such as public acceptance, ethical principles, privacy, and data security. In this respect, KGYS is evaluated not only as a security tool but also as a structure that concretizes the impact of digitalization on social transformation. With its multilayered nature, the study offers both an applied and critical perspective to the literature.

Keywords: Urban Security Management System (USMS), digital transformation, urban security, privacy, data security, social perception

ÖNSÖZ

“Dijital Dönüşüm Sürecinde Kent Güvenliği: (KGYS) Üzerine Bir Araştırma” başlıklı bu tez çalışması, uzun soluklu bir akademik emeğin ve yoğun bir düşünsel sürecin ürünü olarak tamamlanmıştır. Çalışmanın her aşamasında yönlendirici katkıları, akademik birikimi ve kıymetli rehberliği ile sürece ışık tutan değerli danışmanım, Sayın Prof. Dr. Mustafa KOCAOĞLU’na en içten teşekkürlerimi sunmak isterim.

Ayrıca, gerek bilimsel yaklaşımları gerekse yapıcı eleştirileriyle tez savunma sürecine anlamlı katkılarda bulunan Sayın Prof. Dr. H. Buluthan ÇETİNTAŞ’ ve Sayın Doc. Dr. Hikmet Salahaddin GEZİCİ’ye de ayrı ayrı şükranlarımı sunarım.

Bu akademik sürecin en temel dayanağını ise hiç kuşkusuz hayatım boyunca bana destek olmayı sürdüren ailem oluşturmuştur. Maddi ve manevi olarak her koşulda yanımda yer alan, inançlarını ve sevgilerini hiçbir zaman eksik etmeyen kıymetli annem Şerife AKARSU ve babam Ali AKARSU’ya, yaşam yolculuğumdaki en büyük yoldaşım ve en güçlü desteğim olan eşim Zeynep AKARSU’ya minnettarlığımı ifade etmek isterim. Bu çalışmanın ortaya çıkmasında onların sabrı, anlayışı ve inancı her zaman yol gösterici olmuştur.

Tez sürecinde edinilen bilgiler ve yapılan çıkarımların, dijitalleşen güvenlik pratiklerine ve kent güvenliği yönetiminin kurumsal dönüşümüne katkı sunması temennisıyla...

Mustafa AKARSU

8.12.2025

İÇİNDEKİLER LİSTESİ

BİLİMSEL ETİK SAYFASI	i
ÖZET	ii
ABSTRACT	iv
ÖNSÖZ	vi
İÇİNDEKİLER LİSTESİ	vii
TABLolar LİSTESİ	x
GİRİŞ	1
BÖLÜM I	5
DİJİTAL DÖNÜŞÜM VE KENT GÜVENLİĞİ: KAVRAMSAL ÇERÇEVE	5
1.1. Dijitalleşme ve Dijital Dönüşüm Süreci	5
1.1.1. Dijital, Dijitalleşme ve Dijital Dönüşüm Kavramları.....	5
1.1.2. Kamu Yönetiminde Dijitalleşme	8
1.1.3. Akıllı Kentler ve Dijital Altyapılar	11
1.1.4. Dijital Dönüşümün Toplum ve Güvenlik Üzerindeki Etkileri.....	15
1.2. Kent Güvenliği ve Suç Kavramı Üzerine Kuramsal Yaklaşımlar	18
1.2.1. Kent Güvenliğinin Tanımı, Kapsamı ve Tarihsel Gelişimi.....	18
1.2.2. Kentsel Suç Kavramı ve Suç Türleri	24
1.2.3. Suç Önleme Stratejileri ve Güvenlik Yaklaşımları	27
1.2.4. Kent Güvenliğinde Teknolojik Uygulamalar	31
1.2.5. Yerel Yönetimlerin Kent Güvenliğindeki Rolü	35
BÖLÜM II	41
TÜRKİYE’DE KENT GÜVENLİK VE DİJİTAL İZLEME SİSTEMLERİNİN YAPISI, BİLEŞENLERİ VE GELİŞİM SÜRECİ	41
2.1. Kent Güvenlik Yönetim Sistemlerinin Yapısı ve Bileşenleri.....	41
2.1.1. Kent Güvenliğinde Görüntüleme Sistemleri: CCTV, IP Kameralar ve Sayısal Kayıt Teknolojileri	42
2.1.2. Mobil Uygulamalar ve Entegrasyon	44
2.1.3. Komuta Kontrol Merkezleri ve Veri Yönetimi	46
2.1.4. Veri Toplama, Saklama ve İşleme Süreçleri	48

2.2.	MOBESE ve KGYS Sistemlerinin Tarihsel Gelişimi	50
2.2.1.	MOBESE Sistemi: Kurulum Süreci ve Amaçları	51
2.2.2.	MOBESE'nin Teknik Bileşenleri	52
2.2.1.1.	Komuta Kontrol Merkezi (KKM)	53
2.2.1.2.	Görüntüleme Sistemleri	54
2.2.1.3.	Plaka Tanıma Sistemleri	55
2.2.1.4.	Araç Takip Sistemi (ATS).....	58
2.2.1.5.	Mobil Araç Sorgulama Sistemi (MAS)	60
2.2.1.6.	Muhtarlık Otomasyon Sistemi (MOS)	62
2.3.	Türkiye’de Dijital Güvenlik Sistemlerinin Evrimi	63
2.3.1.	Dijitalleşmede Güvenlik Politikaları: Hukuki ve Kurumsal Çerçeve..	63
2.3.2.	KGYS ve MOBESE Sistemlerinin Entegrasyon Süreci	65
BÖLÜM III.....		67
KENT GÜVENLİĞİ UYGULAMALARINA YÖNELİK SAHA		
ARAŞTIRMASI		67
3.1.	Araştırmanın Amacı, Kapsamı ve Yöntemi	67
3.1.1.	Araştırmanın Amacı ve Önemi	67
3.1.2.	Veri Toplama Yöntemleri ve Katılımcı Profili.....	68
3.1.3.	Sınırlılıklar	69
3.2.	MAXQDA Yazılımı ile Nitel Veri Analizi	70
3.3.	Analiz Sonuçları ve Raporlama Süreci	71
3.3.1.	Temalar ve Alt Temalar	72
3.3.2.	Katılımcı Görüşleri	74
3.3.3.	Kod Frekans Tablosu ve Kod Matrisi	76
3.3.4.	Örnek Kod Ağaçları (KGYS Üzerine).....	78
3.4.	Kütahya İl Merkezindeki Emniyet Personeline Yönelik Görüşme Verileri	80
3.4.1.	Deneyim Temasına İlişkin Bulgular	81
3.4.2.	Dijitalleşmenin Kent Güvenliğine Etkisine İlişkin Bulgular	83
3.4.3.	Dijital Güvenlik Sistemlerine İlişkin Bulgular	85
3.4.4.	Dijital Dönüşümün Kent Güvenliğine Etkisine İlişkin Bulgular	90
3.4.5.	Dijital Sistemlere Yönelik Algı ve Tutuma İlişkin Bulgular	93
3.4.6.	Sistemin Etkinliği ve Karşılaşılan Sorunlara İlişkin Bulgular	95

3.5. TARTIŞMA.....	98
3.5.1. KGYS'nin Etkililiğine Dair Görüşler.....	102
SONUÇ VE ÖNERİLER.....	109
KAYNAKÇA	114
EKLER	123



TABLÖLAR LİSTESİ

Tablo 1. Dijital Dönüşüm ve KGYS Bağlamında Görüşlerin Tematik Analizi 103



GİRİŞ

Dijitalleşme süreci, günümüz toplumlarında kamu yönetimi, toplumsal yapı ve güvenlik anlayışı üzerinde köklü değişimlere neden olmaktadır. Özellikle kentleşmenin hız kazandığı bir dönemde, dijital teknolojilerle desteklenen yönetim biçimleri, geleneksel uygulamaların yerini daha dinamik ve veri temelli sistemlere bırakmaktadır. Bu değişim, güvenlik hizmetlerinin sunumunu da derinden etkilemiştir. Artık kamu güvenliğine yönelik stratejiler, teknolojik altyapılar ve otomasyon destekli çözümler üzerinden şekillenmektedir.

KGYS, dijital çağın güvenlik ihtiyaçlarına yanıt verebilmek amacıyla geliştirilen, kentlerde güvenlik hizmetlerinin izlenmesini ve yönetilmesini sağlayan bütünlük bir sistemdir. Kent yaşamının karmaşıklaşması, artan güvenlik talepleri, suç tipolojilerinin çeşitlenmesi ve ulaşım ağlarının yoğunlaşması gibi unsurlar, geleneksel güvenlik anlayışını yetersiz hâle getirmiştir. Bu doğrultuda KGYS gibi sistemler, sadece olay sonrası müdahaleye değil, aynı zamanda önleyici güvenlik politikalarının uygulanmasına da imkân tanımaktadır.

Dijital dönüşüm kavramı, dijitalizasyon ve dijitalleşme süreçlerinden farklı olarak, teknolojik gelişmelerin kurumların işleyiş biçimlerini ve hizmet sunum modellerini yapısal olarak dönüştürdüğü bir süreci ifade etmektedir. Bu bağlamda dijitalizasyon, analog verilerin dijital ortama aktarılmasını; dijitalleşme, bu verilerin kullanılabilirliğini ve paylaşılabilirliğini; dijital dönüşüm ise bu teknolojilerin kurumsal karar alma mekanizmalarıyla bütünleşmesini ifade etmektedir. KGYS, bu dönüşüm sürecinin güvenlik alanındaki somut örneklerinden biri olarak değerlendirilmektedir.

Dijital güvenlik sistemlerinin kent yaşamına entegrasyonu, sadece teknik değil, aynı zamanda sosyolojik, yönetsel ve etik boyutları da içeren çok katmanlı bir dönüşümü gündeme getirmektedir. Güvenlik ile bireysel özgürlükler arasında kurulması gereken denge, bu tür sistemlerin işleyişinde önemli bir tartışma alanı yaratmaktadır. Kamuoyunda dijital güvenlik uygulamalarının nasıl algılandığı, toplumsal meşruiyetin sağlanmasında belirleyici olmaktadır. Dolayısıyla, bu sistemlerin sadece teknik yeterlilik üzerinden değil, aynı zamanda sosyal kabul ve yönetsel etkinlik çerçevesinde de değerlendirilmesi gerekmektedir.

Bu arařtırmada, KGYS'nin dijital dnřm srecindeki iřlevi ile kent gvenlięi politikalarının yeniden yapılandırılmasına yaptıęı katkı ele alınmaktadır. Dijitalleřmenin gvenlik hizmetlerine etkisi teknoloji merkezli bir bakıřla sınırlı tutulmayıp aynı zamanda insan odaklı bir yaklařımla deęerlendirilmiřtir. Sistemlerin teknik performansları kadar hizmet sunumu zerindeki yansımaları ve toplumsal algıda oluřturduęu etkiler de incelemenin temel odak noktaları arasında yer almaktadır.

Metin, giriř ve sonu blmleri dıřında  ana blmden oluřmaktadır. İlk blmde dijital dnřm, kent gvenlięi ve gzetim teknolojilerine iliřkin kavramsal ve kuramsal ereve sunulmuřtur. Bu kapsamda dijitalleřmenin kamu ynetimi zerindeki etkileri deęerlendirilmeye; dijitalizasyon, dijitalleřme ve dijital dnřm kavramları arasındaki kuramsal ayrımlar aıklanmaya alıřılmıřtır. Akıllı kent uygulamaları ve dijital altyapılar baęlamında gvenlik politikalarının geirdięi evrim tartıřılmıř, dijital dnřmn toplumsal yapılar ve gvenlik algısı zerindeki etkilerine odaklanılmıřtır. Ayrıca kent gvenlięi kavramının tarihsel geliřimi, kentsel su trleri, su nleme stratejileri ve teknolojik gvenlik uygulamaları ayrıntılı biimde incelenmiřtir.

İkinci blmde, Trkiye'deki kent gvenlik ynetim sistemlerine ynelik yapısal bir zmlenme yapılmıřtır. MOBESE ve KGYS sistemleri, teknik bileřenleri, tarihesi ve iřleyiř yapısıyla birlikte ele alınmıř; grntleme sistemleri, komuta-kontrol merkezleri, mobil uygulamalar ve veri ynetimi sreleri sistematik biimde deęerlendirilmiřtir. Ayrıca, bu gvenlik sistemlerinin dijitalleřme sreci ierisindeki rol, hukuki ve kurumsal baęlamda analiz edilmiřtir. KGYS ve MOBESE entegrasyonuna dair sreler tartıřılmıř; veri toplama, iřleme ve kullanma biimleri ile bu srelerin gvenlik politikalarına etkisi ortaya konmuřtur.

nc blmde ise, arařtırmanın yntemine ve sahadan elde edilen bulguların analizine yer verilmiřtir. Arařtırma kapsamında kullanılan nitel yntem, grřme teknięi, katılımcı profili ve veri analiz sreci detaylandırılmıřtır. MAXQDA yazılımı aracılıęıyla yrtlen ierik analizinde oluřturulan kod sistemi, tema yapıları ve rnek katılımcı ifadeleri zerinden bulgular sunulmuřtur. Polis memurları ile yapılan grřmeler sonucunda elde edilen veriler ıřıęında, KGYS'nin kent gvenlięi

üzerindeki etkileri, bireysel mahremiyet algısı, dijital sistemlerin operasyonel katkısı ve kamu güvenliği algısına dair gözlemler değerlendirilmiştir.

Ayrıca bu bölümde, Kütahya il merkezinde gerçekleştirilen ikili görüşmelere dayanan çalışmanın bulgularına yer verilmiştir. Katılımcıların dijital güvenlik sistemlerine ilişkin algıları, tutumları ve bu sistemlerin işlevselliğine dair deneyimleri, betimleyici bir yaklaşımla ele alınmış; anlamlandırma süreci, sözlü anlatılar üzerinden yapılandırılmıştır. Görüşme içeriklerinden elde edilen veriler, tematik bütünlük çerçevesinde çözümlenmiş ve öne çıkan eğilimler, ilgili literatürle karşılaştırmalı olarak değerlendirilmiştir.

Araştırmadan elde edilen bulgulardan hareketle ulaşılan genel çıkarımlar tartışmaya açılmış; uygulayıcı kurumlar ile akademik çevreler açısından yol gösterici olabilecek önerilere yer verilmiştir. Bununla birlikte, dijital güvenlik sistemleri bağlamında gelecekte yürütülebilecek araştırmalar için potansiyel çalışma alanları tanımlanmış ve bu teknolojilerin olası gelişim yönleri üzerine değerlendirmeler sunulmuştur.

Bu çerçevede, çalışmanın temel amacı, dijital dönüşümün kent güvenliği politikaları üzerindeki etkilerini KGYS odağında incelemektir. Bu amaç doğrultusunda, nitel araştırma yöntemiyle yürütülen saha çalışmasına dayalı olarak aşağıdaki araştırma sorularına yanıt aranmıştır:

1. KGYS sistemine dair polis memurlarının bilgi düzeyleri, deneyimleri ve bu sistemin işleyişine yönelik değerlendirmeleri nelerdir?
2. Dijitalleşmenin kent güvenliği üzerindeki etkileri, güvenlik aktörleri tarafından nasıl algılanmakta ve yorumlanmaktadır?
3. KGYS'nin dijital dönüşüm sürecindeki rolü ve operasyonel etkinliği nasıl değerlendirilmektedir?
4. Dijital güvenlik sistemlerinin bireysel mahremiyet, veri güvenliği ve toplumsal denetim üzerindeki etkileri nelerdir?
5. Toplumun KGYS sistemine yönelik farkındalık düzeyi, tutumu ve katılım potansiyeli ne düzeydedir?
6. KGYS'nin geleceğine dair beklentiler nelerdir ve yeni teknolojilerin (örneğin yapay zekâ, büyük veri) entegrasyonu nasıl değerlendirilmektedir?

Bu sorular, hem dijital güvenlik sistemlerinin teknik performansına hem de toplumsal kabul ve yönetsel etkinliğine dair bütüncül bir analiz yapabilmek amacıyla oluşturulmuştur. Ayrıca, çalışma kapsamında elde edilen bulgular, sadece güvenlik hizmetlerinin etkinliği değil, aynı zamanda birey-devlet ilişkileri, mahremiyet sınırları ve dijital gözetim kavramları etrafında da ele alınmıştır.



BÖLÜM I

DİJİTAL DÖNÜŞÜM VE KENT GÜVENLİĞİ: KAVRAMSAL ÇERÇEVE

Dijitalleşme, günümüzde yalnızca teknolojik bir gelişim değil, aynı zamanda toplumsal ve yönetsel dönüşümün temel bir aracı olarak değerlendirilmektedir. Bu kısımda; dijitalleşme ve dijital dönüşüm kavramları açıklanacak, kamu yönetimindeki uygulamaları incelenecek ve akıllı kent altyapılarının gelişimi ele alınacaktır. Ayrıca, dijital dönüşümün toplumsal yapılar ve kent güvenliği üzerindeki etkileri tartışılarak kavramsal çerçeve oluşturulacaktır.

1.1. Dijitalleşme ve Dijital Dönüşüm Süreci

Son yıllarda bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler, kamu yönetimi ve toplumsal yapılar dâhil olmak üzere pek çok alanda köklü değişimlerin yaşanmasına neden olmuştur. Bu değişim süreci içerisinde özellikle dijitalleşme ve dijital dönüşüm kavramları ön plana çıkmış; yönetim biçimlerinin, hizmet sunum modellerinin ve toplumsal ilişkilerin yeniden tanımlanmasına yol açmıştır. Bu bölümde, söz konusu kavramların kuramsal arka planı ele alınmakta; dijitalleşmenin kamu yönetimi üzerindeki etkileri değerlendirilmekte ve akıllı kent uygulamaları bağlamında dijital altyapıların dönüşüm sürecine katkısı incelenmektedir. Ayrıca, dijital dönüşümün güvenlik pratikleri ve toplumsal yapılar üzerindeki yansımalarına odaklanılarak, bu sürecin çok boyutlu etkilerine dair bütüncül bir çerçeve sunulmaktadır.

1.1.1. Dijital, Dijitalleşme ve Dijital Dönüşüm Kavramları

Bilgi toplumunun şekillenme sürecinde temel belirleyicilerden biri hâline gelen dijitalleşme, yüzeyde yalnızca teknolojik bir gelişim gibi algılansa da, özünde çok daha kapsamlı bir dönüşümü ifade etmektedir. Dijitalleşme süreci, sadece bilgi üretiminin teknik araçlarla gerçekleştirilmesini değil; aynı zamanda bilginin dolaşımı, paylaşımı ve yorumlanması gibi temel kültürel ve yönetsel pratikleri de doğrudan etkilemektedir. Bu bağlamda, dijitalleşmenin çok katmanlı doğasının kavranabilmesi için çoğu zaman birbirinin yerine kullanılan bazı kavramların açık bir biçimde ayrıştırılması önem arz etmektedir. Özellikle “dijital”, “dijitizasyon”, “dijitalleşme” ve

“dijital dönüşüm” kavramlarının kuramsal ayrımları yapılmadan, dijital çağın yönetsel ve toplumsal etkilerinin sağlıklı biçimde analiz edilmesi mümkün olamamaktadır (Teichert, 2019:49; Yıldız, 2020:112).

"Dijital" terimi, köken itibarıyla Latince “digitus” (parmak) kelimesinden türetilmiş olup, günümüzde sayısal verilere dayanan sistemlerin temelini oluşturan bir kavramsal çerçeve olarak kullanılmaktadır. Bu kavram aracılığıyla yalnızca sayısal temsile dayalı veri yapıları değil; aynı zamanda bu yapıların belirli algoritmalarla işlenmesi, dönüştürülmesi ve yeniden yapılandırılması süreci de ifade edilmektedir. Sayısal bilginin 0 ve 1 gibi ikili kodlar üzerinden iletiildiği bu yapı, dijital teknolojilerin işlem mantığını ve çağdaş bilgi sistemlerinin matematiksel temelini oluşturmaktadır (Ceritli, 2003:27; Tanrıverdi, 2021:293; Erdil, 2023: 94).

Dijital kavramının teknik altyapısı üzerinde yükselen ilk dönüşüm aşaması olarak değerlendirilen dijitalizasyon (digitization), analog formda bulunan verilerin dijital ortama aktarılması sürecine karşılık gelmektedir. Bu aktarım süreci; belge tarama, ses ya da görüntü dosyalarının dijital formata dönüştürülmesi gibi biçimsel işlemleri kapsamaktadır. Ancak bu tür bir dönüşüm, sadece veri formatının değişmesini sağlamakta; içeriğin yapısı, anlamı veya işlevi üzerinde doğrudan bir etki oluşturmamaktadır. Dolayısıyla dijitalizasyon, dijitalleşme sürecinin ön koşulu olmakla birlikte, kendi başına kurumsal ya da toplumsal bir dönüşüm üretmemektedir (Akmeşe, 2020:108).

Bu teknik düzeyin ötesine geçilerek, dijital araçların kamusal süreçlere entegre edilmesiyle birlikte dijitalleşme (digitalization) evresi ortaya çıkmaktadır. Dijitalleşme, kamu kurumlarının hizmet sunum modellerinde önemli değişimlere yol açmakta; bilgi işleme, iletişim kurma ve karar alma süreçlerinin dijital teknolojiler aracılığıyla gerçekleştirilmesini mümkün kılmaktadır. Bu aşamada kamu hizmetleri sadece fiziksel ortamlardan dijital platformlara taşınmakla kalmamakta; aynı zamanda işlem süreçlerinde hız, şeffaflık ve erişilebilirlik gibi nitelikler de ön plana çıkmaktadır (Aslan ve Bulut, 2019:55; Çelik, 2023:69). Örneğin e-devlet uygulamaları, dijitalleşmenin doğrudan bir çıktısı olarak, kamu-vatandaş ilişkisini yeniden tanımlamakta ve hizmet sunum biçimlerinde belirgin bir değişimi temsil etmektedir (Doğan ve Ustakara, 2013:109; Erdoğan, 2021:72).

Dijitalleşme ile birlikte gelen bu yapısal değişimin ötesinde, daha kapsamlı ve stratejik bir dönüşüm evresine işaret eden dijital dönüşüm (digital transformation) kavramı ise yalnızca teknolojinin değil; insanın, kurumun ve kültürel yapının birlikte dönüşümünü içeren bütünsel bir paradigma değişimini ifade etmektedir. Bu süreçte dijital teknolojiler, kurumsal yapının yeniden inşasında, yönetim stratejilerinin şekillendirilmesinde ve hizmet sunum modellerinin dönüştürülmesinde merkezi bir rol üstlenmektedir (Teichert, 2019:37). Dijital dönüşümün yalnızca operasyonel fayda sağlamayı hedeflemediği, aynı zamanda yeni bir yönetim zihniyeti ve kurumsal kültür inşa etmeyi amaçladığı belirtilmektedir. Bu nedenle dijital dönüşüm süreci, teknik kapasitenin ötesinde dijital okuryazarlık, etik farkındalık ve eleştirel düşünme gibi insani yetkinliklerin geliştirilmesini de zorunlu kılmaktadır (Şahin ve Korkmaz, 2021:59; Şeker, Gül ve Demirtaş, 2025:33).

Dönüşümün sürdürülebilir şekilde gerçekleştirilebilmesi için, teknik yatırımların yanında toplumsal kabul, kültürel uyum ve yönetsel esneklik gibi unsurların da gözetilmesi gerekmektedir. Aksi takdirde, yalnızca teknolojik altyapıların güncellenmesiyle sınırlı kalan uygulamaların, uzun vadede toplumsal direnç ve adaptasyon eksikliği gibi sorunlara neden olabileceği ifade edilmektedir (Uğurlu, 2010:33; Yıldız, 2022:113).

Reis ve Melão (2023) tarafından yapılan çalışmada, dijitalleşme süreci üç temel kavram çerçevesinde ele alınmıştır. İlk olarak, “dijitizasyon” kavramı; analog verilerin dijital formata dönüştürülmesi olarak tanımlanmış, ancak bu sürecin yalnızca biçimsel bir değişim sağladığı belirtilmiştir. “Dijitalleşme”, dijital teknolojilerin mevcut iş süreçlerine entegre edilmesiyle müşteri deneyiminin ve verimliliğin artırılmasını ifade etmektedir. “Dijital dönüşüm” ise, teknolojinin ötesinde, iş modelleri ve örgütsel yapıların da kapsamlı biçimde yeniden şekillendirilmesini içeren stratejik bir dönüşüm olarak tanımlanmıştır.

Sonuç olarak; dijitizasyon, dijitalleşme ve dijital dönüşüm kavramları birbirine bağlı olsa da, içeriksel olarak farklı düzlemlerde şekillenmektedir. Dijitizasyon, teknik veri aktarımıyla sınırlı kalırken; dijitalleşme, bu verilerin iş süreçlerine entegre edilmesini ve kamu hizmetlerinin dijital ortamda sunulmasını içermektedir. Dijital dönüşüm ise tüm bu sürecin ötesine geçerek, kamu yönetiminin temel işleyişini yeniden kurgulayan çok katmanlı bir dönüşüm süreci olarak değerlendirilmektedir

(Uysal, 2020:113). Bu kavramların doğru biçimde ayrıştırılması, dijital çağın dinamiklerinin kavranması ve etkili dijital yönetim uygulamalarının geliştirilmesi açısından kritik bir önem taşımaktadır.

1.1.2. Kamu Yönetiminde Dijitalleşme

Dijitalleşme, 21. yüzyılın en belirleyici dönüşüm süreçlerinden biri olarak, kamu yönetimi alanında da köklü değişimlere yol açmaktadır. Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, sadece bireylerin ve özel sektörün değil, aynı zamanda kamu kurumlarının da işleyişini yeniden şekillendirmektedir. Kamu yönetiminde dijitalleşme süreci, yalnızca teknik bir yenilenme değil; aynı zamanda yönetsel zihniyetin, vatandaş-devlet ilişkisinin ve hizmet sunum biçimlerinin dönüşümünü de ifade eder. Bu bağlamda, dijitalleşmenin kamu hizmetlerine entegrasyonu, verimlilik, şeffaflık ve katılımcılık gibi yönetim ilkeleriyle yeniden yorumlanmaktadır.

Kamu yönetiminde dijitalleşme sürecinin temelleri, modern devletin temel işlevlerini daha hızlı, daha etkin ve daha geniş kitlelere eşit biçimde ulaştırma gereksiniminden kaynaklanan yapısal bir ihtiyaç doğrultusunda atılmıştır. Bu bağlamda, dijitalleşmenin yalnızca teknolojik bir tercihten ibaret olmadığı; aynı zamanda kamu hizmetlerinin erişilebilirliğini artırmaya, işlem sürelerini kısaltmaya ve bürokratik yükleri azaltmaya yönelik zorunlu bir dönüşüm olarak şekillendiği görülmektedir. Özellikle 1990'lı yıllardan itibaren, Türkiye'nin de dâhil olduğu çok sayıda ülke, kamu hizmetlerini daha erişilebilir kılmak amacıyla e-devlet uygulamalarını hayata geçirmiştir (Şeker, Gül ve Demirtaş, 2025: 24). Bu ilk aşamada, her kamu kurumunun kendi dijital altyapısını bağımsız biçimde oluşturduğu bir yapı gözlemlenmiş; ancak zamanla bu dağınık sistemlerin bir arada işlemesini sağlayacak bütünleşik çözümlere duyulan ihtiyaç belirginleşmiştir. Söz konusu gelişmeler, yalnızca kurumsal düzeyde teknik bir organizasyon gerektirmemiş; aynı zamanda kamu hizmetlerine yönelik toplumsal taleplerin, özellikle hız, şeffaflık ve erişim konularında artış göstermesiyle birlikte dijitalleşme sürecinin kaçınılmaz olarak hız kazanmasına yol açmıştır. Geleneksel bürokratik modellerin bu yeni beklentileri

karşılama yetersiz kalması, kamu yönetiminin dijital dönüşüme yönelmesini yalnızca stratejik değil, aynı zamanda işlevsel bir zorunluluk hâline getirmiştir.

Kamu yönetiminde dijitalleşmenin, yalnızca teknolojik gelişmelere yanıt vermek amacıyla değil, aynı zamanda kriz dönemlerinde kamu hizmetlerinin sürekliliğini sağlamak için zorunlu hâle geldiği ifade edilmiştir. Dijital kamu hizmetlerinin geliştirilmesiyle birlikte, yönetim kapasitesinin artırılması gerekliliği vurgulanmış; bu süreçte hem yenilikçi fırsatlar hem de yönetsel belirsizliklerin ortaya çıktığı belirtilmiştir (Uslu, 2023:18).

Dijitalleşmenin kamu yönetimi üzerindeki etkisi, yalnızca dışa dönük hizmet sunumuyla sınırlı kalmayıp; aynı zamanda kamu kurumlarının içsel işleyiş yapısında da köklü bir dönüşümü beraberinde getirmektedir. Kurum içi organizasyon süreçlerinde dijital teknolojilerin benimsenmesiyle birlikte, özellikle belge yönetimi, insan kaynakları planlaması, performans izleme ve stratejik raporlama gibi işlevsel alanlarda ciddi bir etkinlik ve hız kazanımı sağlanmaktadır. Geleneksel kâğıt temelli uygulamaların yerini dijital dokümantasyon sistemlerine bırakması, bilgiye erişim süresini azaltmakta; karar alma mekanizmalarının daha hızlı ve nesnel veriye dayalı biçimde çalışmasına olanak tanımaktadır. Bu durum, yönetsel kararların daha şeffaf, ölçülebilir ve denetlenebilir bir zemine oturtulmasına katkı sunmaktadır. Aynı zamanda dijital altyapılar aracılığıyla geliştirilen otomasyon sistemleri sayesinde, kamu çalışanlarının günlük operasyonel yükü hafifletilmekte ve analitik düşünme, stratejik planlama gibi yüksek beceri gerektiren işlemlere odaklanmaları teşvik edilmektedir (Erdil, 2023:94). Bu bağlamda dijitalleşme, kamu yönetimi pratiklerini yalnızca teknik olarak değil; aynı zamanda yönetsel kültür ve kurumsal refleksler açısından da dönüştüren çok katmanlı bir gelişim süreci olarak değerlendirilmelidir.

Türkiye örneği, dijitalleşmenin kamu yönetimi açısından yalnızca teknolojik bir yenilik değil, aynı zamanda doğrudan bir devlet politikası hâline getirildiğini açık biçimde ortaya koymaktadır. Özellikle 2000'li yılların başında başlatılan e-Devlet Kapısı projesi, dijital dönüşüm sürecinin kurumsal ve bütüncül bir yaklaşımla ele alındığının ilk somut göstergesi olarak değerlendirilmiştir. Bu proje aracılığıyla, kamu hizmetlerinin farklı kurumlardaki dağıtık yapıları tek bir dijital platformda toplanarak hem vatandaşlara yönelik hizmet sunumunun kalitesi artırılmış hem de bu hizmetlerin daha hızlı, şeffaf ve izlenebilir bir biçimde sunulması sağlanmıştır. Ayrıca,

vatandaşların kamu süreçlerine erişiminin kolaylaştırılması sayesinde yönetim anlayışında da belirgin bir dönüşüm yaşanmış; kamu yönetimi üzerindeki sivil denetim kapasitesi güçlenmiştir. 2018 yılında gerçekleştirilen anayasa değişikliği sonrasında Cumhurbaşkanlığı Hükümet Sistemi'ne geçilmesiyle birlikte, dijital dönüşüm süreci daha merkezi ve eşgüdümlü bir yapıya kavuşturulmuş; bu kapsamda Dijital Dönüşüm Ofisi'nin kurulmasıyla tüm kamu kurumlarının dijitalleşme süreçleri tek elden koordine edilmeye başlanmıştır. Böylece, dijitalleşme yalnızca teknik bir modernleşme süreci olarak değil; aynı zamanda kamu yönetiminin stratejik yönetim kapasitesini artıran bir paradigma olarak içselleştirilmiştir (Şeker, Gül ve Demirtaş, 2025:42). Bu kapsamda kurulan Dijital Dönüşüm Ofisi, kamu kurumlarının dijitalleşme süreçlerini planlamakta ve koordine etmektedir. Bu durum, dijitalleşmenin kurumsal düzeyde içselleştirildiğini ve yalnızca bir araç değil, stratejik bir yönetim paradigması olarak benimsendiğini göstermektedir.

Her ne kadar dijitalleşme süreci kamu yönetiminde önemli fırsatlar sunmakta ve hizmet sunumunun etkinliğini artırma yönünde güçlü potansiyeller barındırmakta olsa da, bu süreç aynı zamanda çeşitli yapısal ve toplumsal zorlukları da beraberinde getirmektedir. Özellikle dijital kamu hizmetlerinin toplumsal kesimler arasında eşit ve adil biçimde sunulabilmesi noktasında karşılaşılan engeller, bu dönüşümün kapsayıcılığını sınırlayan temel faktörler arasında yer almaktadır. Bu bağlamda, veri güvenliği konusunda yaşanan belirsizlikler ve siber tehditlerin artan yoğunluğu, kamu hizmetlerinin güvenilirliği açısından ciddi riskler oluşturmakta; bireylerin kişisel bilgilerini paylaşma konusundaki çekinceleri artırmaktadır. Aynı şekilde, dijital okuryazarlık düzeyindeki eşitsizlikler, birçok bireyin dijital hizmetlere etkin biçimde erişmesini engellemekte; bu durum özellikle yaşlı nüfus, kırsal bölgelerde yaşayanlar ve düşük gelirli gruplar açısından önemli bir dezavantaj yaratmaktadır. Teknolojik altyapının bölgesel düzeyde homojen dağılmaması, bağlantı kalitesi ve donanım yetersizlikleri gibi teknik problemler de dijitalleşmenin eşitlikçi potansiyelini zayıflatmaktadır. Tüm bu unsurlar bir arada değerlendirildiğinde, dijital uçurumun hâlen önemli bir sorun olarak varlığını sürdürdüğü ve bu uçurumun giderilmemesi hâlinde dijitalleşmenin getirdiği avantajların yalnızca belirli kesimlerle sınırlı kalabileceği görülmektedir (Doğan ve Ustakara, 2013:109). Bu noktada kamu

yönetimi, yalnızca teknoloji yatırımlarıyla değil; aynı zamanda kapsayıcı, etik ve sürdürülebilir politikalarla dijitalleşmeyi desteklemek durumundadır.

Kamu yönetiminde dijitalleşme, sadece teknolojik bir geçişi değil, aynı zamanda yönetsel bir paradigma değişimini ifade etmektedir. Türkiye örneği, dijitalleşmenin planlı ve merkezi bir biçimde kamu yönetimine entegre edilebileceğini göstermektedir. Ancak bu sürecin başarılı olabilmesi için teknolojik altyapının yanı sıra kurumsal kapasite, vatandaş odaklılık ve sosyal kapsayıcılık gibi unsurların da gözetilmesi gerekmektedir. Dijitalleşme, doğru politikalarla desteklendiğinde yalnızca kamu hizmetlerinin etkinliğini artırmakla kalmaz, aynı zamanda demokratik katılımı ve şeffaflığı güçlendiren bir araç haline gelir. Bu nedenle dijitalleşme, modern kamu yönetiminin vazgeçilmez bir unsuru olarak ele alınmalıdır.

1.1.3. Akıllı Kentler ve Dijital Altyapılar

21. yüzyılın kentleri, giderek artan nüfus yoğunluğu, çevresel bozulma, sınırlı doğal kaynakların daha verimli kullanılması gerekliliği ve giderek karmaşıklaşan yönetim yapıları karşısında, geleneksel şehircilik anlayışlarının ötesine geçilerek yeni ve sürdürülebilir çözüm yolları geliştirmek zorunda kalmıştır. Bu zorunluluk, yalnızca fiziksel altyapının modernizasyonunu değil; aynı zamanda kent yaşamının bütünsel olarak yeniden kurgulanmasını gerekli kılmıştır. Bu bağlamda “akıllı kentler” kavramı, yalnızca teknolojik araçların kentsel mekâna entegre edilmesini değil; aynı zamanda kamu yönetiminin dijitalleşmesiyle birlikte verimlilik, sürdürülebilirlik, toplumsal katılım ve yaşam kalitesi gibi çok boyutlu hedefleri içeren bir yönetim yaklaşımını temsil etmektedir. Akıllı kent vizyonu, fiziksel, dijital ve sosyal altyapıların birbirine entegre edildiği, karar alma süreçlerinin veriye dayalı olarak yürütüldüğü ve yurttaşların bu süreçlere aktif biçimde katılabildiği bir kentsel düzenin inşasını öngörmektedir. Bu nedenle akıllı kentler, yalnızca teknolojik gelişmelerin mekâna yansıtılmasıyla sınırlı olmayan; çevresel duyarlılığı, yönetim kalitesini, enerji verimliliğini ve toplumsal kapsayıcılığı bütüncül biçimde önceleyen bir dönüşüm modeli olarak değerlendirilmelidir (Yıldız, 2022:114). Bu kapsamda dijital altyapılar, hem teknik hem de yönetsel olarak bu dönüşümün temelini oluşturmaktadır.

Akıllı kentler, dijital teknolojilerin sunduğu olanakların kent yaşamına entegre edilmesi yoluyla kamu hizmetlerinin daha erişilebilir, çevresel açıdan daha duyarlı ve uzun vadede sürdürülebilir bir biçimde sunulmasını hedefleyen yenilikçi bir kentleşme modelidir. Bu bağlamda, büyük veri analitiği, nesnelerin interneti (IoT), yapay zekâ uygulamaları, sensör temelli izleme sistemleri ve bulut tabanlı bilişim altyapıları gibi ileri düzey dijital çözümlerden etkin biçimde yararlanılmaktadır. Söz konusu teknolojiler sayesinde, kent içi ulaşım, enerji yönetimi, atık kontrolü, güvenlik hizmetleri ve acil durum müdahale sistemleri gibi alanlarda gerçek zamanlı veri toplanabilmekte; bu veriler doğrultusunda daha hızlı, doğru ve ihtiyaç temelli karar alma süreçleri geliştirilebilmektedir. Böylece hem kamusal kaynakların daha verimli kullanılması hem de kent sakinlerinin yaşam kalitesinin artırılması mümkün hâle gelmektedir. Bu teknolojik dönüşüm aynı zamanda kamu yönetimi açısından da yeni bir yönetim anlayışının habercisi olmakta; hizmetlerin vatandaş odaklı, dinamik ve etkileşimli bir yapıda sunulmasını teşvik etmektedir (Özdemir, 2022:153-158). Bu teknolojiler, kentsel hareketliliği, enerji yönetimini, atık kontrolünü ve güvenlik sistemlerini gerçek zamanlı izleyebilir ve yönlendirebilir hâle getirmiştir.

Dijital altyapılar, akıllı kentlerin bütünsel yapısının en temel teknolojik zeminini oluşturarak, kentsel yaşamın farklı boyutlarında yenilikçi hizmetlerin geliştirilebilmesine olanak tanımaktadır. Bu bağlamda geliştirilen sistemler, yalnızca teknik birer çözüm olarak değil; aynı zamanda kent yönetiminde katılımı, şeffaflığı ve etkileşimi artıran araçlar olarak işlev görmektedir. Özellikle akıllı ulaşım sistemleri, kent içi trafik akışının optimize edilmesini ve ulaşım kaynaklarının daha verimli kullanılmasını sağlamakta; bu sayede hem çevresel etkiler azaltılmakta hem de yaşam kalitesi yükseltilmektedir. Uzaktan sayaç okuma uygulamaları, su ve enerji tüketiminin daha hassas biçimde izlenebilmesine olanak sunarken; çevre sensörleri hava kirliliği, gürültü ve ısı gibi çevresel değişkenlerin gerçek zamanlı takibini mümkün kılmaktadır. Buna ek olarak, bütünleşmiş güvenlik sistemleri sayesinde kentteki güvenlik açıkları proaktif biçimde tespit edilmekte; dijital belediyecilik hizmetleri aracılığıyla da vatandaşlara daha hızlı, daha erişilebilir ve kullanıcı dostu hizmet kanalları sunulmaktadır. Tüm bu dijital bileşenlerin ortak etkisiyle birlikte, kent yönetiminin yalnızca veri temelli değil; aynı zamanda vatandaş merkezli, esnek ve sürdürülebilir bir yapıya kavuşması mümkün hâle gelmektedir (Yıldız, 2020: 27-29).

Bu dönüşüm, geleneksel yönetim modellerinden katılımcı, şeffaf ve etkileşimli bir kentsel yönetime geçişi zorunlu kılmıştır.

Akıllı kent uygulamalarında dijital altyapıların kullanımı, yalnızca teknik verimliliği artıran çözümler üretmekle sınırlı kalmamakta; aynı zamanda toplumsal yapılar üzerindeki etkileriyle birlikte değerlendirilmesi gereken çok boyutlu bir dönüşümü temsil etmektedir. Bu bağlamda, dijitalleşmenin kent mekânında mevcut olan eşitsizlikleri daha da derinleştirme riski taşıdığı ve özellikle kırılgan topluluklar açısından dışlayıcı sonuçlar doğurabileceği ifade edilmiştir. Bu nedenle dijital sistemlerin yönetim süreçlerine entegrasyonunda; yerel bağlamın özgün dinamikleri, toplumsal ihtiyaçların çeşitliliği ve dezavantajlı grupların korunmasına yönelik duyarlılıklar gözetilmeli, teknolojik ilerleme ile toplumsal adalet arasında dengeli bir yaklaşım benimsenmelidir (Hayta, 2021:935–936, 941).

Türkiye özelinde değerlendirildiğinde, dijital kentleşme politikalarının kurumsal bir çerçeveye oturtulması amacıyla hazırlanan Akıllı Şehirler Stratejisi ve Eylem Planı (2020–2023), yerel yönetimlerin dijital dönüşüm süreçlerine yönelik ilgisini artırmış ve belediyeleri daha bütüncül adımlar atmaya teşvik etmiştir. Bu stratejik belge doğrultusunda, birçok belediyede dijital altyapı yatırımlarına öncelik verilmiş; ulaşım, enerji, çevre, afet yönetimi ve şehir güvenliği gibi alanlarda veri temelli çözümler geliştirilerek uygulamaya konulmuştur. Özellikle büyükşehir belediyeleri başta olmak üzere, çeşitli yerel yönetimler hem kurumsal kapasitelerini dijital çağın gereklerine göre yeniden yapılandırmış hem de kent sakinlerinin ihtiyaç ve beklentilerine daha hızlı ve etkin yanıt verebilecek dijital hizmet modellerini geliştirme yoluna gitmiştir. Böylece, kentsel sorunların daha akılcı, çevreci ve sürdürülebilir yöntemlerle ele alınması mümkün hâle gelmiş; aynı zamanda kent yönetiminde şeffaflık ve katılımcılık ilkeleri daha görünür bir biçimde öne çıkmıştır (T.C. Çevre ve Şehircilik Bakanlığı, 2019). Ancak bu süreçte altyapı eşitsizliği, bütçe kısıtları ve kurumsal koordinasyon eksikliği gibi yapısal zorluklarla da karşılaşmıştır.

Diğer yandan, akıllı kent uygulamalarında merkeze yerleştirilen veri odaklı yönetim yaklaşımının, yalnızca teknik verimlilik sağlamakla sınırlı kalmayıp; aynı zamanda etik sorumluluklar ile hukuki yükümlülükler bağlamında da çeşitli tartışmalara yol açtığı görülmektedir. Özellikle bireylerin gündelik yaşamlarına dair verilerin dijital sistemler aracılığıyla sürekli olarak izlenebilir hâle gelmesi,

mahremiyetin korunmasına yönelik kaygıların artmasına neden olmuş; bu durum, kişisel verilerin toplanması, depolanması ve işlenmesi süreçlerinin şeffaflık ilkesi çerçevesinde değerlendirilmesini zorunlu kılmıştır. Bahsi geçen gelişmeler doğrultusunda yalnızca teknik güvenlik önlemlerinin artırılması değil; aynı zamanda etik ilkelerin yönetim süreçlerine bütüncül ve sistematik biçimde entegre edilmesi gerekliliği ortaya çıkmıştır. Dijital sistemlerin bireylerin özel hayatına müdahale potansiyeli taşıması, bireysel özgürlüklerin korunması açısından kritik bir eşik oluşturmuş; bu bağlamda siber güvenlik politikalarının güçlendirilmesi ve hukuki düzenlemelerin dijital dönüşüm sürecine eş zamanlı şekilde güncellenmesi gerektiği vurgulanmıştır. Dijital altyapının yaygınlaşmasıyla birlikte kamu otoritelerinden yalnızca hizmet üretmeleri değil; aynı zamanda temel hak ve özgürlükleri koruyacak bir yönetim anlayışını kurumsallaştırmaları beklenmektedir (Hayta, 2021:931-935). Akıllı kameralar, plaka tanıma sistemleri ve yüz tanıma gibi güvenlik uygulamaları hem kamu güvenliğine katkı sağlamakta hem de sürekli gözetim ve denetim tartışmalarını alevlendirmektedir.

Bununla birlikte, dijital teknolojilerin kentsel yönetime entegrasyonu sürecinde ortaya çıkan dijital eşitsizlik, akıllı kent uygulamalarının karşı karşıya olduğu en kritik yapısal sorunlardan biri olarak öne çıkmaktadır. Akıllı kentlerin sunduğu hizmetlere erişimin büyük ölçüde dijital araçlar ve çevrim içi platformlar üzerinden sağlanması, bu hizmetlerin toplumsal kesimlere eşit derecede ulaşmasını zorlaştırabilmektedir. Özellikle gelir düzeyi düşük bireyler, yaşlı nüfus, engelli bireyler ve dijital okuryazarlık düzeyi sınırlı olan gruplar, bu dönüşümden faydalanma açısından önemli dezavantajlarla karşı karşıya kalmakta; bu durum, dijital dışlanma riskini artırmaktadır. Teknolojik olanakların fiziksel olarak sunulması kadar, bu olanaklardan yararlanma kapasitesinin de toplumsal olarak dengeli biçimde geliştirilmesi gerektiği açıktır. Aksi takdirde, akıllı kent vizyonu toplumsal bütünleşmeyi güçlendirmek yerine, mevcut eşitsizlikleri daha da derinleştirebilecek bir yapı hâline dönüşme potansiyeli taşımaktadır. Bu nedenle, akıllı kent politikalarının sadece teknik altyapı yatırımlarına değil; aynı zamanda kapsayıcı ve adil dijital erişim stratejilerine de öncelik vermesi zorunluluk hâline gelmiştir (Yıldız, 2020:115). Dolayısıyla dijital altyapı yatırımlarında sadece teknolojik değil; sosyal kapsayıcılık, adalet ve eşitlik ilkeleri de gözetilmelidir.

Akıllı kentler ve dijital altyapılar, yalnızca teknolojik birer yenilik değil; aynı zamanda toplumsal ve yönetsel bir dönüşüm projesidir. Akıllı kent uygulamaları, kentlerin yaşam kalitesini artırmakla birlikte, daha hesap verebilir, verimli ve vatandaş odaklı yönetim anlayışlarını da teşvik etmektedir. Ancak bu dönüşümün sağlıklı ilerlemesi için teknik altyapının yanı sıra yasal düzenlemelerin, sosyal politikaların ve kurumsal kapasitelerin de güçlendirilmesi gerekmektedir. Türkiye'nin bu alandaki deneyimi, hem potansiyel fırsatları hem de zorlukları açık biçimde ortaya koymaktadır. Akıllı kent vizyonunun başarılı olabilmesi için dijital altyapı yatırımları kadar, insan merkezli bir dönüşüm anlayışı da esas alınmalıdır.

1.1.4. Dijital Dönüşümün Toplum ve Güvenlik Üzerindeki Etkileri

Dijital dönüşümün kamu yönetimi üzerindeki etkisi, yalnızca teknik altyapının geliştirilmesiyle sınırlı kalmayıp; aynı zamanda toplumsal düzeyde devletle birey arasındaki ilişkinin doğrudan biçimlenmesinde de belirleyici rol oynamaktadır. Özellikle kamu hizmetlerinin dijital kanallar aracılığıyla sunulmaya başlanması, vatandaşların bu hizmetlere mekânsal ve zamansal sınırlamalardan bağımsız biçimde ulaşabilmesini mümkün kılmakta; bu durum, kamu hizmetlerine erişimin niceliksel olarak genişlemesini sağlarken, hizmet sunumunun etkinliğini de gözle görülür biçimde artırmaktadır. Erişimin kolaylaşmasıyla birlikte, vatandaşların kamu kurumlarına yönelik memnuniyet düzeyinde artış gözlenmekte; bu durum, toplumsal güven duygusunu pekiştiren bir faktör olarak değerlendirilmektedir. Aynı zamanda dijital platformlar üzerinden sağlanan kolay geri bildirim ve etkileşim imkânları, vatandaşların yönetsel süreçlere daha aktif şekilde katılımını teşvik etmekte; böylece demokratik katılımın dijitalleşmeyle birlikte yeni bir boyut kazandığı görülmektedir (Çelik, 2023:70-71). Ancak tüm bu olumlu gelişmelere karşın, dijital dönüşümün toplumun tüm kesimleri için aynı düzeyde erişilebilir ve işlevsel olmayabileceği de dikkatle göz önünde bulundurulmalıdır. Gelir düzeyi, yaş grubu, eğitim seviyesi ve yaşanılan coğrafi bölge gibi faktörlere bağlı olarak ortaya çıkan dijital eşitsizlik, kamu hizmetlerinden dışlanma riski taşıyan grupların sistemin dışında kalmasına yol açabilmektedir. Bu durum, dijitalleşmenin kapsayıcılık ilkesini zedeleyerek sosyal

bütünleşme açısından yeni kırılmalar yaratma potansiyeline sahiptir (Özen ve Gürel, 2020:16-18).

Dijital dönüşümün toplum üzerindeki etkilerinin yalnızca teknolojik kolaylıklarla sınırlı kalmadığı; aynı zamanda bireysel mahremiyet, veri güvenliği ve kullanıcı davranışları üzerinde yeni tehdit alanları oluşturduğu ifade edilmiştir. Bu bağlamda, güvenlik risklerinin teknik önlemlerin ötesinde sosyo-kültürel farkındalık ve insan odaklı güvenlik yaklaşımlarıyla ele alınması gerektiği vurgulanmıştır (Ismailova vd., 2022: 393 – 394).

Dijitalleşmenin kamu yönetiminde yarattığı en dikkat çekici toplumsal etkilerden biri, şeffaflık ve hesap verebilirlik ilkelerinin kurumsal düzeyde daha güçlü biçimde hayata geçirilebilmesine olanak tanınmasıdır. Kamu hizmetlerinin dijital platformlar üzerinden sunulması, yalnızca vatandaşlara hızlı ve kolay erişim imkânı sağlamakla kalmamakta; aynı zamanda kamu yönetiminin karar alma süreçlerinin daha açık ve izlenebilir bir yapıya kavuşmasına da zemin hazırlamaktadır. Bu durum, yönetim anlayışının geleneksel hiyerarşik modelden daha katılımcı, etkileşimli ve denetlenebilir bir yapıya doğru evrilmesini mümkün kılmaktadır. Özellikle e-hizmet uygulamaları ile kamu verilerinin erişime açık hâle getirildiği açık veri politikaları, vatandaşların yalnızca bilgiye ulaşmasını değil; aynı zamanda yönetsel süreçlere doğrudan müdahil olmasını da teşvik etmekte, böylece kamu yönetiminde demokratik meşruiyetin yeniden tanımlanmasına katkı sunmaktadır (Bimay ve Kaypak, 2019:24-25). Ancak söz konusu dijital gelişmeler, beraberinde çeşitli risk alanlarını da gündeme taşımaktadır. Özellikle kişisel verilerin dijital ortamda depolanması, işlenmesi ve paylaşılması sürecinde ortaya çıkan güvenlik açıkları; hem bireysel mahremiyetin ihlal edilme riskini artırmakta hem de kamu kurumlarının siber saldırılara karşı yeterli direnç gösterip gösteremeyeceğine dair kaygıları beslemektedir. Bu bağlamda, dijital dönüşümün yalnızca teknik altyapı eksenli değil; aynı zamanda güvenlik, etik ve hukuki çerçeveleri içeren çok katmanlı bir stratejiyle ele alınması gerekliliği ortaya çıkmaktadır (Akmeşe, 2020:109).

Veri güvenliği çerçevesinde değerlendirildiğinde, kamu kurumlarının çeşitli dijital platformlar aracılığıyla topladığı büyük veri setleri; özellikle sağlık, eğitim, sosyal yardımlar ve nüfus hareketliliği gibi toplumun doğrudan refahını etkileyen alanlarda stratejik karar alma süreçlerinin temelini oluşturmaktadır. Bu veriler, kamu

politikalarının daha bütüncül, hedef odaklı ve veriye dayalı biçimde şekillendirilmesine imkân tanıdığı için, dijital kamu yönetiminin en değerli kaynakları arasında yer almaktadır. Ancak söz konusu verilerin dijital ortamlarda saklanması ve işlenmesi sürecinde oluşabilecek güvenlik açıkları, yalnızca teknik aksaklıklarla sınırlı kalmayıp; aynı zamanda vatandaşların kişisel bilgilerinin kötü niyetli kullanımlara maruz kalması gibi ciddi sonuçlara da yol açabilmektedir. Bu tür ihlaller, kamu kurumlarına duyulan güvenin zedelenmesine ve dijitalleşme sürecine karşı toplumsal direnç gelişmesine neden olabilmektedir. Bu nedenle, dijital güvenliğin sağlanmasında yalnızca teknik çözümler ve siber savunma sistemleri değil; aynı zamanda etik sorumluluklar ve güncel yasal düzenlemeler de sürecin ayrılmaz bileşenleri olarak ele alınmalıdır. Özellikle kişisel verilerin toplanmasında, işlenmesinde ve paylaşımında şeffaflık, hesap verebilirlik ve toplumsal fayda ilkelerinin gözetilmesi, veri temelli yönetişimin sürdürülebilirliğini sağlamak açısından büyük önem taşımaktadır (Gürbüz, 2019:34-41).

Toplumsal düzeyde dijitalleşmenin yol açtığı en dikkat çekici risklerden biri, bireylerin mahremiyet alanının giderek daralması ve dijital mahremiyetin ciddi biçimde erozyona uğrama tehlikesidir. Kamu yönetiminde yapay zekâ, büyük veri analitiği ve makine öğrenmesi gibi ileri dijital teknolojilerin kullanımı, karar alma süreçlerinin daha veriye dayalı, hızlı ve öngörülebilir hâle gelmesini sağlamaktadır. Ancak bu teknolojilerin denetimden uzak biçimde ya da şeffaflık ilkesine aykırı olarak kullanılması, bireylerin kişisel yaşamlarına yönelik görünmez ve çoğu zaman fark edilemeyen müdahaleleri de beraberinde getirebilmektedir. Özellikle bireylerin farkında olmadan geride bıraktığı dijital izlerin çeşitli algoritmalar tarafından analiz edilmesi yoluyla davranışlarının tahmin edilmesi ve buna bağlı olarak yönlendirilmeleri, mahremiyetin yalnızca korunması gereken bir alan olmaktan çıkarılıp, yönetilmesi gereken bir veriye dönüştürülmesine neden olmaktadır. Bu durum, kamu hizmetlerinde etkinlik sağlama hedefiyle çelişebilecek ölçüde bireysel özgürlüklerin sınırlandırılması riskini doğurmaktadır. Dolayısıyla dijital kamu yönetiminde teknoloji kullanımının yalnızca teknik yeterlilikle değil; aynı zamanda etik denetim mekanizmaları ve hukuki çerçevelerle desteklenmesi, birey haklarının korunabilmesi açısından zorunlu bir ön koşul hâline gelmiştir (Tanrıverdi, 2021:295).

Özellikle kişisel verilerin izinsiz işlenmesi ya da ticari amaçlarla üçüncü taraflarla paylaşılması, dijital güvenliğin ötesinde bir etik ihlal anlamına gelir.

Dijital dönüşüm, kamu hizmetlerinde etkinlik ve verimliliği artırma potansiyelinin yanı sıra, toplumla devlet arasındaki ilişkileri yeniden tanımlayan dinamik bir süreçtir. Bu süreç, topluma daha erişilebilir, katılımcı ve şeffaf kamu hizmetleri sunma imkânı sağlamakta; aynı zamanda veri güvenliği, mahremiyet ve dijital eşitsizlik gibi sorunları da beraberinde getirmektedir. Dijital dönüşümün toplum ve güvenlik üzerindeki etkilerinin yönetilebilmesi için, teknolojik yatırımlar kadar etik, hukuki ve yönetişimsel yaklaşımların da eş zamanlı olarak geliştirilmesi gerekmektedir. Böylece kamu hizmetlerinde dijital dönüşüm, sadece teknik bir yenilik değil; toplumsal güvenin ve adaletin yeniden inşası için stratejik bir araç haline gelebilecektir.

1.2. Kent Güvenliği ve Suç Kavramı Üzerine Kuramsal Yaklaşımlar

Kent güvenliği, yalnızca fiziksel tehditlere karşı alınan önlemlerle sınırlı kalmamakta; aynı zamanda suç olgusuyla doğrudan ilişkili toplumsal ve yönetsel dinamikleri de kapsamaktadır. Suçun kent mekânında ortaya çıkışı, yayılımı ve denetimi bağlamında geliştirilen kuramsal yaklaşımlar, modern güvenlik stratejilerinin şekillenmesinde belirleyici bir rol oynamaktadır. Bu bölümde, kent güvenliği ve suç ilişkisi kavramsal temelleriyle ele alınarak, güvenliğe dair çağdaş yaklaşımlar kuramsal bir çerçevede değerlendirilecektir.

1.2.1. Kent Güvenliğinin Tanımı, Kapsamı ve Tarihsel Gelişimi

Kentler, tarihsel süreç boyunca yalnızca insanların barınma ihtiyacına yanıt veren fiziksel yerleşim alanları olarak değil; aynı zamanda toplumsal, ekonomik, siyasal ve kültürel dinamiklerin şekillendiği, etkileşim içinde evrilen çok katmanlı yapılar olarak varlık göstermiştir. Bu çok boyutlu yapının süreklilik arz eden ve kent yaşamının her döneminde öncelikli konulardan biri olarak öne çıkan ihtiyacı ise güvenlik olgusu olmuştur. İnsanların ortak yaşam alanlarını paylaşmaya başlamasıyla birlikte, güvenliğin yalnızca bireysel değil, kolektif bir ihtiyaç olduğu gerçeği ortaya çıkmış; böylece güvenlik, kentlerin fiziksel planlamasından sosyal örgütlenmesine kadar birçok alanda belirleyici bir rol üstlenmiştir. Ne var ki, güvenlik kavramı da kent

gibi sabit ve evrensel bir tanıma sahip olmaktan uzak olup; dönemsel ihtiyaçlara, siyasal önceliklere ve toplumsal beklentilere bağlı olarak değişen, bağlamsal bir anlam kazanmıştır. Bu değişkenlik, güvenliğin yalnızca suç ve şiddetle mücadele perspektifinden değil; aynı zamanda bireylerin temel haklarını güvence altına alan, yaşam kalitesini artıran ve kentteki refah seviyesini yükseltmeyi amaçlayan bütüncül bir çerçevede ele alınmasını gerekli kılmaktadır. Bu bağlamda kent güvenliği, fiziksel müdahale yöntemleriyle sınırlı olmayan; sosyal bütünleşme, kamusal alanların kapsayıcılığı, risklerin önceden öngörülebilirliği ve bireylerin huzur içinde yaşama hakkının teminat altına alınması gibi birçok boyutu içeren geniş bir kavramsal zemine oturmaktadır (Kaypak, 2016:35; Alacadağlı, 2020:155).

Kent güvenliğinin tanımlanışı, hem disiplinler arası akademik yaklaşımlar hem de tarihsel bağlamlar itibarıyla değişkenlik göstermektedir. Güvenlik kavramı, yalnızca suçla mücadele ve kamu düzeninin sağlanmasına indirgenmiş bir biçimde değil; aynı zamanda bireyin gündelik yaşamında karşılaştığı fiziksel, sosyal ve psikolojik tehditleri içerecek biçimde yeniden düşünülmektedir. Geleneksel yaklaşımlar, genellikle güvenliği devletin kolluk kuvvetleri eliyle sağlanan bir hizmet olarak değerlendirmiştir. Bu çerçevede, kent güvenliği daha çok kriminal olayların önlenmesi ve kamu asayişinin korunmasıyla ilişkilendirilmiştir. Ancak çağdaş yönetim paradigmasında, güvenlik yalnızca fiziksel tehlikelerin bertaraf edilmesiyle sınırlı bir olgu olmaktan çıkarak; bireylerin mekânsal, duygusal ve sosyal ihtiyaçlarını gözeten bütüncül bir sistem olarak ele alınmaktadır. Bu dönüşüm, güvenliğin sadece devlet merkezli bir kamu hizmeti değil; aynı zamanda katılımcı, çok aktörlü ve çok katmanlı bir yönetim alanı olduğunu ortaya koymaktadır (Hayta, 2021:929–931, 940–941). Bu yeni yaklaşım, kent güvenliğini yalnızca müdahaleye dayalı değil, aynı zamanda önleyici, kapsayıcı ve bütüncül politikalarla yapılandırılması gereken bir alan olarak görmektedir. Söz konusu çerçevede kent güvenliği, fiziksel mekânların güvenli biçimde düzenlenmesinden altyapı hizmetlerinin eşgüdümüne, dijital gözetim teknolojilerinin etik kullanımından sosyal kapsayıcılığı önceleyen kent politikalarının geliştirilmesine kadar geniş bir yönetim alanını kapsamaktadır. Böylece kent güvenliği, yalnızca bir güvenlik meselesi değil; aynı zamanda sosyal adalet, eşitlik ve kamusal yaşamın kalitesine doğrudan etki eden stratejik bir yönetim başlığı hâline gelmektedir (Bülbul, 2019:62; Uysal, 2020:115).

Kent güvenliği olgusu, kentlerin tarihsel gelişimiyle eşzamanlı biçimde evrilmiş; bu evrim süreci boyunca her tarihsel dönem, kendi özgül toplumsal, siyasi ve mekânsal bağlamına uygun güvenlik biçimleri üretmiştir. İlk kentleşme örneklerinin görüldüğü Antik çağlarda, kent yalnızca bir yerleşim alanı değil, aynı zamanda siyasi bir organizasyon biçimi olarak kabul edilmiş; bu çerçevede güvenlik, büyük ölçüde kentin çevresine inşa edilen surlar, gözetleme kuleleri ve askeri savunma sistemleri aracılığıyla sağlanmıştır. Güvenliğin fiziksel mekânla bu denli iç içe geçmiş biçimde tasarlandığı bu dönemde, kentin sınırlarının belirginleştirilmesi, dış tehditlere karşı hem somut bir koruma hem de topluluk bilincini pekiştiren simgesel bir yapı işlevi görmüştür. Roma dönemine gelindiğinde ise güvenlik olgusu, daha karmaşık ve sistematik bir yapıya bürünmüş; kentin fiziksel planlamasında güvenli yaşam koşullarını sağlayacak altyapı düzenlemeleri ön plana çıkmıştır. Bu dönemde taş döşeli yolların yapılması, kanalizasyon sistemlerinin kurulması ve kamusal alanların işlevsel olarak yeniden düzenlenmesi gibi pratikler, yalnızca konforu değil, aynı zamanda sağlık temelli güvenliği de gözeten bir yönetsel bilinçle hayata geçirilmiştir (Uğurlu, 2010:35).

Orta Çağ'a gelindiğinde ise güvenlik kavramı, dinsel sembollerle donatılmış kent yapıları içerisinde, daha çok dış tehditlere karşı fiziksel savunmayı temel alan bir kolektif sorumluluk biçiminde ortaya çıkmıştır. Bu dönemin kentlerinde, surlar ve tahkimat yapıları yalnızca askeri birer bariyer değil; aynı zamanda kent kimliğini şekillendiren ve güvenlik duygusunu pekiştiren toplumsal mekanizmalardı. Kent sakinlerinin bu savunma sistemlerinin inşasında ve bakımında doğrudan görev alması, güvenliğin merkezi otoritenin tek başına yüklenebileceği bir sorumluluk olmaktan çıkarak, kolektif bir yükümlülük alanına dönüştüğünü göstermektedir. Öte yandan, dönemin ticari faaliyetlerinin artmasıyla birlikte, güvenlik algısı yalnızca askeri tehditlerle sınırlı kalmamış; ekonomik yaşamın sürekliliğini garanti altına almak da kent güvenliği politikalarının asli bir bileşeni hâline gelmiştir. Özellikle pazar yerlerinin korunması, ticaret yollarının güvence altına alınması ve mal-hizmet alışverişinin denetlenebilir kılınması, dönemin güvenlik öncelikleri arasında yer almıştır (Pustu, 2006:142; Chambliss, 1996:249).

Sanayi Devrimi ile birlikte yalnızca üretim biçimleri ve ekonomik yapılar değil, kentlerin fiziksel yapısı ve bu yapılar içerisinde güvenliğe ilişkin anlayışlar da

köklü bir biçimde dönüşüme uğramıştır. Bu dönemde ortaya çıkan yoğun kentleşme dalgası, nüfusun hızla kent merkezlerine yönelmesine neden olmuş; iş gücünün belirli sanayi bölgelerinde yoğunlaşması, kent içi mekânsal sıkışmayı beraberinde getirmiştir. Bu yeni kentsel yapı, özellikle alt sınıf mahallelerinde yaşam koşullarının kötüleşmesine ve buna bağlı olarak sosyal sorunların derinleşmesine zemin hazırlamıştır. Kentlerde giderek artan yoksulluk, düzensiz göç ve işsizlik gibi faktörler, suç oranlarının yükselmesine doğrudan etki etmiş; böylece güvenlik, sanayi kentlerinin gündeminde öncelikli bir yer edinmiştir. Bu bağlamda, güvenliğin sağlanmasına yönelik olarak modern polis örgütlerinin kurumsallaşması hız kazanmış; ceza adalet sistemlerinde yapısal reformlara gidilmiş ve güvenlik teknolojilerinin kullanılmaya başlanmasıyla birlikte kent güvenliği daha sistematik ve merkezileşmiş bir çerçeveye oturtulmuştur (Aksoy, 2007:11).

Kent güvenliği, tarihsel olarak doğal afetlere yönelik müdahale yaklaşımlarıyla sınırlı bir çerçevede ele alınmış; ancak zamanla, kamu sağlığı krizleri, teknolojik kazalar ve sosyal güvenlik tehditlerini de içeren daha geniş bir kapsam kazandığı belirtilmiştir. Bu evrimsel süreçte, güvenliğin yalnızca fiziksel koruma değil, aynı zamanda sistemin değişken koşullara karşı dayanıklılık gösterme ve kendini yenileyebilme kapasitesiyle ilişkili olduğu vurgulanmıştır (Huang vd., 2023:35).

Özellikle sanayi bölgelerine yakın, altyapıdan yoksun ve yoğun nüfuslu işçi mahallelerinde artan asayiş sorunları, kent yönetimlerinin güvenlik önceliklerini yeniden gözden geçirmesini zorunlu kılmıştır. Bu süreçte, yalnızca fiziksel önlemler değil; aynı zamanda sosyal düzenin sağlanmasına dönük politikalar da gündeme gelmiş, güvenlik olgusu kent planlamasının ayrılmaz bir unsuru hâline getirilmiştir. Böylece Sanayi Devrimi, modern kent güvenliği anlayışının temellerinin atıldığı bir dönem olarak, güvenliğin hem mekânsal hem de kurumsal boyutlarda yeniden tanımlandığı bir kırılma noktası olarak değerlendirilmiştir (Ayhan ve Çubukçu, 2007:35).

20. yüzyılın ikinci yarısında güvenlik olgusu, ağırlıklı olarak devletlerin askeri tehditlere karşı korunması ekseninde ele alınmış; ulusal güvenlik anlayışı, dış tehditlere karşı caydırıcılık ve savunma stratejileri üzerinden tanımlanmıştır. Bu dönemde, güvenlik politikalarının odağında daha çok sınırların korunması, orduların güçlendirilmesi ve devlet merkezli tehdit algılarının yönetilmesi yer almıştır. Ancak

Soğuk Savaş'ın sona ermesiyle birlikte bu dar çerçeveli güvenlik yaklaşımının yetersizliği ortaya çıkmış ve kavram giderek daha geniş ve çok boyutlu bir anlam kazanmaya başlamıştır. 1990'lı yıllardan itibaren özellikle uluslararası alanda insani güvenlik paradigması yaygınlık kazanmış; güvenliğin yalnızca devletlerin varlığına yönelik değil, bireylerin gündelik yaşamlarını doğrudan etkileyen tehditlere karşı da sağlanması gerektiği kabul edilmiştir. Bu yeni yaklaşım çerçevesinde güvenlik, askeri tehditlerin ötesine geçerek sosyal, ekonomik, çevresel ve teknolojik boyutları kapsayan bütüncül bir anlayışa dayandırılmıştır. Böylece, bireylerin yalnızca savaş ve şiddetten değil; aynı zamanda yoksulluk, işsizlik, doğal afetler, çevresel yıkım, salgın hastalıklar ve dijital çağın getirdiği siber tehditler gibi çok çeşitli risklere karşı korunması gerektiği vurgulanmıştır. İnsani güvenlik perspektifi, bireyi güvenlik politikalarının pasif bir öznesi olmaktan çıkararak, doğrudan korunması gereken temel aktör konumuna taşımış; bu yönüyle devlet merkezli geleneksel güvenlik anlayışından radikal bir kopuşu temsil etmiştir (Erdem, 2016:255; Redo, 2008:12).

Kent güvenliği kavrayışında yaşanan dönüşüm, yalnızca suç ve asayişe ilişkin klasik önlemlerle sınırlı kalmamış; çevresel kirlilik, ulaşım ağlarındaki yetersizlikler, doğal afet riskleri, dijital eşitsizlikler ve veri güvenliği gibi çok boyutlu sorunları da içine alacak biçimde genişlemiştir. Böylece güvenlik, kentlerin yalnızca fiziksel korunmasına yönelik bir olgu olmaktan çıkarak, aynı zamanda yaşam kalitesini, sürdürülebilirliği ve toplumsal bütünlüğü doğrudan etkileyen bir alan hâline gelmiştir (Ceritli, 2003:32; Öner ve Çam, 2022:1170). Özellikle 21. yüzyıla gelindiğinde bilgi ve iletişim teknolojilerinde gerçekleşen hızlı ilerlemeler, kent güvenliğinin yeniden tanımlanmasına yol açmış ve “akıllı güvenlik” yaklaşımı öne çıkmaya başlamıştır.

Bu yeni yaklaşımda, güvenlik hizmetleri yalnızca insan gücü ve geleneksel yöntemlerle değil, dijital altyapılar aracılığıyla da sağlanmakta; akıllı kameralar, sensör tabanlı ağlar, büyük veri sistemleri ve yapay zekâ destekli analiz araçları, kent yönetimlerinin güvenlik politikalarının merkezine yerleştirilmektedir. Söz konusu teknolojiler aracılığıyla suçların gerçekleşmeden önce öngörülmesi, riskli bölgelerin belirlenmesi ve olası tehditlere daha hızlı müdahale edilmesi mümkün hâle gelmektedir. Ayrıca bu dijital çözümler, yalnızca suç önleme kapasitesini artırmakla kalmayıp, güvenlik birimlerinin kaynaklarını daha verimli kullanmasına da imkân tanımaktadır (Aslan ve Bulut, 2019:57; Anagnostopoulos vd., 2006:378).

Günümüzde kent güvenliği anlayışı, yalnızca bireylerin fiziksel güvenliğini sağlamaya yönelik klasik önlemlerle sınırlı kalmamakta; aynı zamanda dijital güvenliğin korunması, kişisel mahremiyetin gözetilmesi ve giderek artan siber tehditlere karşı direnç geliştirilmesi gibi çok boyutlu unsurları da kapsamaktadır. Bu çerçevede, güvenlik olgusu yalnızca suç ve şiddetin önlenmesiyle değil, aynı zamanda bireylerin dijital yaşam alanlarında korunmasıyla da ilişkilendirilmektedir. Özellikle bilgi ve iletişim teknolojilerinin yoğun biçimde gündelik yaşamın bir parçası hâline gelmesi, kent güvenliğini hem fiziksel hem de dijital düzlemde yeniden düşünmeyi zorunlu kılmıştır.

Bu bağlamda Türkiye’de de uygulamaya konulan KGYS, MOBESE kameraları ve plaka tanıma sistemleri gibi bütünleşmiş güvenlik altyapıları, şehirlerde güvenliğin sağlanmasında kritik araçlar olarak kullanılmaktadır. Söz konusu teknolojiler aracılığıyla hem trafik denetiminin hem de asayişin daha etkin bir biçimde yürütülmesi mümkün olmakta; suçların önlenmesi, olayların daha hızlı tespit edilmesi ve kamu düzeninin korunması yönünde önemli kazanımlar elde edilmektedir. Ayrıca bu sistemler, yalnızca anlık müdahaleyi kolaylaştırmakla kalmayıp, aynı zamanda uzun vadede kentlerin daha kapsayıcı, sürdürülebilir ve güvenli bir yapıya kavuşmasına katkı sunmaktadır (Karaağaçlı, 2022:740; Bahar, 2013:198).

Kent güvenliği, günümüzde yalnızca suç oranlarının azaltılmasına indirgenen dar bir hedef olmaktan çıkmış; bireylerin yaşam kalitesinin yükseltilmesi, toplumsal bütünleşmenin desteklenmesi ve kentlerin çeşitli tehditlere karşı daha dirençli hâle getirilmesi gibi çok boyutlu amaçları kapsayan bir yönetim süreci olarak değerlendirilmektedir. Bu çerçevede güvenlik, yalnızca bireylerin fiziksel varlıklarının korunması değil, aynı zamanda sosyal adaletin güçlendirilmesi, kentsel alanların daha kapsayıcı hâle getirilmesi ve dayanıklı toplulukların inşa edilmesi ile ilişkilendirilmektedir. Böylelikle güvenlik, yalnızca kolluk kuvvetlerinin müdahalesine dayalı bir olgu olmaktan çıkarak, kent planlaması, sosyal politikalar, çevresel sürdürülebilirlik ve dijital güvenlik uygulamalarıyla bütünleşmiş çok katmanlı bir süreç hâline gelmiştir.

Kent güvenliğinin tarihsel gelişim süreci ise bu dönüşümün kavranabilmesi açısından kritik bir işlev görmektedir. Tarihsel perspektif, yalnızca geçmişteki güvenlik uygulamalarının anlaşılmasına katkı sunmamakta; aynı zamanda günümüz

kentlerinin karşı karşıya kaldığı sorunların kökenlerinin anlaşılmasına ve gelecekte uygulanabilecek politikaların temellendirilmesine de ışık tutmaktadır. Dolayısıyla güvenlik, hem geçmişin bir yansıması hem de geleceğin kentsel stratejilerini şekillendiren temel bir referans noktası olarak görülmektedir (Shaw, 2001:141; Gündüzöz, 2016:328).

1.2.2. Kentsel Suç Kavramı ve Suç Türleri

Kentsel yaşamın sosyolojik dokusu içerisinde suç olgusu, yalnızca bireysel eğilimlerin ya da anlık sapmaların ürünü değil; çok boyutlu toplumsal, ekonomik ve mekânsal dinamiklerin kesişiminde şekillenen karmaşık bir sorunsal olarak değerlendirilmektedir. Kentleşme süreci, nüfus yoğunluğunun artışı ve mekânsal genişleme ile sınırlı bir dönüşüm olmayıp, aynı zamanda sosyal örgütlenmelerin biçimlenmesini, ekonomik yapının yeniden düzenlenmesini, kültürel etkileşimlerin çeşitlenmesini ve politik ilişkilerin farklılaşmasını beraberinde getirmektedir. Bu çok katmanlı değişim süreci, modern kentlerde yalnızca mevcut suç türlerinin yeniden şekillenmesine yol açmakla kalmamış, aynı zamanda kentsel mekânın özgün koşullarıyla bağlantılı yeni suç biçimlerinin ortaya çıkmasına da zemin hazırlamıştır. Dolayısıyla suç, kent bağlamında yalnızca bireysel davranışlar üzerinden değil; mekânsal düzenlemeler, sosyal ilişkiler ve toplumsal eşitsizlikler üzerinden kavramsallaştırılması gereken çok boyutlu bir olgu niteliği taşımaktadır (Yüceyılmaz, 2007:89).

Kentsel suç, kent yaşamı içerisinde bireylerin birbirleriyle ve içinde buldukları mekânla kurdukları sosyal, ekonomik ve kültürel ilişkiler çerçevesinde ortaya çıkan, yasa dışı, sapkın ve çoğu zaman kentsel düzenin istikrarını tehdit eden eylemler bütünü olarak tanımlanmaktadır (Aksoy, 2007:13). Bu tür suçların ortaya çıkışı, yalnızca bireysel eğilimlere indirgenemeyip; kentlerin yoğun nüfus yapısı, heterojen toplumsal bileşimleri, ekonomik eşitsizlikleri, göç süreçleri, işsizlik ve yoksulluk gibi çok yönlü değişkenlerin etkileşimi sonucu şekillenmektedir (Ceritli, 2003:35). Kentin anonimleşen ve parçalı yapısı, toplumsal dayanışmayı sağlayan sosyal bağların zayıflamasına yol açmakta; bu durum ise bireylerin toplumsal

denetimden uzaklaşarak suça yönelimlerini artıran önemli bir faktör olarak değerlendirilmektedir (Demirbaş, 2005:45).

Kentsel suç, yalnızca bireylerin güvenliğini değil, aynı zamanda kentsel yaşamın genel istikrarını tehdit eden çok boyutlu bir olgu olarak tanımlanmıştır. Özellikle mülkiyet suçları, kentsel alanlarda en sık karşılaşılan suç türü olurken; uyuşturucu bağlantılı olayların da önemli bir orana ulaştığı belirtilmiştir. Bu suçların yoğunlaştığı alanların tespitiyle, “hotspot”¹ kavramı öne çıkarken; suçun mekânsal dağılımının rastlantısal olmadığı, belirli bölgelerde kalıcı biçimde yoğunlaştığı vurgulanmıştır. Ayrıca suç türlerinin modellenmesinde, bireylerin günlük rutinleri, sosyo-ekonomik durumları ve güvenlik güçlerinin varlığı gibi değişkenlerin belirleyici rol oynadığı ifade edilmiştir (Palma-Borda vd., 2025:110547).

Kentsel suçun en dikkat çekici yönlerinden biri, mekânsal bağlamla birlikte değerlendirilmesinin zorunluluğudur. Suçun işlendiği alanın fiziksel özellikleri, erişilebilirlik düzeyi, denetlenebilirliği ve kullanım biçimleri, suçun ortaya çıkışında doğrudan belirleyici olabilmektedir. Bu nedenle kentsel suç, yalnızca bireysel eğilimler ya da sosyoekonomik göstergeler üzerinden açıklanamaz; aynı zamanda mekânsal örgütlenme biçimlerinin ve kentsel düzenlemelerin ayrıntılı bir biçimde incelenmesini de gerekli kılmaktadır (Othman vd., 2020: 271-272).

Kentsel suçlar, sosyolojik bir perspektiften değerlendirildiğinde, genellikle dört temel kategori altında sınıflandırılmaktadır: mülkiyet suçları, şiddet suçları, kamu düzenini ihlal eden suçlar ve kent mekânına yönelik suçlar. Mülkiyet suçları kapsamında; hırsızlık, yankesicilik ve gasp gibi bireylerin mal varlıklarını hedef alan eylemlerin yer aldığı belirtilmektedir. Şiddet suçlarının ise cinayet, cinsel saldırı ve yaralama gibi bireylerin doğrudan yaşam güvenliğini tehdit eden fiilleri içerdiği ifade edilmektedir (Ackerman,1998:377). Kamu düzenini ihlal eden suçlar, hem toplumsal gösteriler sırasında meydana gelen yasa dışı eylemleri hem de trafik düzenine yönelik ihlalleri kapsayan geniş bir alanı barındırmaktadır. Kent mekânına yönelik suçların ise; vandalizm, izinsiz yapılaşma ve çevresel tahribat gibi, kentsel yaşam alanlarının

¹ *Hotspot*, kelime anlamıyla “sıcak nokta” olup, farklı disiplinlerde çeşitli anlamlarda kullanılmaktadır. Genel olarak, belirli bir olayın, etkinliğin veya yoğunluğun diğer alanlara göre daha yüksek olduğu coğrafi ya da kavramsal bölgeyi ifade eder. Örneğin, biyolojide yüksek tür çeşitliliğine sahip çevreyle ilgili bölgeleri; jeolojide volkanik faaliyetlerin yoğun olduğu alanları; coğrafya veya turizmde ise ziyaretçi yoğunluğunun arttığı bölgeleri tanımlamak için kullanılmaktadır.

fiziksel ve sosyal yapısını bozmaya yönelik davranışlar şeklinde ortaya çıktığı aktarılmaktadır (Ayhan ve Çubukçu, 2007:37).

Kentsel alanlarda suç türlerinin yoğun bir biçimde ortaya çıkması, radikal kriminoloji kuramının temel varsayımlarından biri olan, suçun toplumsal yapıdaki eşitsizliklerin doğrudan bir sonucu olduğu yönündeki görüşle örtüşmektedir. Bu yaklaşıma göre suç, bireysel tercihler ya da yalnızca ahlaki zafiyetlerle değil; ekonomik, sosyal ve politik yapının ürettiği yapısal dengesizliklerle ilişkilendirilmektedir. Özellikle kapitalist sistemin kentsel mekânları belirli sınıfsal konumlara göre örgütlemesi, kentin belli bölgelerinde yoğun yoksulluk, işsizlik ve sosyal dışlanma gibi sorunların derinleşmesine yol açmakta; bu da suçun dezavantajlı gruplarda daha belirgin biçimde görülmesine neden olmaktadır. Böylece suç, sadece bireysel bir eylem olarak değil, kent mekânının sınıfsal temelde ayrıştırılmasının yarattığı yapısal bir sonuç olarak değerlendirilmekte ve bu durum radikal kriminolojinin kentsel suçlara yönelik eleştirel perspektifini doğrulamaktadır (Chambliss, 1996:250). Bu bağlamda, suç olgusu yalnızca bireysel eğilimlerin ya da kişisel tercihlerden doğan sapmaların sonucu olarak değil, aynı zamanda mekânsal olarak dışlanan ve toplumsal yaşamın merkezinden uzaklaştırılan grupların maruz kaldıkları yapısal baskıların bir yansıması olarak ele alınmaktadır. Bu durum, ekonomik, sosyal ve kültürel açıdan dezavantajlı konumda bulunan bireylerin, kentsel mekânlardaki eşitsiz örgütlenme biçimlerinin doğrudan bir ürünü olarak suç davranışına daha yatkın hale gelmesine neden olmaktadır. Dolayısıyla suçun anlaşılmasında bireysel faktörler kadar, toplumsal eşitsizliklerin ürettiği baskı mekanizmalarının da dikkate alınması gerekliliği ortaya çıkmaktadır (Matsueda, 2014:685).

Kentlerdeki suç oranlarının yüksekliğine ilişkin gerçekleştirilen deneysel araştırmalar, suç olgusunun yalnızca bireysel faktörlerle açıklanamayacağını; aynı zamanda sistemsal, ekonomik ve toplumsal nedenlerle yakından ilişkili olduğunu ortaya koymaktadır. Bu doğrultuda yapılan incelemelerde, suçun bireysel davranışların ötesine geçen bir boyuta sahip olduğu ve toplumsal yapının ürettiği eşitsizliklerden beslendiği görülmektedir. Nitekim Cahil ve Mulligan (2003), sosyal ve ekonomik farklılıkların kentlerdeki suç oranları üzerinde doğrudan belirleyici bir etkisinin bulunduğunu ortaya koymuş; gelir dağılımındaki adaletsizliklerin ve

sosyoekonomik farklılaşmaların suçun artışında kritik bir rol oynadığını saptamıştır. Benzer biçimde McClain (2001) tarafından yapılan çalışmalar, sosyal açıdan dezavantajlı bölgelerde suçun diğer kentsel alanlara kıyasla daha yoğun bir şekilde ortaya çıktığını göstermiştir. Bu bulgular, suçun yalnızca mekânsal düzlemdeki farklılıklardan değil, aynı zamanda yapısal eşitsizliklerin sürekliliğinden kaynaklandığını ve bu nedenle kentsel suçun çok boyutlu bir toplumsal sorun olarak değerlendirilmesi gerektiğini ortaya koymaktadır.

Kentsel suç kavramı, modern şehirlerin karmaşık yapısı içinde hem bireysel hem de yapısal faktörlerin etkileşimiyle ortaya çıkan bir olgu olarak ele alınmalıdır. Suçun mekânsal dağılımı, suç türlerinin çeşitliliği ve suç davranışlarının şekillenme biçimleri, kent yaşamının dinamikleriyle doğrudan ilişkilidir. Mülkiyet, şiddet ve kamu düzenine yönelik suçlar gibi çeşitli türlerde tezahür eden kentsel suçlar, aynı zamanda sosyoekonomik eşitsizliklerin, mekânsal ayrışmanın ve toplumsal dışlanmanın da birer yansımasıdır. Bu nedenle kentsel suç olgusunu analiz ederken, sadece bireysel sorumluluklar değil, toplumsal yapıdaki çatlaklar ve mekânsal düzenlemeler de dikkate alınmalıdır. Böylelikle kentsel suçun anlaşılması ve önlenmesine yönelik daha bütüncül bir yaklaşım geliştirilebilir.

1.2.3. Suç Önleme Stratejileri ve Güvenlik Yaklaşımları

Kentlerde artan suç oranları, yalnızca bireysel güvenlik tehdidi yaratmakla kalmamakta, aynı zamanda sosyal bütünlüğü, ekonomik kalkınmayı ve yaşam kalitesini de olumsuz yönde etkilemektedir. Bu nedenle suçun önlenmesi, sadece adli kurumların değil, yerel yönetimlerin de temel sorumluluk alanlarından biri haline gelmiştir. Modern güvenlik yaklaşımları, birey odaklı ve toplumsal katılımı esas alan stratejilerle şekillenmektedir. Bu kapsamda geliştirilen suç önleme stratejileri, hem teorik hem de uygulamaya dönük birçok ilkeyi ve yöntemi içermektedir.

Günümüzde suç önleme kavramı, yalnızca suç işlendikten sonra müdahale etmeyi ya da cezai yaptırımlar yoluyla sonuçları yönetmeyi hedefleyen geleneksel yaklaşımlardan ayrılarak, suçun ortaya çıkışını önceden engellemeyi amaçlayan bütüncül bir anlayış olarak ele alınmaktadır. Bu anlayışta, suçun yalnızca bireysel tercihlerin sonucu olmadığı; aynı zamanda sosyal, ekonomik ve çevresel koşulların bir

araya gelmesiyle şekillendiği kabul edilmektedir. Bu nedenle suçun önlenmesine yönelik stratejiler, sosyal politikaların güçlendirilmesinden çevresel düzenlemelere, kurumsal mekanizmaların geliştirilmesinden topluluk temelli girişimlere kadar geniş bir yelpazede çeşitlenmektedir. Birleşmiş Milletler tarafından yayımlanan “Suç Önleme Rehberi”nde de vurgulandığı üzere, etkili suç önleme politikalarının yalnızca kısa vadeli çözümlerle sınırlı kalmaması; sistematik, sürdürülebilir ve toplumsal bağlamı dikkate alan ilkeler üzerine inşa edilmesi gerekmektedir (Redo, 2008:14; UNODC, 2010). Bu bağlamda, suç önleme stratejilerinin sekiz temel ilkeye dayandırıldığı belirtilmektedir: hükümet liderliği, sosyo-ekonomik kalkınma, kurumlar arası iş birliği, sürdürülebilirlik, bilgiye dayalı planlama, insan haklarına saygı, karşılıklı bağımlılığın gözetilmesi ve toplumsal farklılıkların dikkate alınması. Bu ilkeler, suç önleme politikalarının yalnızca güvenlik kurumlarının sorumluluğu olmadığını; aynı zamanda devletin, yerel yönetimlerin, sivil toplum kuruluşlarının ve toplumun farklı kesimlerinin ortak katkısıyla uygulanması gereken çok boyutlu bir süreç olduğunu göstermektedir.

Sosyal gelişim temelli suç önleme yaklaşımı (*Crime Prevention through Social Development – CPSD*), bireyleri suça iten sosyal, ekonomik ve kültürel risk etmenlerinin azaltılmasını veya tamamen ortadan kaldırılmasını hedefleyen bir suçla mücadele stratejisi olarak değerlendirilmektedir. Bu yaklaşım, özellikle gençler, kadınlar ve aileler gibi kırılgan grupların güçlendirilmesini ve toplumsal yaşama daha güvenli biçimde bütünleşmiş edilmelerini amaçlamaktadır. Bu doğrultuda; eğitim olanaklarının yaygınlaştırılması, istihdam fırsatlarının artırılması ve sosyal hizmetlerin erişilebilirliğinin geliştirilmesi gibi mekanizmalar üzerinden bireylerin toplumsal uyumunun desteklendiği ifade edilmektedir. Böylelikle suç, yalnızca gerçekleşmesinin ardından cezai yaptırımlarla değil, aynı zamanda ortaya çıkmadan önce sosyal politikalara dayalı önleyici müdahalelerle engellenmeye çalışılmaktadır (*International Centre for the Prevention of Crime – ICPC*, 2015).

Suç önleme stratejilerinde, özellikle terör eylemlerinin engellenmesine yönelik olarak, durum odaklı yaklaşımların giderek daha fazla önem kazandığı belirtilmiştir. Fiziksel çevrenin tasarımı, gözetim olanaklarının artırılması ve hedef güçlendirme gibi önlemlerin, potansiyel faillerin karar alma süreçlerini doğrudan etkilediği vurgulanmıştır. Bu yaklaşımların, yalnızca saldırıların gerçekleşmesini zorlaştırmakla

kalmayıp, aynı zamanda saldırganlar açısından caydırıcılığı da artırdığı ifade edilmiştir (Marchment vd., 2025).

Çevresel tasarımla suç önleme (Crime prevention through environmental design-CPTED) yaklaşımı ise suçun ortaya çıkışını kolaylaştıran fiziksel mekân koşullarının yeniden düzenlenmesine odaklanmaktadır. Bu anlayışa göre kent mekânlarının planlanması ve tasarlanması, suç fırsatlarını azaltacak biçimde gerçekleştirildiğinde suç oranlarının düşürülmesi mümkün hâle gelmektedir. Örneğin, yeterli aydınlatma sistemlerinin kurulması, kamusal alanların görünürlüğünün artırılması, sokakların ve parkların düzenlenmesi, güvenli ulaşım noktalarının sağlanması ve kentsel alanlarda doğal gözetim imkânlarının geliştirilmesi bu stratejinin temel unsurları arasında yer almaktadır. Böylelikle çevresel düzenlemeler, bireylerin suçla karşılaşma riskini azaltırken aynı zamanda kentte güven duygusunun güçlenmesine de katkı sunmaktadır (CSIR, 2001).

Yerel düzeyde geliştirilen suç önleme stratejileri, “yerel sorunlara yerel çözümler” anlayışının bir yansıması olarak şekillendirilmekte ve kentlerin özgün sosyal, ekonomik ve kültürel koşullarına göre çeşitlilik göstermektedir. Bu yaklaşım çerçevesinde belediyelerin rolü, yalnızca hizmet sunumuna odaklanan idari birimler olmaktan çıkarılmakta; toplumun güvenliğini doğrudan sağlamakla yükümlü, önleyici politikaların merkezinde yer alan bir aktör olarak yeniden tanımlanmaktadır (Shaw, 2001:143). Yerel yönetimlerin bu bağlamda üstlenmesi gereken temel sorumluluklardan biri, kentsel suçların ortaya çıkış nedenlerini ayrıntılı biçimde analiz ederek, yerelin ihtiyaçlarına uygun, gerçekçi ve uygulanabilir çok paydaşlı eylem planları geliştirmektir.

Bu eylem planlarının etkin olabilmesi için yalnızca yerel yönetimlerin değil, aynı zamanda kamu kurumlarının, sivil toplum kuruluşlarının, güvenlik birimlerinin ve doğrudan mahalle halkının sürece katılımı gerekmektedir. Bu çok aktörlü yapı sayesinde, yerel sorunlara yönelik çözümler hem daha kapsayıcı hem de sürdürülebilir bir nitelik kazanmaktadır. Dolayısıyla suç önleme politikalarının başarısı, merkeziyetçi yaklaşımlardan ziyade, yerel düzeyde oluşturulan iş birliği mekanizmalarının işlerliğiyle yakından ilişkilidir (ICPC, 2016).

Toplum temelli güvenlik anlayışı, güvenliğin yalnızca devletin sunduğu bir hizmet değil, aynı zamanda bireylerin temel bir kamu hakkı olarak tanınmasını esas

alan bir yaklaşım olarak değerlendirilmektedir. Bu anlayışta, bireylerin günlük yaşamlarını suç korkusu duymadan sürdürebilmeleri, kent içindeki hareket özgürlüklerini kısıtlayacak herhangi bir tehditten uzak bir yaşam sürebilmeleri temel hedef olarak belirlenmektedir. Dolayısıyla toplum güvenliği, yalnızca fiziksel tehlikelerden korunmayı değil, aynı zamanda bireylerin sosyal yaşamda kendilerini güvende hissetmelerini sağlayacak koşulların oluşturulmasını da içermektedir. Bu çerçevede geliştirilen stratejiler, şiddetin sistematik biçimde azaltılmasını, kamu düzeninin korunmasını ve kentte yaşam kalitesinin yükseltilmesini sağlayacak önlemlerden oluşmaktadır. Söz konusu önlemler yalnızca güvenlik kurumlarının faaliyetleriyle sınırlı kalmamakta; yerel yönetimlerin, sivil toplum kuruluşlarının ve bireylerin aktif katılımıyla desteklenen çok katmanlı politikaları kapsamaktadır (UN-Habitat, 2007). Toplumsal güvenlik politikalarının en önemli yönlerinden biri, suç oranlarının azaltılmasına yönelik kısa vadeli çözümlerin ötesine geçerek, uzun vadede toplumsal bütünlük ve dayanışmanın güçlendirilmesine katkı sunmasıdır. Bu bağlamda, toplum temelli güvenlik anlayışı, yalnızca bireyleri korumaya odaklı değil; aynı zamanda kolektif refahın ve kent yaşamında barışçıl bir düzenin inşasına hizmet eden bütüncül bir yaklaşım olarak öne çıkmaktadır.

Bu stratejilerin etkili biçimde uygulanabilmesi ve uzun vadede sürdürülebilir sonuçlar üretebilmesi, iyi yönetim anlayışı ile doğrudan ilişkilendirilmelidir. İyi yönetim, yalnızca idari süreçlerin şeffaf yürütülmesi anlamına gelmemekte; aynı zamanda güvenlik politikalarının etkin, kapsayıcı ve toplum temelli bir yaklaşımla yönetilmesini de zorunlu kılmaktadır. İyi yönetim anlayışının; liderlik süreçlerinin etkinliği, kaynak yönetiminde verimlilik ve toplumsal katılımın kurumsallaştırılması gibi üç temel ilkeye dayandığı çeşitli kurumsal çerçevelerde vurgulanmaktadır (UN-Habitat, 2007). Etkin liderlik, güvenlik stratejilerinin yalnızca hazırlanmasını değil, aynı zamanda uygulanmasını ve izlenmesini mümkün kılmakta; verimli finansman, kaynakların adil ve dengeli biçimde kullanılmasını sağlamaktadır. Vatandaş katılımı ise toplumun yalnızca edilgen bir izleyici değil, güvenlik politikalarının oluşturulmasında ve uygulanmasında aktif bir paydaş olarak konumlandırılmasını öngörmektedir. Dolayısıyla iyi yönetim olmaksızın, suç önleme stratejilerinin kapsayıcı, şeffaf ve uzun vadeli sonuçlar üretmesi mümkün görünmemektedir (UN-

Habitat, 2007). Yerel yönetimlerin, suç önleme stratejilerini uygularken şeffaflık, hesap verebilirlik ve kapsayıcılık ilkelerini gözetmesi gerekmektedir.

Suç önleme stratejileri ve güvenlik yaklaşımları, geleneksel kolluk odaklı anlayışın ötesine geçerek, çok katmanlı ve katılımcı politikalarla yeniden tanımlanmaktadır. Sosyal, çevresel ve kurumsal düzeyde uygulanan bu stratejiler, yalnızca suç oranlarını düşürmekle kalmaz, aynı zamanda kent yaşamının kalitesini artırır. Yerel yönetimlerin bu süreçteki rolü, yalnızca destekleyici değil, aynı zamanda yönlendirici ve uygulayıcıdır. Etkili suç önleme, yerel düzeyde geliştirilen, bilgiye dayalı ve toplumsal ihtiyaçları gözeten bütüncül politikalarla mümkündür. Bu nedenle güvenlik ve suç önleme politikalarının, yerel yönetimlerin gündeminde öncelikli bir yer tutması kaçınılmazdır.

1.2.4. Kent Güvenliğinde Teknolojik Uygulamalar

Kent güvenliği, geleneksel kolluk hizmetlerinin ötesine geçerek, kent planlaması ve teknolojik altyapılarla bütünleşmiş biçimde ele alınan çok boyutlu bir olguya dönüşmüştür. Bu dönüşüm, teknolojik gelişmelerin kent yaşamının her alanına nüfuz etmesiyle birlikte hız kazanmış ve güvenliğin sağlanmasında dijital çözümler ön plana çıkmıştır. Özellikle nüfusun yoğunlaştığı metropollerde, suçun önlenmesi ve müdahale sürecinin etkinleştirilmesinde dijital teknolojiler belirleyici bir rol üstlenmektedir.

Kent güvenliğinde dijital teknolojilerin kullanımı, yalnızca teknik araçların gelişimi olarak değil, aynı zamanda kent yönetiminde köklü bir zihinsel ve yapısal dönüşüm süreci olarak değerlendirilmelidir. Bu bağlamda geliştirilen uygulamalar, dijitalizasyon, dijitalleşme ve dijital dönüşüm kavramları ekseninde çok katmanlı bir bakış açısıyla ele alınmakta ve her bir aşama güvenlik politikalarının farklı yönlerini şekillendirmektedir. İlk aşama olan dijitalizasyon süreci, analog verilerin dijital ortama aktarılması olarak tanımlanmakta; kent güvenliği bağlamında bu süreç, ses kayıtlarının, görüntülerin ve hareket verilerinin dijitalleştirilmesi aracılığıyla somutlaşmaktadır. Bu dönüşüm sayesinde, güvenlik alanında kapalı devre kamera sistemleri (CCTV), plaka tanıma sistemleri (LPR) ve vücut kameraları gibi teknolojilerin etkin biçimde kullanılabilmesi mümkün hâle gelmiştir. Böylece suçların

tespit edilmesi, olayların kayıt altına alınması ve gerektiğinde delil olarak kullanılacak verilerin toplanması çok daha sistematik bir biçimde gerçekleştirilmektedir. Ayrıca bu teknolojiler, yalnızca suçun işlenmesinden sonra kanıt elde edilmesine değil, aynı zamanda suçun önlenmesine yönelik caydırıcı bir unsur olarak da işlev görmektedir. Dolayısıyla dijitalizasyon süreci, kent güvenliğinin yalnızca teknik açıdan değil, aynı zamanda yönetsel karar alma ve stratejik planlama süreçleri açısından da yeni bir boyut kazanmasına katkı sunmaktadır (Bahar, 2013:199).

Kent güvenliğinde teknolojik uygulamaların kullanımı, geleneksel yöntemlerin ötesine geçerek, suç önleme stratejilerinde yapay zekâ ve bilgisayarla görme gibi ileri dijital çözümlerin entegrasyonunu gündeme getirmiştir. Özellikle akıllı şehir sistemlerinde, gözetim kameralarından elde edilen görüntülerin otomatik olarak analiz edilmesiyle potansiyel tehditlerin önceden tespit edilebildiği ve güvenlik birimlerinin müdahale süresinin önemli ölçüde azaltılabildiği ifade edilmiştir. Bu süreçte, yalnızca olay sonrası analiz değil; aynı zamanda gerçek zamanlı suç tahmini ve risk odaklı kaynak dağılımı da mümkün hâle gelmiştir. Ancak teknolojinin etkinliğinin, algoritmaların doğruluğu, veri kalitesi ve etik ilkelerle uyum gibi çok boyutlu unsurlara bağlı olduğu da vurgulanmıştır (Kim vd., 2023:3681)

Dijitalleşme, yalnızca dijital teknolojilerin kullanılmasıyla sınırlı kalmayıp, aynı zamanda bu teknolojilerin kurumsal işleyişin bütününe sistematik bir şekilde entegre edilmesini de kapsamaktadır. Bu entegrasyon süreci, teknolojinin basit bir araç olarak görülmesinden öte, kurumların karar alma, denetim ve operasyonel süreçlerinin doğrudan parçası hâline getirilmesini zorunlu kılmaktadır. Kent güvenliği bağlamında dijitalleşme, olaylara ilişkin verilerin yalnızca toplanmasını değil; aynı zamanda bu verilerin işlenmesini, analiz edilmesini ve gerektiğinde anlık müdahalelerin organize edilmesini mümkün kılan bütünlük sistemlerinin kurulmasını içermektedir. Bu tür sistemler sayesinde güvenlik birimleri, olaylara daha hızlı tepki verebilmekte ve kararlarını daha veriye dayalı biçimde şekillendirebilmektedir (Aslan ve Bulut, 2019:65).

Türkiye özelinde bakıldığında ise, dijitalleşme sürecinin en somut örneklerinden birini Emniyet Genel Müdürlüğü çatısı altında geliştirilen Kent Güvenlik Yönetim Sistemleri (KGYS) oluşturmaktadır. KGYS uygulamaları, kent içi

güvenliğin sağlanması amacıyla kamera sistemleri, plaka tanıma teknolojileri ve veri merkezleri aracılığıyla elde edilen bilgilerin merkezi bir sistem üzerinden izlenmesi ve değerlendirilmesi esasına dayanmaktadır. Bu sayede yalnızca suç sonrası soruşturmaların etkinliği artırılmamakta, aynı zamanda suçların önceden tespit edilmesi ve önlenmesine yönelik proaktif güvenlik stratejileri de geliştirilebilmektedir. Böylelikle dijitalleşme, kent güvenliğini hem operasyonel hem de stratejik düzeyde dönüştüren kritik bir unsur olarak öne çıkmaktadır (EGM, 2013).

Dijital dönüşüm, kent güvenliği bağlamında yalnızca mevcut teknolojilerin kullanılmasını değil; aynı zamanda bu teknolojiler temelinde yeni bir yönetim anlayışının geliştirilmesini ve içselleştirilmesini ifade etmektedir. Bu süreçte güvenlik, salt teknik altyapıların güçlendirilmesi ile sınırlı kalmamakta; dijital teknolojilerin sunduğu imkânlar aracılığıyla daha şeffaf, katılımcı ve veri temelli bir yönetim modelinin oluşturulması amaçlanmaktadır. Böylece kent güvenliği, klasik güvenlik hizmetlerinin ötesine geçerek, stratejik planlamadan kurumsal koordinasyona kadar pek çok alanı dönüştüren bir boyut kazanmıştır. Bu yaklaşım doğrultusunda T.C. Çevre ve Şehircilik Bakanlığı tarafından yayımlanan “2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı”nda kent güvenliği, akıllı çevre, ulaşım, afet yönetimi ve yönetim gibi temel başlıklarla birlikte bütünleşik biçimde ele alınmıştır (ÇŞB, 2019). Strateji belgesinde güvenlik, yalnızca kolluk kuvvetlerinin görev alanı içinde değerlendirilen dar bir kavram olmaktan çıkarılmış; veri temelli karar alma süreçleri, çok paydaşlı iş birliği mekanizmaları ve dijital altyapıların geliştirilmesi gibi geniş kapsamlı bir kamusal sorumluluk alanı olarak tanımlanmıştır. Bu tanım, güvenliğin yalnızca güvenlik birimlerinin müdahaleleriyle sağlanamayacağını; aynı zamanda merkezi yönetim, yerel yönetimler, özel sektör ve vatandaşların ortak katkısıyla sürdürülebilecek çok katmanlı bir süreç olduğunu vurgulamaktadır (Şahin ve Korkmaz, 2021:60).

Kent güvenliğinde kullanılan teknolojik uygulamalar, artık yalnızca görsel gözetim sistemleriyle sınırlı kalmayıp; çok katmanlı ve veri odaklı analiz süreçleriyle desteklenen gelişmiş bir yapıya evrilmektedir. Bu dönüşüm sayesinde güvenlik uygulamaları, salt denetim odaklı işlevlerinin ötesine geçerek; suçun oluşum nedenlerini analiz etme, suçun önlenmesine yönelik proaktif stratejiler geliştirme ve risk temelli müdahale modelleri oluşturma kapasitesine ulaşmaktadır. Özellikle coğrafi

bilgi sistemleri (CBS), suç yoğunluk haritaları, risk analizleri ve diğer mekânsal veri çözümleri, suç olaylarının kent mekânında dağılımını ayrıntılı şekilde ortaya koyarak; güvenlik politikalarının mekân temelli ve hedef odaklı biçimde tasarlanmasını mümkün kılmaktadır. Bu araçlar, kentsel güvenlik yönetiminin analitik boyutunu güçlendirerek, kamu güvenliğinin daha bütüncül ve etkili bir biçimde sağlanmasına katkı sunmaktadır (Hayta, 2021:933–934).

Bu teknolojiler aracılığıyla kentsel alanlarda çöküntü bölgelerinin belirlenmesi, suçun yoğun olarak görüldüğü bölgelerin önceden tespit edilmesi ve mevcut kaynakların daha dengeli ve verimli biçimde dağıtılması mümkün hâle gelmektedir. Ayrıca güvenlik güçlerinin kent içinde konumlandırılması, rastlantısal ya da tepkisel bir mantığa dayanmaktan çıkarılmakta; bunun yerine bilimsel analizlere dayalı proaktif güvenlik stratejileriyle planlanmaktadır. Böylece hem suçların önlenmesine hem de kamu güvenliğinin daha sürdürülebilir biçimde sağlanmasına yönelik somut adımlar atılabilmektedir (Tozkoparan, 2019:419; Akmeşe, 2020:110).

Bununla birlikte, kent güvenliği alanında dijital teknolojilerin entegrasyonu yalnızca operasyonel etkinliğin artırılmasıyla sınırlı bir gelişme olarak değerlendirilmemelidir; aynı zamanda etik, hukuki ve toplumsal boyutlarıyla da ele alınması gereken çok katmanlı bir süreç olarak görülmelidir. Dijitalleşmenin sağladığı gözetim kapasitesinin artışı, bir yandan suçların önlenmesi ve güvenliğin güçlendirilmesi açısından önemli fırsatlar yaratırken; diğer yandan bireylerin temel hak ve özgürlükleri üzerinde yeni tartışmaları gündeme taşımaktadır. Özellikle veri gizliliğinin korunması, dijital hakların gözetilmesi ve gözetim toplumuna dönüşüm riski, bu süreçte dikkate alınması gereken en hassas alanlar arasında yer almaktadır. Bu risklerin göz ardı edilmesi, kent güvenliği politikalarının kısa vadede başarıya ulaşmasına rağmen uzun vadede toplumsal güven kaybına yol açma potansiyeli taşımaktadır. Dolayısıyla dijital güvenlik uygulamalarının geliştirilmesinde yalnızca teknik altyapı ve operasyonel kapasite değil, aynı zamanda etik ilkeler, yasal düzenlemeler ve toplumsal katılım da eşit derecede önemsenmelidir. Bu yaklaşım, güvenliğin bireylerin hak ve özgürlükleri pahasına sağlanmasının önüne geçerek, hem güvenliği hem de demokratik değerleri koruyan dengeli bir yapı oluşturulmasını mümkün kılmaktadır (Ulubaş, 2023:67; Ün, 2022:415).

Sonuç olarak kent güvenliği alanında dijital teknolojilerin kullanımı, yalnızca teknik bir yenilik ya da mevcut araçların çeşitlendirilmesi şeklinde değerlendirilemez; bu gelişim aynı zamanda kent yönetiminin genel mantığında paradigmatik bir değişimin yaşandığını ortaya koymaktadır. Dijitalleşme ile birlikte güvenlik, klasik yöntemlerin ötesine geçerek daha veriye dayalı, daha öngörülebilir ve daha kapsayıcı bir yapıya bürünmektedir. Ancak bu dönüşümün kalıcı ve etkili olabilmesi, teknolojinin salt araçsal bir unsur olarak değil, insan odaklı bir yönetim anlayışının merkezinde konumlandırılmasıyla mümkündür. İnsan haklarını, toplumsal kapsayıcılığı ve etik ilkelere bağlılığı önceleyen bir yaklaşım benimsendiğinde, dijital teknolojilerin sunduğu olanaklar güvenlik politikalarının sürdürülebilirliğine önemli katkılar sağlayabilmektedir. Böyle bir anlayış, kentlerde yalnızca suç oranlarının azaltılmasına değil, aynı zamanda toplumun güven duygusunun pekiştirilmesine, kamusal yaşam kalitesinin artırılmasına ve kent yönetiminde demokratik katılımın güçlendirilmesine de hizmet etmektedir. Dolayısıyla dijitalleşmenin getirdiği dönüşüm, doğru yönetildiğinde, daha etkin, daha sürdürülebilir ve daha kapsayıcı kent güvenliği politikalarının inşa edilmesi için stratejik bir fırsat sunmaktadır.

1.2.5. Yerel Yönetimlerin Kent Güvenliğindeki Rolü

Kent güvenliği, günümüzde yalnızca geleneksel kolluk hizmetlerinin yürütülmesiyle sınırlandırılmamakta; kent planlaması, sosyal politikalar ve teknolojik altyapılarla bütünleşmiş biçimde ele alınan çok boyutlu bir olguya dönüşmüş durumdadır. Bu dönüşüm, teknolojik gelişmelerin kent yaşamının her alanına giderek daha güçlü biçimde nüfuz etmesiyle hız kazanmış; güvenliğin sağlanmasında dijital çözümler vazgeçilmez araçlar hâline gelmiştir. Artık güvenlik, yalnızca suçlara müdahale etmeyi değil, aynı zamanda suçların ortaya çıkmadan önce öngörülmesini, risk alanlarının belirlenmesini ve toplumsal güvenlik algısının güçlendirilmesini de içermektedir. Özellikle nüfusun yoğunlaştığı metropol alanlarında, geleneksel yöntemlerin yetersiz kaldığı durumlarda suçun önlenmesi, olayların hızlı biçimde tespit edilmesi ve müdahale süreçlerinin etkinleştirilmesi büyük ölçüde dijital teknolojiler aracılığıyla mümkün hâle gelmektedir. Kapalı devre kamera sistemlerinden plaka tanıma teknolojilerine, coğrafi bilgi sistemlerinden büyük

veri analizlerine kadar pek çok dijital uygulama, kent güvenliği politikalarının temel bileşenleri arasında yer almaktadır. Bu bağlamda dijital teknolojiler, yalnızca operasyonel bir destek unsuru olarak değil, aynı zamanda kentsel güvenliğin bütüncül biçimde yönetilmesini sağlayan stratejik araçlar olarak değerlendirilmektedir (Gündüzöz, 2016:330).

Günümüzde kent güvenliği, artık yalnızca merkezi otoritelerin tek başına sorumluluk üstlendiği bir mesele olarak görülmemekte; yerel yönetimlerin aktif katılımını ve doğrudan katkısını zorunlu kılan çok aktörlü bir yönetim alanı olarak değerlendirilmektedir. Özellikle dijital teknolojilerin kentsel mekâna entegrasyonu ile güvenliğin sağlanması, salt teknik kapasitenin ötesine geçmekte; yerel düzeyde politika üretimini, altyapı planlamasını ve toplumsal koordinasyonu aynı anda zorunlu kılan daha kapsamlı bir sürece dönüşmektedir (Ulubaş, 2023:69; Alacadağlı, 2020:156).

Kent güvenliğinin dijital boyut kazanmasıyla birlikte, yerel yönetimlerin rolü giderek daha karmaşık ve stratejik bir hâl almıştır. Özellikle siber güvenlik alanında, belediyelerin hem hizmet sağlayıcı hem de altyapı koruyucusu olarak ikili sorumluluğa sahip oldukları görülmektedir. Bununla birlikte, yeterli kaynak eksikliği, uzman personel yetersizliği ve mevzuatın güncel tehditleri karşılamada yetersiz kalması, yerel düzeyde güvenlik açıklarının artmasına neden olmaktadır. Kurumsal farkındalık ve üst düzey liderlik desteğinin olmaması, bu zayıflıkları daha da derinleştirmektedir. Bu bağlamda, yerel yönetimlerin yalnızca teknik değil, yönetsel kapasite açısından da güçlendirilmesi gerektiği vurgulanmaktadır (Hossain vd., 2025:15).

Yerel yönetimler, sahip oldukları mekânsal planlama yetkisi, kamu hizmeti sunma kapasitesi ve yurttaşlarla doğrudan iletişim kurabilme imkânı sayesinde kent güvenliğini etkileyen birçok unsur üzerinde belirleyici bir rol üstlenmektedir. Bu bağlamda yerel otoritelerin katkısı, yalnızca temel hizmetlerin sağlanmasıyla sınırlı kalmamakta; aynı zamanda kentsel alanların güvenliğinin artırılmasına yönelik somut politikaların geliştirilmesini de içermektedir. Özellikle kent mekânlarının etkin biçimde aydınlatılması, terk edilmiş alanların yeniden işlevlendirilmesi ve suçun yoğunlaştığı bölgelerde sosyal destek projelerinin hayata geçirilmesi, yerel

yönetimlerin önleyici güvenlik stratejilerinin önemli bileşenleri arasında değerlendirilmektedir (Kaypak, 2016:37; Gündüzöz, 2016:335).

Aynı zamanda yerel yönetimler, Kent Güvenlik Yönetim Sistemleri (KGYS) gibi teknolojik altyapıların uygulanabilirliğini artıran aktörler olarak öne çıkmakta; veri akışının sağlanması ve yerel ihtiyaçların analiz edilmesi noktasında merkezi otoriteyle yakın bir iş birliği içerisinde faaliyet göstermektedir. Böylece yerel düzeyde geliştirilen stratejiler, yalnızca teknik altyapının güçlendirilmesine değil, aynı zamanda toplumsal katılımın teşvik edilmesine ve güvenlik politikalarının sürdürülebilirliğinin sağlanmasına da katkı sunmaktadır (Bülbül, 2019:65).

Kamu yönetiminde dijitalleşmenin yaygınlaşmasıyla birlikte, yerel düzeyde yürütülen güvenlik politikalarının da teknoloji temelli ve veri odaklı bir çerçevede yeniden yapılandırıldığı görülmektedir. Bu doğrultuda, geleneksel yöntemlerin ötesine geçen güvenlik uygulamaları, dijital altyapıların sunduğu analitik imkânlardan yararlanılarak daha bütüncül ve etkin biçimde planlanmaktadır. Özellikle coğrafi bilgi sistemleri (CBS) aracılığıyla gerçekleştirilen suç haritalama çalışmaları, sadece olayların mekânsal olarak belgelenmesini değil; aynı zamanda risk taşıyan bölgelerin önceden tespit edilmesini ve bu alanlara yönelik müdahale stratejilerinin bilimsel verilere dayalı olarak geliştirilmesini mümkün kılmaktadır. Böylece güvenlik yönetimi, daha rasyonel, proaktif ve yerel koşullara duyarlı bir yapıya kavuşmaktadır (Hayta, 2021:933–934; Erkek, 2017). Bu tür araçlar sayesinde belediyeler, suçla mücadele süreçlerine teknik düzeyde katkı sağlamakla kalmamakta; aynı zamanda önleyici güvenlik hizmetlerinin planlanmasında daha stratejik ve bilimsel temelli yaklaşımlar geliştirebilmektedir. Böylelikle dijitalleşme, yerel güvenlik politikalarının hem etkinliğini hem de sürdürülebilirliğini artıran temel bir unsur hâline gelmektedir.

Yerel yönetimlerin güvenlik alanındaki rolü, yalnızca teknik destek sağlamakla sınırlı kalmamakta; aynı zamanda katılımcı yönetim anlayışı doğrultusunda toplumun güvenlik algısının şekillendirilmesinde de belirleyici bir işlev üstlenmektedir. Bu noktada, yerel düzeyde uygulanan politikalar ve iletişim stratejileri, güvenliğin yalnızca kurumsal bir hizmet değil, aynı zamanda toplumsal bir sorumluluk olarak benimsenmesine katkı sunmaktadır. Özellikle mahalle ölçeğinde yürütülen halkla ilişkiler faaliyetleri, muhtar bilgi sistemleri (T.C. İçişleri Bakanlığı, 2015) ve mobil uygulamalar gibi dijital araçlar aracılığıyla kent sakinlerinin güvenlik süreçlerine aktif

biçimde dâhil edilmesi kolaylaştırılmaktadır (Koç, 2023:3). Bu durum, yalnızca yönetsel etkililiğin artırılmasını sağlamamakta; aynı zamanda vatandaşların sürece katılımı sayesinde güvenlik politikalarının toplumsal meşruiyetini ve kabul edilebilirliğini de güçlendirmektedir. Böylece güvenlik yönetimi, yukarıdan aşağıya işleyen bir mekanizma olmaktan çıkarılarak, yerel düzeyde toplumsal katılımı önceleyen daha kapsayıcı bir yapıya dönüştürülmektedir.

Türkiye özelinde değerlendirildiğinde, “2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı” ile yerel yönetimlere, dijital güvenlik altyapılarının kurulması, yönetilmesi ve sürdürülebilirliğinin sağlanması yönünde çok boyutlu sorumluluklar yüklendiği görülmektedir. Söz konusu strateji belgesi, kent güvenliğinin yalnızca merkezi otoritelerin kontrolüne bırakılmaması gerektiğini, aynı zamanda yerel düzeyde planlama ve koordinasyon mekanizmalarının güçlendirilmesi gerektiğini açıkça ortaya koymaktadır. Bu kapsamda akıllı ulaşım, afet yönetimi, çevresel güvenlik ve kamusal alanların izlenmesi gibi birçok alanın doğrudan yerel yönetimlerin eşgüdümünde yürütülmesi gerektiği özellikle vurgulanmaktadır. Böylece güvenlik, teknik altyapıya indirgenmeyen; planlama, koordinasyon ve sürdürülebilirlik boyutlarını içeren bütüncül bir yaklaşım çerçevesinde ele alınmaktadır (T.C. ÇŞB, 2019).

Kent güvenliğinde teknolojik uygulamalar yalnızca gözetim sistemleriyle sınırlandırılmamakta; aynı zamanda suç analizleri, risk haritaları ve coğrafi bilgi sistemleri gibi veri odaklı yöntemleri de kapsamaktadır. Bu yaklaşımlar, güvenliğin yalnızca anlık müdahalelerle değil, suçun mekânsal ve toplumsal dinamiklerinin önceden tespit edilmesiyle sağlanabileceğini ortaya koymaktadır. Özellikle mekânsal suç bölgelerinin belirlenmesi, çöküntü alanlarının saptanması ve güvenli kentler indeksi gibi araçların geliştirilmesi, suçun önlenmesine yönelik kapsamlı analiz imkânları sunmaktadır. Bu analizler aracılığıyla elde edilen veriler, güvenlik politikalarının daha isabetli biçimde şekillendirilmesine olanak tanımakta; suçun yoğunlaştığı bölgelerde kolluk kuvvetlerinin daha etkin biçimde konumlandırılmasını ve önleyici tedbirlerin sistematik olarak alınmasını mümkün kılmaktadır. Böylece kent güvenliği, yalnızca teknolojik gözetimle değil; veriye dayalı planlama ve risk odaklı stratejilerle desteklenen bütüncül bir anlayışla ele alınmaktadır (Gündüzöz, 2016:336).

Akıllı kentler paradigması çerçevesinde güvenlik hizmetlerinin dönüşümü, yalnızca kurumsal politikaların etkinliğini artırmakla kalmamakta; aynı zamanda bireylerin gündelik yaşamda sahip oldukları güvenlik algısının şekillenmesine de doğrudan katkı sunmaktadır. Kentin farklı noktalarına yerleştirilen kameralar ve alarm sistemleri, suçun ortaya çıkmasını caydırıcı bir unsur olarak işlev görmekte; bireylerin kamusal alanlarda daha güvende hissetmelerini sağlamaktadır (Öner ve Çam, 2022:1171).

Bununla birlikte, güvenliğin yalnızca fiziksel mekânla sınırlı olmadığı; dijital ortamda da bireylerin korunmasını gerektirdiği vurgulanmalıdır. Özellikle siber güvenlik tehditlerine karşı alınan önlemler ile kişisel verilerin korunmasına yönelik geliştirilen politikalar, dijital güvenliğin tesis edilmesinde ve sürdürülmesinde kilit rol oynamaktadır. Bu çerçevede güvenlik, hem fiziksel hem de dijital boyutlarıyla ele alınmakta ve bütüncül bir anlayış çerçevesinde yeniden tanımlanmaktadır (Ün, 2022:416).

Öte yandan, kent güvenliğinde teknolojik altyapıların kurulumu kadar, bu altyapıların kent sakinleriyle etkileşimli biçimde işletilmesi de en az kurulum süreci kadar kritik öneme sahiptir. Çünkü güvenliğin yalnızca teknik araçlarla sağlanamayacağı, aynı zamanda toplumsal katılım ve iş birliğiyle desteklenmesi gerektiği kabul edilmektedir. Bu bağlamda toplum destekli kolluk uygulamaları, teknolojik imkânların vatandaşlarla birlikte değerlendirildiği, yönetim temelli bir yaklaşım sunmaktadır. Bu modelde vatandaş, suçun önlenmesi sürecinde edilgen bir izleyici konumunda bırakılmamakta; güvenliğin sağlanmasında ve sürdürülmesinde aktif bir aktör olarak sürece dâhil edilmektedir. Böylece birey, yalnızca güvenlik hizmetlerinin yararlanıcısı değil, aynı zamanda güvenliğin inşa edilmesinde katkı sağlayan ortak bir paydaş olarak konumlandırılmaktadır. Bu durum, hem güvenlik hizmetlerinin toplumsal meşruiyetini artırmakta hem de kentlerde daha kapsayıcı bir güvenlik anlayışının gelişmesine zemin hazırlamaktadır (Gündüzöz, 2016:338).

Sonuç olarak, kent güvenliğinde teknolojik uygulamaların başarısı, yalnızca kullanılan araçların modernliğiyle değil, bu araçların hangi anlayışla ve hangi stratejik bütünlük içerisinde kullanıldığıyla ilişkilidir. Dijitizasyon, dijitalleşme ve dijital dönüşüm süreçlerinin her biri, kentin güvenliğini sağlamaya yönelik bütüncül bir güvenlik politikasıyla anlam kazanmaktadır. Bu çerçevede, teknoloji yalnızca bir araç

deęil, kent gvenlięinin inřasında kurumsal ve toplumsal iřbirlięini mmkn kılan stratejik bir unsurdur.



BÖLÜM II

TÜRKİYE’DE KENT GÜVENLİK VE DİJİTAL İZLEME SİSTEMLERİNİN YAPISI, BİLEŞENLERİ VE GELİŞİM SÜRECİ

Türkiye’de kent güvenlik sistemlerinin gelişimi, özellikle 2000’li yılların başından itibaren hız kazanan teknolojik dönüşümlerle birlikte şekillenmiştir. İlk aşamada MOBESE ve KGYS uygulamaları, temel olarak suçun önlenmesine ve kentlerde güvenliğin sağlanmasına yönelik gözetim odaklı çözümler şeklinde tasarlanmıştır (Beşe ve Geleri, 2013:245). Zamanla bu sistemler yalnızca izleme araçları olmaktan çıkarılarak veri yönetimi, entegrasyon ve karar destek mekanizmalarıyla donatılmış, böylece kent güvenliğinin dijital altyapısının evrimi hızlandırılmıştır (Karaağaçlı, 2022:741). Bu dönüşüm sürecinde, dijitalleşmenin güvenlik politikaları üzerindeki etkisi de belirginleşmiş; özellikle kamu yönetiminde dijital güvenlik yaklaşımlarının güçlendirilmesi gerekliliği vurgulanmıştır (Akmeşe, 2020:111; Demirel, 2021). Böylelikle, hem tarihsel gelişim hem de dijital güvenlik evrimi dikkate alınarak kent güvenliği alanında daha kapsamlı ve sürdürülebilir bir yapı inşa edilmiştir.

Bu kısımda, Türkiye’de kent güvenliği kapsamında geliştirilen KGYS ve MOBESE uygulamaları çerçevesinde kullanılan teknolojik bileşenler detaylı biçimde ele alınacaktır. Öncelikle, görüntüleme sistemlerine (CCTV, IP kameralar vb.) dair uygulamalara yer verilecek; ardından mobil güvenlik uygulamaları ve bunların mevcut sistemlerle entegrasyonu değerlendirilecektir. Devamında, komuta kontrol merkezlerinin işleyişi ve veri yönetimi süreçleri incelenecek; son olarak veri toplama, depolama ve işleme aşamaları açıklanacaktır. Böylece Türkiye’de dijital kent güvenliği altyapısının temel bileşenlerine ilişkin kapsamlı bir çerçeve sunulmuş olacaktır.

2.1. Kent Güvenlik Yönetim Sistemlerinin Yapısı ve Bileşenleri

Bu kısımda, kent güvenlik yönetim sistemlerinin yapısal özellikleri ve bileşenleri kapsamlı biçimde ele alınacaktır. Öncelikle, gözetim ve denetim süreçlerinde yaygın olarak kullanılan görüntüleme sistemlerine (CCTV, IP kameralar vb.) değinilecek; ardından, mobil uygulamaların mevcut sistemlerle entegrasyonu

incelenecektir. Devamında, komuta kontrol merkezlerinin işleyişi ile veri yönetim mekanizmaları üzerinde durulacak ve son olarak veri toplama, saklama ve işleme süreçleri açıklanacaktır. Böylelikle kent güvenlik yönetim sistemlerinin temel unsurlarına ilişkin bütüncül bir çerçeve ortaya konulmuş olacaktır.

2.1.1. Kent Güvenliğinde Görüntüleme Sistemleri: CCTV, IP Kameralar ve Sayısal Kayıt Teknolojileri

Kent güvenliği politikalarının gelişimi, teknolojik araçların yoğun biçimde kullanılmasını beraberinde getirmiştir. Özellikle gözetim teknolojileri, suçun önlenmesi ve toplumsal düzenin sağlanmasında merkezi bir rol oynamaktadır. Bu bağlamda, kapalı devre televizyon sistemleri (CCTV), IP kameralar ve benzeri görüntüleme teknolojileri, kentlerin güvenlik altyapısının vazgeçilmez bileşenleri hâline gelmiştir. Görüntüleme sistemlerinin kent güvenliğindeki rolü, dijitalleşme süreçleri bağlamında ele alındığında daha kapsamlı bir şekilde değerlendirilebilir.

Görüntüleme sistemlerinin gelişimi, dijitalizasyon süreci ile doğrudan ilişkilidir. Fiziksel olayların, hareketlerin ya da mekânsal verilerin dijital veriye dönüştürülmesi anlamına gelen dijitalizasyon, güvenlik açısından görüntü ve ses verilerinin kaydedilmesini ve dijital ortamda depolanmasını sağlamaktadır. Bu süreçte, geleneksel analog sistemlerden dijital CCTV sistemlerine geçiş, veri güvenliği ve işleme kapasitesinde önemli iyileştirmeler sunmuştur (Erkek, 2017). Dijital kameralar sayesinde elde edilen görüntüler daha uzun süre saklanabilmekte ve gelişmiş analiz yöntemleriyle işlenebilmektedir.

Dijitalleşme, bu sistemlerin sadece kayıt amaçlı değil, aynı zamanda analiz ve müdahale aracı olarak kullanılmasını mümkün kılar. Kamera sistemlerine entegre edilen hareket algılama, yüz tanıma, plaka tanıma gibi algoritmalar, kolluk kuvvetlerine olaylara anlık müdahale etme fırsatı sunmaktadır (Gültekin Varkonyi, 2024:25). Bu sistemler, yalnızca izleme değil, aynı zamanda karar destek sistemlerine veri sağlama açısından da önem taşır. Örneğin, belirli bölgelerde yoğunlaşan hareketlilik ya da şüpheli aktiviteler, sistem tarafından otomatik olarak işaretlenebilmekte ve operatörler tarafından değerlendirilebilmektedir.

Dijital dönüşüm bağlamında ise, görüntüleme sistemlerinin kent yönetiminin bütünleşik bir parçası hâline gelmesi söz konusudur. Akıllı kent stratejilerinde kamera sistemleri, trafik yönetimi, afet koordinasyonu, kamu düzeni sağlanması gibi pek çok alanda kullanılmakta; böylece güvenlik kavramı sadece kolluk faaliyeti olmaktan çıkmakta, çok disiplinli bir yönetim aracına dönüşmektedir (Ulubaş, 2023:70). Türkiye’de yayımlanan “2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı” da bu dönüşümü desteklemektedir (T.C. ÇŞB, 2019). Bu belgede güvenliğin, teknoloji temelli kent yönetiminin temel bileşenlerinden biri olduğu açıkça ifade edilmiştir. Ancak bu teknolojilerin kent yaşamına entegrasyonu, yalnızca teknik altyapı kurulumu ile sınırlı değildir. Toplumsal meşruiyetin sağlanması, kişisel verilerin korunması ve mahremiyetin gözetilmesi gibi etik ve hukuki boyutlar da dikkate alınmalıdır. Bu çerçevede, kamera sistemlerinin yaygınlaştırılması kadar, bu sistemlerin hangi amaçla, kim tarafından ve nasıl kullanılacağına şeffaf biçimde belirlenmesi gerekmektedir (Ün, 2022:419). Aksi halde, güvenlik adına yapılan dijitalleşme hamleleri, toplumsal denetim aracı olarak algılanabilir ve kamuoyunda güvenlik yerine güvensizlik duygusu yaratabilir.

Kentlerde kurulan kamera sistemlerinin etkinliği, yalnızca suçun azaltılması ya da caydırıcılık yönüyle değil, aynı zamanda bireylerin güvenlik algısı üzerindeki etkisiyle de değerlendirilmelidir. Kameraların varlığı, kimi bireylerde güvende hissetme duygusunu artırırken, kimilerinde sürekli gözetlenme hissiyle rahatsızlık yaratabilir (Öner ve Çam, 2022:1175). Bu bağlamda, güvenliğin sağlanması kadar, bu güvenliğin nasıl inşa edildiği ve hangi değerlerle desteklendiği de önem arz eder.

Kentsel güvenliğin artırılmasında, CCTV ve IP kameralar gibi görüntüleme sistemlerinin kullanımı giderek yaygınlaştırılmış ve bu sistemler sayesinde kent genelinde sürekli ve kapsamlı bir gözetim ağı oluşturulabilmiştir. Bu teknolojiler aracılığıyla toplanan video verilerinin, sayısal kayıt sistemleri vasıtasıyla depolanması ve gerçek zamanlı analiz için uygun hâle getirilmesi sağlanmıştır. Söz konusu sistemlerin kent güvenliğine katkısı, yalnızca suçların tespiti ve delillendirilmesiyle sınırlı kalmayıp, aynı zamanda suçun önlenmesine yönelik erken uyarı mekanizmalarının geliştirilmesini de mümkün kılmıştır. Ancak bu teknolojilerin etkili biçimde çalışabilmesi için yüksek çözünürlüklü kayıt altyapısı ve yapay zekâ destekli

analiz mekanizmalarına duyulan ihtiyaç da vurgulanmıştır (Dardour, El Haji & Begdouri, 2025:15).

Sonuç olarak, CCTV, IP kameralar ve benzeri görsel izleme teknolojileri, kent güvenliğine yönelik dijital altyapının en temel bileşenleri arasında yer almaktadır. Bu sistemlerin; dijitalizasyonla başlayan, dijitalleşme süreciyle olgunlaşan ve dijital dönüşümle kurumsal bir yapıya kavuşan evrimi sayesinde kentler, daha güvenli, daha kolay izlenebilir ve gerektiğinde daha hızlı müdahale edilebilir alanlara dönüşmektedir. Ancak bu teknolojik imkânların etkili ve sürdürülebilir bir güvenlik anlayışı yaratabilmesi için, hukuki düzenlemelerle desteklenmesi, toplumsal katılıma açık olması ve etik ilkelere dayalı bir çerçeve içinde uygulanması büyük önem taşımaktadır.

2.1.2. Mobil Uygulamalar ve Entegrasyon

Dijitalleşme sürecinin kamu güvenliği alanındaki yansımaları, teknolojik altyapıların daha etkin kullanılmasını gerekli kılmaktadır. Bu çerçevede KGYS, özellikle mobil uygulamalarla bütünleşerek daha dinamik ve etkili bir güvenlik yönetimi sunma kapasitesine ulaşmıştır. Mobil uygulamalar, kent güvenliği alanında bilgiye hızlı erişim, yerinde müdahale ve veri paylaşımında büyük avantajlar sağlamaktadır. Bu sistemlerin bütünleşmiş bir biçimde çalışması, güvenlik birimlerinin operasyonel etkinliğini artırmakta ve kamu düzeninin sağlanmasına katkı sunmaktadır.

Kent güvenliği alanında mobil uygulamaların entegrasyonu, sadece veri görselleştirme işleviyle sınırlı kalmayıp, gerçek zamanlı tahmin ve uyarı mekanizmalarının geliştirilmesine de olanak tanımıştır. Bu bağlamda, suç yoğunluğu yüksek bölgelerin tespitine yönelik geliştirilen sistemin, makine öğrenmesi algoritmalarıyla desteklendiği ve mobil arayüz üzerinden kullanıcılarla etkileşimli biçimde çalıştığı belirtilmiştir. Uygulamanın, kullanıcıların suç bildiriminde bulunabildiği, harita üzerinden riskli alanları görüntüleyebildiği ve anlık uyarılar alabildiği bir yapıya sahip olduğu aktarılmıştır. Böylece hem bireysel farkındalık artırılmış hem de kamusal güvenliğe yönelik kolektif veri üretimi desteklenmiştir (Vega-Huerta vd., 2025:8).

KGYS, temelde görüntüleme, çağrı yönetimi ve mobil uygulamalar olmak üzere üç ana bileşenden oluşur. Bu sistemler arasında entegrasyonun sağlanması, güvenlik yönetiminin bütüncül bir yapıya kavuşmasını mümkün kılar. Özellikle mobil uygulamalar, sahada görev yapan güvenlik personelinin anlık veri alışverişinde bulunmasını sağlayarak operasyonel süreçlerin verimliliğini artırır (Beşe ve Geleri, 2013:247).

Mobil uygulamalar; GPS destekli araç takibi, mobil kimlik sorgulama, plaka tanıma ve suç veritabanı taramaları gibi fonksiyonlarla donatılmıştır. Bu donanımlar sayesinde, güvenlik güçleri olay yerine ulaşmadan önce bilgi edinebilmekte, olay anında ise eş zamanlı veri paylaşımı gerçekleştirebilmektedir. Bu durum, suçla mücadelede zaman kaybını önlemekte ve olaylara müdahale süresini azaltmaktadır (EGM, 2013).

Özellikle Bursa ve İzmir örneklerinde görüldüğü üzere, mobil uygulamaların sistematik kullanımıyla birlikte suç önleme, izleme ve müdahale süreçlerinde kayda değer ilerlemeler sağlanmıştır. Bursa'da hayata geçirilen BEMTAP projesi, mobil sorgulama sistemlerinin bütünleşmiş edildiği ilk uygulamalardan biri olarak öne çıkmakta; polis ekiplerinin sahada bireylerin kimliklerini hızlıca sorgulamasına olanak tanımaktadır (Portakal, 1999). Aynı şekilde İzmir KGYS'de mobil uygulamalar, görüntü analiz yazılımlarıyla bütünleşmiş biçimde çalışmakta, olay tespiti ve önleyici güvenlik uygulamaları daha sistematik bir şekilde yürütülmektedir (Özhan, 2014:243).

Ankara KGYS uygulamasında mobil teknolojilerin daha gelişmiş hali görülmektedir. 100 adet mobil bilgisayar ve 300 araç takip sistemi, merkezle sahadaki ekipler arasında kesintisiz iletişim kurulmasına olanak sağlamaktadır. Mobil donanım sayesinde, çağrı yönetimiyle eş zamanlı veri paylaşımı yapılmakta ve bu veriler anlık olarak analiz edilerek yöneticilere karar desteği sunmaktadır. Bu, hem stratejik planlama hem de saha operasyonlarında ciddi bir avantaj yaratmaktadır (Gündem, 2010).

Mobil uygulamaların entegrasyonunun teknik boyutu da göz ardı edilmemelidir. İzmir KGYS örneğinde olduğu gibi, görüntüleme sistemleri ile mobil sistemlerin aynı yazılım platformunda entegre edilmesi, farklı birimlerin eş zamanlı çalışabilmesini sağlamıştır. Bu tür yazılım tabanlı entegrasyonlar, yalnızca izleme değil, müdahale ve raporlama süreçlerini de optimize etmektedir (Özhan, 2014:245).

Mobil uygulamalar sadece güvenlik amacıyla değil, trafik düzenlemeleri ve toplumsal olayların yönetiminde de etkili şekilde kullanılmaktadır. Özellikle trafik ihlallerinin tespiti ve şüpheli araç takibinde mobil plaka tanıma sistemleri hızlı sonuçlar üretmekte; anlık tespit edilen ihlaller, merkezi veri tabanları ile senkronize edilerek işlem yapılmaktadır (EGM, 2013).

KGYS içinde mobil uygulamalar, bütünleşmiş güvenlik yönetiminin vazgeçilmez bir bileşeni haline gelmiştir. Gelişen teknolojilere uyum sağlayan bu mobil sistemler, güvenlik yönetiminde esnekliği ve etkinliği artırmakta, hem suçla mücadelede hem de önleyici güvenlik politikalarının uygulanmasında kritik rol oynamaktadır. Türkiye’de Bursa, İzmir ve Ankara örneklerinde olduğu gibi, mobil uygulamalarla desteklenen bütünleşmiş güvenlik sistemleri, kentlerde güvenlik hizmetlerinin niteliğini artırmakta, kamu güvenliğinin sağlanmasında önemli katkılar sunmaktadır.

2.1.3. Komuta Kontrol Merkezleri ve Veri Yönetimi

Kent Güvenlik Yönetim Sistemleri (KGYS), dijitalleşen güvenlik anlayışının somut bir yansıması olarak karşımıza çıkmaktadır. Bu sistemin işleyişinde merkezi rol üstlenen Komuta Kontrol Merkezleri, hem izleme ve yönlendirme fonksiyonlarını yürütmekte hem de güvenliğin koordinasyonunu sağlamaktadır. Teknolojik gelişmelerle uyumlu olarak yeniden yapılandırılan bu merkezler, güvenlik verisinin toplanması, sınıflandırılması, analiz edilmesi ve müdahale süreçlerine yön verilmesinde temel bir işlev üstlenir. Bu bağlamda, dijital dönüşümün üç temel aşaması olan dijitalizasyon, dijitalleşme ve dijital dönüşüm kavramları üzerinden Komuta Kontrol Merkezlerinin rolü kavramsal ve işlevsel yönleriyle ele alınmalıdır.

Komuta Kontrol Merkezleri, güvenlik yönetiminde dijitalleşmenin ilk halkasını oluşturan dijitalizasyon süreciyle birlikte, fiziksel verilerin dijital ortama aktarılması işlevini üstlenmiştir. Kentte yer alan kameraların sağladığı görsel veriler ve olaylara dair anlık bilgiler, bu merkezlerde toplanarak dijital formda depolanmaktadır (Beşe ve Geleri, 2013:252). Ancak bu süreç, sadece veri depolamayı değil; aynı zamanda veri yönetimini ve analizini de kapsayan daha geniş bir çerçeveye sahiptir.

Akıllı kentlerde komuta kontrol merkezlerinin, çok katmanlı veri akışlarını eş zamanlı olarak izleyip yönlendiren birer dijital beyin işlevi üstlendiği ifade edilmiştir. Bu merkezlerde, IoT cihazlarından gelen çok boyutlu veriler ağ geçitleri aracılığıyla toplanmakta ve bulut bilişim altyapısı sayesinde ölçeklenebilir bir şekilde işlenebilmektedir. Ağ protokollerinin dönüştürülmesi ve farklı sensör türlerinin entegre edilmesi yoluyla, veri tutarlılığı ve analiz edilebilirlik düzeyi artırılmıştır. Gerçek zamanlı karar destek mekanizmalarının oluşturulması, güvenli, gecikmesiz ve düşük paket kayıplı iletişim altyapısıyla mümkün hâle getirilmiştir. Bu yapının, kentsel operasyonların merkezî biçimde izlenmesi ve veriye dayalı yönetim stratejilerinin uygulanabilmesi açısından kritik öneme sahip olduğu vurgulanmıştır (Su, Chen ve Lu, 2022:3676).

Dijitalleşme aşamasında, toplanan verilerin işlenmesi ve operasyonel süreçlerle entegre edilmesi ön plana çıkmaktadır. Komuta Kontrol Merkezleri, farklı birimlerden gelen verileri senkronize şekilde yönetebilme kapasitesine sahiptir. Örneğin, İzmir KGYS uygulamasında, görüntü sistemleri ile mobil sorgu altyapısının ortak yazılım platformunda birleştirilmesi, Komuta Kontrol Merkezlerinde anlık olay analizlerinin yapılmasına olanak sağlamaktadır (Özhan, 2014:246). Bu tür uygulamalar, yalnızca olaylara müdahale sürecini hızlandırmakla kalmamakta, aynı zamanda veri temelli güvenlik politikalarının oluşumuna da zemin hazırlamaktadır.

Bu merkezlerin dijitalleşme sürecindeki en önemli kazanımı, karar destek mekanizmalarının güçlendirilmesi olmuştur. Ankara örneğinde görüldüğü üzere, 300 araç takip sistemi ve 100 mobil bilgisayar aracılığıyla elde edilen saha verileri, Komuta Kontrol Merkezlerinde değerlendirilmekte ve yöneticilere stratejik kararlar için temel bilgi sunmaktadır (Gündem, 2010). Bu veriler aynı zamanda çağrı yönetim sistemleriyle bütünleşmiş çalışarak, olaylara hızlı ve yerinde müdahaleyi mümkün kılmaktadır.

Dijital dönüşüm aşamasında ise, Komuta Kontrol Merkezleri sadece veri yönetiminde birimler arası koordinasyonu sağlamakla kalmamakta, aynı zamanda kurumsal işleyişin yeniden yapılandırıldığı bir organizasyon merkezine dönüşmektedir. Bursa'da geliştirilen BEMTAP projesinde olduğu gibi, sayısal sistemlerle entegre edilen komuta merkezleri, olayları önceden tahmin etmeye yönelik analizler yaparak önleyici güvenlik hizmetlerinin etkinliğini artırmaktadır (Portakal,

1999). Bu dönüşüm, veri odaklı bir yönetim modelinin güvenlik alanına da nüfuz ettiğini göstermektedir.

Veri yönetimi açısından Komuta Kontrol Merkezleri, yalnızca veri toplamakla kalmaz; aynı zamanda bu verilerin gizliliği, bütünlüğü ve kullanılabilirliğini sağlayacak şekilde koruma mekanizmaları geliştirir. İzmir KGYS uygulamasında, tüm görüntü sistemleri ve sorgu altyapısı tek merkezden kontrol edilmekte, böylece veri güvenliği merkezi düzeyde denetim altına alınmaktadır (EGM, 2013). Bu durum, hem operasyonel güvenliği hem de kamu güvenliği algısını olumlu yönde etkilemektedir.

Komuta Kontrol Merkezleri, dijitalleşmenin kamu güvenliği alanındaki stratejik yansıması olarak, KGYS içinde merkezi bir konuma sahiptir. Bu merkezler, dijitalizasyon ile dijital verinin elde edilmesini, dijitalleşme ile operasyonlara entegre edilmesini ve dijital dönüşümle birlikte kurumsal yapının yeniden şekillenmesini mümkün kılar. İzmir, Bursa ve Ankara örnekleri, bu merkezlerin farklı düzeylerde dijitalleşme aşamalarını başarıyla gerçekleştirdiğini göstermektedir. Veri yönetimindeki rolü, yalnızca bilgi akışını sağlamakla sınırlı kalmayan Komuta Kontrol Merkezleri, aynı zamanda kent güvenliğinin dijital çağda yeniden tanımlanmasına katkı sunan kritik yapılardır.

2.1.4. Veri Toplama, Saklama ve İşleme Süreçleri

Dijital teknolojilerin güvenlik sistemlerine entegre edilmesiyle birlikte, veri toplama, saklama ve işleme süreçleri kent güvenliği yönetiminde stratejik öneme sahip hale gelmiştir. KGYS kapsamında bu süreçler, yalnızca bilgi depolamaya yönelik işlemler değil; aynı zamanda olaylara dair erken uyarı sistemlerinin geliştirilmesi, karar destek mekanizmalarının güçlendirilmesi ve güvenlik birimleri arasında eşgüdüm sağlanması açısından kritik roller üstlenmektedir. Bu çerçevede dijitalizasyon, dijitalleşme ve dijital dönüşüm kavramları, veri yönetimi süreçlerinin evrimini anlamak açısından temel kavramsal çerçeveyi sunar.

Veri toplama süreci, dijitalleşmenin ilk aşaması olan dijitalizasyon ile başlamaktadır. Bu aşamada, fiziksel ortamlarda üretilen bilgi ve gözlemler dijital formata dönüştürülmekte; örneğin güvenlik kameraları aracılığıyla elde edilen görüntüler dijital kayıt cihazlarında arşivlenmektedir. Bu veriler, Komuta Kontrol

Merkezlerinde toplanmakta ve sistematik şekilde saklanmaktadır (Beşe ve Geleri, 2013:255). Dijitalizasyon süreci, analog verinin dijital ortama aktarılmasıyla sınırlı kalmayıp, bu verilerin standart formatlarda kaydedilmesini ve ileri aşamalarda analiz edilmesini de mümkün kılar.

Dijitalleşme, verilerin yalnızca dijital ortamda bulunmasından öteye geçerek, bunların aktif olarak işlenmesi ve güvenlik sistemleriyle entegre şekilde kullanılması anlamına gelir. İzmir KGYS uygulamasında olduğu gibi, dijital veriler, mobil uygulamalar ve plaka tanıma sistemleri ile eşgüdüm içinde çalışarak anlık analizlere zemin hazırlamaktadır (Özhan, 2014:248). Bu entegrasyon sayesinde veri, operasyonel süreçlerde doğrudan kullanılabilen; olay yeri görüntüleri, araç hareketlilik bilgileri ve kimlik sorgu sonuçları anlık olarak değerlendirilerek müdahale süreci başlatılabilmektedir.

Veri saklama süreci ise güvenlik yönetiminin sürdürülebilirliği açısından büyük önem taşır. Saklanan verilerin güvenli biçimde depolanması, yalnızca teknik bir zorunluluk değil; aynı zamanda hukuki ve etik bir gerekliliktir. Komuta Kontrol Merkezleri, farklı kaynaklardan gelen verileri sınıflandırarak uzun vadeli arşivleme sistemleri oluşturmakta; böylece geçmiş olaylara ilişkin analizler yapılmasına olanak tanımaktadır. Ankara KGYS örneğinde, araç takip sistemlerinden ve mobil cihazlardan gelen veriler, sistematik biçimde kaydedilmekte ve daha sonra operasyonel değerlendirmeler için kullanılmaktadır (Gündem, 2010).

Veri işleme süreci ise dijital dönüşümün doğrudan tezahür ettiği alandır. Dijital dönüşüm, sadece teknolojik entegrasyonu değil; kurumların karar alma süreçlerinin veri temelli hale gelmesini ve organizasyon yapılarının bu doğrultuda yeniden kurgulanmasını ifade eder. Bursa'da uygulanan BEMTAP projesinde, toplanan veriler yalnızca izleme amaçlı kullanılmamakta; aynı zamanda suç önleme stratejilerinin belirlenmesi, risk analizlerinin yapılması ve kaynak planlamasının geliştirilmesinde aktif rol oynamaktadır (Portakal, 1999). Bu durum, verinin pasif bir bilgi birikimi olmaktan çıkarak aktif bir yönetim aracına dönüştüğünü göstermektedir.

Akıllı kentlerde veri platformlarının etkin işleyişi, yalnızca verilerin toplanmasıyla sınırlı kalmamakta, aynı zamanda bu verilerin güvenli bir şekilde depolanması, analiz edilebilir formatlarda tutulması ve karar destek süreçlerine entegre edilebilmesi ile doğrudan ilişkilidir. Özellikle gerçek zamanlı sensör

verilerinin, kentsel operasyonların anlık yönetimi açısından kritik rol oynadığı vurgulanmaktadır. Bununla birlikte, farklı kaynaklardan gelen verilerin biçimsel tutarsızlıkları, veri kalitesindeki değişkenlik ve kişisel verilerin korunmasına ilişkin yasal çerçeveler, entegrasyon süreçlerini karmaşıklaştırmaktadır. Bu nedenle, sürdürülebilir ve esnek bir kent veri altyapısının, yalnızca teknolojik değil aynı zamanda yönetimsel düzeyde de iyi tasarlanmış bir yapıya sahip olması gerekmektedir (Hashem vd., 2016: 394).

Dijital dönüşümle birlikte, veri işleme yalnızca merkezî düzeyde değil; sahada görev yapan birimler tarafından da yürütülebilmektedir. Mobil uygulamalar sayesinde güvenlik personeli olay yerinde veri girişi yapabilmekte, sistemle gerçek zamanlı bağlantı kurabilmektedir. Bu uygulamalar, veri döngüsünü hızlandırmakta ve operasyonel kararların niteliğini artırmaktadır (EGM, 2013).

Veri toplama, saklama ve işleme süreçleri, KGYS'nin dijital altyapısını oluşturan temel dinamiklerdir. Bu süreçler, dijitalizasyon ile başlayan, dijitalleşme ile genişleyen ve dijital dönüşümle birlikte kurumsal güvenlik anlayışını yeniden şekillendiren aşamalarla gelişmektedir. Verinin etkin şekilde toplanması, güvenli biçimde saklanması ve anlamlı bilgiler hâline getirilerek işlenmesi, modern kent güvenliği politikalarının temel dayanaklarını oluşturur. İzmir, Ankara ve Bursa örneklerinde olduğu gibi, bu süreçlerin etkili biçimde yönetilmesi, güvenlik hizmetlerinin kalitesini artırmakta; veri temelli karar verme kapasitesi sayesinde kamu güvenliğinin daha proaktif ve sistematik biçimde sağlanmasına katkı sunmaktadır.

2.2. MOBESE ve KGYS Sistemlerinin Tarihsel Gelişimi

Bu kısımda, Türkiye’de kent güvenliğinin dijital altyapısını oluşturan MOBESE ve KGYS sistemlerinin tarihsel gelişimi ele alınacaktır. İlk olarak, MOBESE sisteminin kurulma süreci, bu sürecin arka planında yatan ihtiyaçlar ve sistemin amaçları açıklanacaktır. Ardından, MOBESE’nin teknik bileşenleri detaylandırılarak, dijital güvenlik mimarisinin yapısal unsurlarına odaklanılacaktır. Böylece, Türkiye’deki kent güvenliği politikalarının dijitalleşme sürecindeki evrimi bütüncül bir çerçevede incelenmiş olacaktır.

2.2.1. MOBESE Sistemi: Kurulum Süreci ve Amaçları

Kentleşmenin hızlandığı ve nüfus yoğunluğunun arttığı çağdaş şehir yaşamında, güvenlik hizmetlerinin etkinliği, yalnızca insan gücüne değil; aynı zamanda teknolojik altyapılara da bağlıdır. Türkiye’de bu dönüşümün öncüsü olan Mobil Elektronik Sistem Entegrasyonu (MOBESE), KGYS kapsamında geliştirilmiş; izleme, denetim, yönlendirme ve kayıt işlevlerini bir arada yürüten, çok katmanlı bir dijital güvenlik sistemine dönüşmüştür. MOBESE sisteminin kuruluş süreci ve bu süreçte güdülen amaçlar, güvenlik hizmetlerinin dijitalleşmesinin kurumsal ve teknolojik boyutlarını ortaya koymak açısından son derece önemlidir.

MOBESE sisteminin kuruluşu, Türkiye’de 2000’li yılların başında, İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü’nün koordinasyonu ile başlatılmıştır. İlk uygulama örnekleri, büyükşehirlerde pilot projeler şeklinde hayata geçirilmiş; bu deneyimlerden elde edilen sonuçlara göre sistem tüm yurda yayılmıştır. Kurulum süreci kapsamında, sabit ve hareketli kameralar, plaka tanıma sistemleri (PTS), araç takip cihazları ve mobil veri terminalleri gibi teknolojiler tedarik edilerek güvenlik birimlerine entegre edilmiştir (Özhan, 2014:249).

Kurulumun temel amacı, yalnızca olayları kaydetmek değil, aynı zamanda suçun önceden tespiti, kamu düzeninin korunması ve olaylara müdahale süresinin minimize edilmesidir. Bu bağlamda MOBESE, yerel yönetimlerle iş birliği içinde, belirli risk analizleri doğrultusunda kameraların stratejik noktalara yerleştirilmesiyle şekillenmiştir. Özellikle Ankara, İstanbul ve İzmir gibi metropollerde, trafik kontrolü, toplumsal olayların izlenmesi ve olay yeri tespiti gibi çok yönlü amaçlarla yapılandırılmıştır (Karaağaçlı, 2022:743).

Dijitalleşme literatüründe yer alan kavramlar, kent güvenlik sistemlerinin geçirdiği dönüşümün anlaşılmasında önemli bir çerçeve sunmaktadır. Fiziksel olayların dijital ortama aktarılmasıyla başlayan süreç, MOBESE kameraları aracılığıyla gerçek zamanlı verilerin toplanmasıyla somutlaşmaktadır. Bu verilerin işlenmesi, saklanması ve ilgili birimlerle paylaşılması, sistemin yalnızca izleme değil, aynı zamanda karar destek işlevi görmesini mümkün kılmaktadır. Örneğin, elde edilen görüntülerin plaka tanıma sistemleriyle analiz edilmesi, suçla mücadelede doğrudan kullanılabilir çıktılar üretmektedir (Özhan, 2014:251).

Teknolojik gelişmelerin ötesinde, bu altyapıların güvenlik yönetimini dönüştürücü bir etki yarattığı da görülmektedir. MOBESE, operasyonel süreçleri hızlandırarak güvenlik birimlerinin proaktif şekilde hareket edebilmesini sağlamış; böylece hem karar alma mekanizmaları hem de sahadaki personelin etkinliği artırılmıştır (Karaağaçlı, 2022:745).

Kurulum süreci aynı zamanda yerel yönetimlerle yapılan protokolleri, bütçe tahsislerini ve teknik donanımın tedarik süreçlerini de kapsamıştır. Belediyeler, kameraların montajı, altyapının oluşturulması ve enerji temini gibi konularda Emniyet birimleriyle eşgüdümlü çalışmıştır. Bu iş birliği sayesinde, sistem yalnızca güvenlik açısından değil, şehir yönetimi açısından da bütüncül bir dijital izleme kapasitesine kavuşmuştur (Özhan, 2014:253).

MOBESE sistemi, Türkiye’de kamu güvenliğinin sağlanmasında dijitalleşmenin ve teknolojik entegrasyonun öncüsü olmuştur. Kurulum süreci, teknik altyapının inşası kadar kurumsal iş birliği, bütçelendirme ve yerel uyarlamalar gibi çok boyutlu bir yapılanmayı gerektirmiştir. Sistem, dijitalizasyon ile olayları dijitalleştirmiş, dijitalleşme ile veriye dayalı analiz süreçlerini mümkün kılmış, dijital dönüşüm ile güvenlik hizmetlerinin yapısını kökten dönüştürmüştür. Böylece MOBESE, yalnızca teknolojik bir sistem değil; aynı zamanda dijital çağın güvenlik anlayışını temsil eden stratejik bir araç hâline gelmiştir.

2.2.2. MOBESE'nin Teknik Bileşenleri

Bu kısımda, MOBESE sistemlerinin teknik bileşenleri ele alınacaktır. Kent güvenlik yönetiminin temelini oluşturan bu bileşenler, sistemin etkin işleyişini ve farklı güvenlik ihtiyaçlarına yanıt verebilmesini mümkün kılmaktadır. Öncelikle, verilerin toplandığı ve işlendiği komuta kontrol merkezlerine değinilecek; ardından, suçun önlenmesi ve olayların izlenmesinde merkezi bir role sahip olan görüntüleme sistemleri incelenecektir. Bunun devamında, plaka tanıma sistemleri ile araç takip ve mobil araç sorgulama sistemlerinin sunduğu katkılar açıklanacaktır. Son olarak, mahalle ölçeğinde yönetim süreçlerinin dijitalleşmesine olanak tanıyan muhtarlık otomasyon sistemine yer verilecektir. Böylece MOBESE’nin çok katmanlı teknik altyapısına ilişkin kapsamlı bir değerlendirme ortaya konulmuş olacaktır.

2.2.1.1. Komuta Kontrol Merkezi (KKM)

MOBESE, modern güvenlik anlayışının somut bir yansıması olarak kent yaşamında giderek yaygınlaşan bir teknolojik altyapıyı ifade etmektedir. Bu sistemin işlevselliğini sağlayan ve bütün alt bileşenlerin koordinasyonunu gerçekleştiren temel yapıtaşlarından biri, hiç kuşkusuz Komuta Kontrol Merkezi'dir. KKM, yalnızca operasyonel bir izleme ve yönlendirme aracı değil, aynı zamanda dijital gözetim sistemlerinin merkezileştiği, bilgi teknolojilerinin güvenlik aygıtlarıyla bütünleştiği bir yapıdır. Bu bağlamda KKM, dijital dönüşüm çağında güvenlik politikalarının yönetsel ve teknik koordinasyonunu sağlayan ana kumanda noktası olarak değerlendirilmektedir (Ekinci, 2011:87).

KKM, MOBESE sisteminin merkezi sinir ağı gibi çalışmakta, kent genelindeki kameralar, plaka tanıma sistemleri ve mobil araç sorgulama birimlerinden gelen verileri toplayarak merkezi bir çerçevede analiz etmektedir. Bu veriler, yalnızca izleme değil, aynı zamanda yönlendirme, kayıt altına alma ve anlık müdahale gibi işlevlerin yerine getirilmesinde de kullanılmaktadır. İstanbul Emniyet Müdürlüğü'nün tanımına göre KKM, kamu hizmetlerinin iyileştirilmesi ve suç oranlarının azaltılması hedefleri doğrultusunda, 3500 polis aracı ve 10 ayrı sistemin entegre edildiği bir altyapı bütünlüğü içerisinde çalışmaktadır (İstanbul Emniyet Müdürlüğü, 2013).

Teknolojik izleme kapasitesinin artmasıyla birlikte KGYS, yalnızca teknik bir yapı olmaktan çıkarak güvenlik yönetiminin kurumsal bir bileşeni hâline gelmiştir. Bu sistemler aracılığıyla elde edilen veriler düzenli olarak toplanmakta, işlenmekte ve güvenlik birimlerinin kullanımına sunulmaktadır. Böylece suçların önlenmesine, olaylara hızlı müdahale edilmesine ve kamu düzeninin sağlanmasına katkı sağlanmaktadır. Bununla birlikte, kişisel verilerin korunmasına yönelik yasal çerçevenin net biçimde belirlenmesi ve uygulamaların şeffaf şekilde yürütülmesi, sistemin etkinliği kadar güvenilirliği açısından da kritik bir gereklilik olarak öne çıkmaktadır (Bahar, 2013:200).

KKM, akıllı şehir altyapılarında IoT cihazlarından gelen büyük hacimli verilerin analiz edilmesi, olası siber tehditlerin tespit edilmesi ve hizmet sürekliliğinin sağlanması adına merkezi bir rol oynamaktadır. Bu merkezlerde, uçtan uca veri akışları yapay zekâ destekli modellerle sürekli gözetim altında tutulmakta; özellikle trafik

yoğunluğu, DDoS saldırıları veya sistem arızaları gibi olağandışı durumlar gerçek zamanlı olarak tespit edilebilmektedir. Bu sayede, kent güvenliği açısından kritik altyapıların daha hızlı ve etkin müdahale süreçleriyle yönetilmesi mümkün hale gelmektedir (Balachandar ve Chinnaiyan, 2021:18).

Komuta Kontrol Merkezleri, MOBESE sisteminin hem teknik hem de yönetsel işleyişinin temelini oluşturan, dijital güvenlik mimarisinin en kritik bileşenlerinden biridir. Bu merkezler, dijital verilerin toplanması, analiz edilmesi ve yönlendirilmesinde ana aktör olmanın ötesinde, gözetim toplumunun kurumsal omurgasını da temsil etmektedir. Dijitalleşme sürecinin güvenlik politikalarına entegrasyonu, kamusal fayda ile bireysel mahremiyet arasındaki dengeyi yeniden tanımlamakta ve bu alanda yeni normlar üretmektedir. Bu nedenle KKM'lerin işleyişi, sadece teknik verimlilik açısından değil, aynı zamanda sosyopolitik etkileri bağlamında da değerlendirilmelidir.

2.2.1.2.Görüntüleme Sistemleri

Güvenliğin dijital araçlar aracılığıyla yeniden tanımlandığı günümüzde, MOBESE sisteminin en görünür ve temel bileşeni olan görüntüleme sistemleri, hem teknolojik hem de sosyolojik yönleriyle önem taşımaktadır. Kamuya açık alanlarda 24 saat esasına göre çalışan bu sistemler, yalnızca suçun tespiti ve önlenmesi için değil, aynı zamanda bireylerin davranışlarının izlenmesi ve düzenlenmesi amacıyla da kullanılmaktadır. Bu yönüyle görüntüleme sistemleri, kamusal alanın yapısını ve bireylerin bu alandaki varoluş biçimlerini yeniden şekillendiren dijital bir gözetim pratiği olarak karşımıza çıkmaktadır (Bahar, 2013:201).

Görüntüleme sistemleri, MOBESE bileşenleri içerisinde merkezi bir rol oynar. Bahar'a (2013:202) göre bu kameralar, kamusal güvenliğin sağlanması adına kent merkezlerinden sokak aralarına kadar geniş bir coğrafyada konuşlandırılmakta ve toplumsal hayatın dijital kayıt altına alınmasına olanak sağlamaktadır. Bu sistemlerin altyapısı, genellikle yüksek çözünürlüklü (HD) kameralarla desteklenmekte; bu da suçun tespiti, trafik düzeninin sağlanması ve toplumsal olaylara müdahale gibi süreçlerde etkinlik sağlamaktadır (İstanbul Emniyet Müdürlüğü, 2013).

Akıllı şehirlerde güvenliđin sađlanmasına y6nelik olarak g6r6nt6leme sistemleri, yalnızca pasif g6zetim ara7ları olmaktan 7ıkmıř, yapay zekâ destekli analizlerle aktif karar destek sistemlerine d6n6řmüřt6r. Bu sistemlerde toplanan video verileri, 6nceden tanımlanmıř olay senaryoları 7er7evesinde ger7ek zamanlı olarak iřlenmekte; nesne algılama, davranıř analizi ve insan yođunluđu 6l76m6 gibi iřlevlerle anormallikler tespit edilerek hızlı m6dahale s6re7leri tetiklenebilmektedir. Bu bađlamda, kent güvenliđinin artırılması ve risklerin proaktif bi7imde y6netilmesi amacıyla, video analiz sistemlerinin kentsel karar alma s6re7lerinin ayrılmaz bir par7ası hâline geldiđi belirtilmektedir (Singh vd.,2021:1-2).

G6r6nt6leme sistemleri, kent güvenliđini sađlama hedefinin 6tesinde, bireylerin kamusal alandaki hareketlerini s6rekli denetim altında tutarak bir g6zetim toplumunun altyapısını oluřturmaktadır. Dijitalleřmenin sađladıđı olanaklar, bu sistemleri sadece teknik deđil aynı zamanda politik ve sosyolojik birer ara7 haline getirmiřtir. Bu nedenle, g6r6nt6leme sistemlerinin etkinliđini deđerlendirirken sadece güvenlik temelli faydaları deđil, aynı zamanda bireysel hak ve 6zg6rl6kler 6zerindeki etkileri de dikkate alınmalıdır.

2.2.1.3. Plaka Tanıma Sistemleri

Geliřen kentleřme, artan ara7 sayısı ve güvenlik gereksinimleri dođrultusunda, tařıt tanıma ve izleme ihtiya7ı dijital 76z6mlerle karřılanmaya 7alıřılmaktadır. Bu bađlamda plaka tanıma sistemleri (PTS), hem trafik d6zenlemeleri hem de güvenlik uygulamaları a7ısından merkezi 6neme sahip teknolojik ara7lar hâline gelmiřtir. Plaka tanıma teknolojisi, g6r6nt6 iřleme, yapay zekâ ve veritabanı y6netimi gibi 7eřitli disiplinlerin birleřiminden oluřan b6t6nsel bir sistemdir (Anagnostopoulos vd., 2006:380). Zaman i7erisinde klasik y6ntemlerden 6đrenme tabanlı yaklařımlara evrilen bu sistemler, hem dođruluk hem de esneklik a7ısından 6nemli geliřmeler kaydetmiřtir.

Plaka tanıma sistemleri temelde 67 ařamadan oluřmaktadır: Plakanın yerinin tespiti, karakterlerin ayrıřtırılması ve tanınması. İlk ařama olan plaka b6lgesi tespiti, sistemin genel bařarımını belirleyen en kritik adımdır. Geleneksel y6ntemler arasında kenar istatistiklerine dayalı yaklařımlar, morfolojik iřlemler ve renk temelli filtreleme

teknikleri bulunmaktadır (Hongliang ve Changping, 2004:831). Ancak deęişken dıř çevre kořulları, görüntü kalitesindeki farklılıklar ve açısal bozulmalar, bu tekniklerin sınırlılıklarını ortaya çıkarmaktadır. Bu nedenle, daha esnek ve bağlamsal analiz yeteneęi saęlayan kořullu rastgele alan (CRF) modelleri önerilmiřtir (Li vd., 2013:1690).

Plaka tespiti sonrası ikinci adım olan karakter ayrıştırma, Plaka üzerindeki harf ve rakamların bir bütün olarak sistematik şekilde ayrılması sürecidir. Burada genellikle binarizasyon², blob labeling³ ve segmentasyon teknikleri⁴ kullanılır. Ancak karakterler arasındaki boşlukların dar olması, arka plan gürültüsü ve karakter bozulmaları ayrıştırma sürecini zorlařtırmaktadır. Nomura vd. (2005:1966), bozulmuş karakter görüntülerinde uyarlanabilir morfolojik yaklařımlarla daha saęlıklı ayrıştırma yapılabileceęini savunmuřtur.

Son ařamada, ayrıştırılmıř karakterlerin dijital veritabanında yer alan řablonlarla eřleřtirilmesi gerekir. Geleneksel sistemlerde bu iřlem řablon eřleřtirme (template matching)⁵ yöntemiyle geręekleřtirilmiř olup, bu teknik sabit karakter yapılarına karřı yüksek başarı saęlamaktadır (Yoshimori vd., 2003:586). Ancak bu yöntem, font farklılıkları, deformasyon ve düşük çözünürlük gibi durumlarda yetersiz kalmaktadır. Bu nedenle daha yeni çalıřmalarda yapay sinir aęları (YSA)⁶ ve k-en yakın komřu (k-NN)⁷ gibi öğrenmeye dayalı yöntemler kullanılmaktadır (Quiros vd., 2017:1087).

Zhuang vd. (2018:306), özellikle derin öğrenme temelli yaklařımlar, plaka tanıma sistemlerinde çıęır açmıřtır. İnsan düzeyine yakın plaka tanıma başarımının ancak konvolüsyonel sinir aęları (CNN) gibi yapılarla mümkün olduęunu ortaya koymuřtur. CNN modelleri, görüntüden çıkarılacak öznitelikleri otomatik olarak

² Binarizasyon: Bir görüntüdeki piksellerin belirli bir eřik deęerine göre iki sınıfa (genellikle siyah ve beyaz) ayrıldıęı, görüntü iřlemede ön iřleme ařaması olarak kullanılan tekniktir.

³ Blob Labeling: Görüntüde birbirine komřu olan ve aynı özellikleri taşıyan piksel gruplarının tespit edilerek her birine benzersiz bir etiket atanmasını saęlayan nesne tanımlama yöntemidir.

⁴ Segmentasyon Teknikleri: Görüntünün anlamlı parçalara bölünmesini amaçlayan, nesne veya bölge tabanlı analizlerin temelini oluřturan görüntü iřleme yöntemleridir.

⁵ Template Matching: Belirli bir řablonun, daha geniř bir görüntü içinde konumunun veya benzer örneklerinin bulunmasını saęlayan, görüntü tanıma temelli bir karřılařtırma teknięidir.

⁶ YSA: İnsan beyninin öğrenme ve karar verme süreçlerini taklit eden, çok katmanlı yapılar üzerinden veri öğrenimi geręekleřtiren hesaplama modelleridir.

⁷ k-NN: Bir verinin sınıfını, en yakın k adet komřusunun sınıflarına bakarak belirleyen, mesafe ölçümüne dayalı bir gözetimli öğrenme algoritmasıdır.

öğrenmekte ve karakter sınıflandırmasında yüksek doğruluk oranlarına ulaşmaktadır. Bu doğrultuda Mask-RCNN⁸ gibi modeller, hem karakterlerin tespiti hem de sınıflandırılmasını aynı ağ yapısı içinde gerçekleştirebilme kapasitesine sahiptir. Bu mimari sayesinde sistem, geleneksel ön işleme adımlarına ihtiyaç duymadan doğrudan görüntüden öğrenim gerçekleştirebilmekte ve segmentasyon başarısını da artırmaktadır.

Plaka tanıma sistemlerinde doğruluk ve işlem süresi bakımından yaşanan zorlukların aşılması amacıyla derin öğrenme tabanlı yaklaşımlara yönelinmiştir. Bu kapsamda, konvolüsyonel sinir ağları⁹ ve transfer öğrenme teknikleri birleştirilerek düşük kaliteli, çeşitli açılardan çekilmiş veya kısmen gizlenmiş plakaların dahi yüksek başarımla tanınabildiği bir model tasarlanmıştır. Geliştirilen sistemin, özellikle yoğun trafikli kentsel alanlarda gerçek zamanlı kullanım için yeterli doğruluk ve hız performansı sunduğu gösterilmiştir (Khan vd., 2022:1408).

Plaka tanıma sistemlerinin uygulama alanları oldukça geniştir. Trafik ihlallerinin tespiti, paralı geçiş sistemleri, otopark yönetimi, araç hırsızlığıyla mücadele ve kamu binalarına giriş kontrolü gibi alanlarda yoğun olarak kullanılmaktadır (Zhou vd., 2012;4269). Ancak bu sistemlerin yaygınlaşması, veri güvenliği ve etik konuları da beraberinde getirmiştir. Özellikle araç dışı görüntülerin de kaydedilebilmesi ve bu verilerin merkezi veri tabanlarında saklanması, kişisel verilerin korunması açısından yeni düzenlemeleri zorunlu kılmaktadır (Çatal, 2019:79).

Plaka tanıma sistemleri, geçmişten günümüze teknik kapasitesini ciddi oranda geliştirmiş, klasik görüntü işleme yöntemlerinden derin öğrenme temelli modellere uzanan bir evrim geçirmiştir. Her bir aşaması – tespit, ayrıştırma ve tanıma – kendi içinde çeşitli zorluklar barındırmakta; bu nedenle sistem tasarımlarında hem geleneksel teknikler hem de modern yapay zekâ yöntemleri birlikte değerlendirilmektedir.

⁸ Mask-RCNN: Görüntüdeki nesnelerin hem sınıflandırılmasını hem de her bir nesneye ait piksel düzeyinde segmentasyon maskesinin çıkarılmasını sağlayan, bölütleme tabanlı bir derin öğrenme mimarisidir.

⁹ Konvolüsyonel Sinir Ağları: Özellikle görüntü verilerinin işlenmesinde kullanılan, konvolüsyon katmanları sayesinde görsel özellikleri hiyerarşik olarak çıkarabilen derin öğrenme tabanlı yapay sinir ağı modelleridir.

2.2.1.4. Araç Takip Sistemi (ATS)

Dijital teknolojilerin hızlı gelişimiyle birlikte, güvenlik ve denetim alanında kullanılan araçlar da dönüşüme uğramıştır. Bu bağlamda Araç Takip Sistemleri (ATS), kamu güvenliği, lojistik yönetimi ve kent içi denetim mekanizmalarının dijitalleşmesinde kilit bir rol üstlenmiştir. ATS, gerçek zamanlı konum bilgisi sağlayarak araçların izlenmesini mümkün kılan, küresel konumlandırma sistemi (GPS), kablosuz iletişim protokolleri, harita servisleri ve veri analiz yazılımlarının bütünleşmiş biçimde çalıştığı çok bileşenli bir teknolojik yapı sunar (Çatal, 2019:82). Dijitalleşmenin hem teknik hem de yönetsel boyutlarının bir araya geldiği ATS sistemleri, yalnızca taşıt konumlandırması değil, aynı zamanda sürücü davranışlarının analizi, rota optimizasyonu ve güvenlik tehditlerinin erken tespiti gibi işlevleri de üstlenmektedir.

Araç Takip Sistemleri, temel olarak donanım ve yazılım bileşenlerinden oluşur. Donanım kısmında, genellikle araçlara monte edilen GPS modülleri, sensörler ve iletişim antenleri yer alırken; yazılım tarafında ise bu verilerin işlendiği merkezi kontrol sistemleri bulunur. Bu yapı sayesinde araçların anlık konumu, hızı, yönü, duraklama süresi gibi bilgiler merkezi bir platforma aktarılır. Özellikle gerçek zamanlı veri analitiği uygulamaları sayesinde, sistem yöneticileri filo performansını anlık olarak izleyebilmekte ve gerektiğinde müdahale edebilmektedir (Anagnostopoulos vd., 2006:382).

ATS'nin dijital dönüşümdeki rolü, dijitalizasyon, dijitalleşme ve dijital dönüşüm kavramlarıyla açıklanabilir. İlk aşama olan dijitalizasyon, analog araç konum bilgilerinin sayısal forma çevrilmesiyle ilgilidir. Örneğin, manuel yolculuk çizelgelerinin yerini GPS verileri almıştır. Bu süreç teknik bir dönüşüm olup bilgi formatının değişimini ifade eder. Ardından gelen dijitalleşme, iş süreçlerinin dijital teknolojilerle yeniden yapılandırılmasıdır. ATS sayesinde güzergâh planlaması, bakım zamanlaması ve sürücü değerlendirmeleri gibi işlemler otomatikleştirilmiştir (Zhou vd., 2012:4270). Son aşama olan dijital dönüşüm ise, ATS'nin kurumsal karar alma mekanizmalarını değiştirecek düzeyde etkili olduğu aşamayı temsil eder. Örneğin, emniyet teşkilatlarının operasyonel stratejilerini veri odaklı yönetmeleri, bu dönüşümün göstergesidir (Çatal, 2019:83).

Araç Takip Sistemleri'nin bir diğer önemli yönü, güvenlik alanındaki kullanımlarıdır. Kolluk kuvvetleri, şüpheli araçların izlenmesi, acil durum müdahaleleri ve sınır güvenliği uygulamalarında ATS'den yararlanmaktadır. Zhuang vd. (2018:310), araç takip verilerinin plaka tanıma sistemleriyle entegre edilerek analiz edildiğinde, suçla mücadelede daha etkili bir istihbarat altyapısı sağlandığını belirtmiştir. Ayrıca, bu sistemler trafik kazalarının analizinde de kullanılmakta; olay öncesi ve sonrası verilerin değerlendirilmesine olanak tanımaktadır.

Teknolojik olarak bakıldığında, ATS sistemleri giderek daha da bütünleşmiş hâle gelmektedir. Yapay zekâ algoritmaları kullanılarak sürücü alışkanlıkları modellenmekte, anomaliler tespit edilmekte ve bu sayede proaktif güvenlik önlemleri alınabilmektedir. Ayrıca, bulut tabanlı sistemler sayesinde farklı şehirler veya kurumlar arasında veri paylaşımı kolaylaşmakta; büyük ölçekli analizler mümkün hâle gelmektedir (Zhou vd., 2012:4272). Bu gelişmeler, ATS'nin yalnızca bir takip aracı değil, aynı zamanda karar destek sistemi olarak konumlanmasına yol açmıştır.

Araç Takip Sistemleri, dijitalleşmenin güvenlik ve ulaşım yönetimi alanındaki en belirgin uygulamalarından biri olarak öne çıkmaktadır. GPS teknolojilerindeki gelişmelerin yapay zekâ temelli veri analitiği ve bulut tabanlı iletişim altyapılarıyla birleşmesi, bu sistemlerin teknik kapasitesini önemli ölçüde artırmıştır. Bununla birlikte, ATS'nin yalnızca teknik işlevleriyle değerlendirilmesi yeterli değildir; sistemin güvenli, etik ve hukuka uygun biçimde işletilmesi temel bir gereklilik olarak görülmektedir. Özellikle sürücülerin sürekli izlenebilirliği, mahremiyet hakkı ve kişisel veri güvenliği bağlamında tartışmalara yol açmakta; kişisel verilerin korunmasına ilişkin düzenlemeler sistemin tasarımını doğrudan şekillendirmektedir. Bu çerçevede veri anonimleştirme, erişim denetimi ve saklama süresi gibi ilkelerin sistem mimarisi içinde yer alması zorunlu hâle gelmektedir (Çatal, 2019:84). Tüm bu unsurlar dikkate alındığında, ATS'nin yalnızca bir izleme aracı değil, aynı zamanda kurumların iş yapma biçimlerini dönüştüren ve dijital çağın güvenlik politikalarının stratejik bileşenlerinden biri hâline geldiği söylenebilir.

2.2.1.5. Mobil Araç Sorgulama Sistemi (MAS)

Güvenlik teknolojilerinin dijitalleşme süreci, kamusal denetimin daha hızlı, etkili ve yaygın biçimde yürütülmesini mümkün kılmıştır. Bu dönüşümün dikkat çeken örneklerinden biri de Mobil Araç Sorgulama Sistemi (MAS) uygulamalarıdır. MAS, sahada görev yapan güvenlik birimlerinin, araçlara ilişkin kimlik, kayıt ve suç geçmişi gibi bilgilere anlık olarak ulaşabilmelerini sağlayan bir dijital sistemdir (Çatal, 2019:85). Bu sistemler, yalnızca operasyonel verimlilik değil, aynı zamanda kamusal güvenliğin korunmasında da kritik rol üstlenmektedir. MAS uygulamaları, dijital teknolojilerin emniyet teşkilatları bünyesindeki etkisini artırarak, hem süreçlerin hızlanmasını hem de hata paylarının düşmesini mümkün kılmaktadır.

Mobil Araç Sorgulama Sistemleri'nin ortaya çıkışı, temelde dijitalizasyon süreciyle başlamıştır. Daha önce elle veya merkezden radyo telsiz aracılığıyla yürütülen plaka ve araç bilgisi sorgulamaları, artık dijital verilerle çalışan mobil cihazlar üzerinden anlık olarak yapılabilmektedir (Akmeşe, 2020:113). Bu durum, araç bilgilerinin sayısal ortama aktarılmasıyla dijitalizasyonun tamamlandığını göstermektedir. Ancak MAS, yalnızca verinin sayısallaştırılmasıyla sınırlı değildir; aynı zamanda güvenlik birimlerinin çalışma yöntemlerini değiştiren bir yapı sunduğundan, dijitalleşme aşamasını da temsil eder.

MAS, veri tabanlarının mobil uygulamalara entegre edilmesiyle çalışır. Polis memurları, tablet ya da mobil terminaller aracılığıyla araç plakalarını sisteme girerek, sahibinin kimlik bilgilerine, sigorta durumu, muayene bilgisi, çalıntı kaydı gibi birçok veriye saniyeler içinde ulaşabilirler. Bu süreç, merkezi veri tabanlarının mobil cihazlara uyarlanması, uygulama arayüzlerinin kullanıcı dostu hâle getirilmesi ve şifreli iletişim protokollerinin sağlanması gibi çok boyutlu dijitalleşme adımlarını içerir (Bozkurt vd., 2021:37).

Dijital dönüşüm ise MAS'ın, yalnızca teknik değil, yapısal bir değişim yaratmasıyla ilgilidir. Bu sistem sayesinde polislik uygulamalarında karar alma süreçleri daha veriye dayalı hâle gelmiş, bireysel inisiyatiften çok algoritmik denetim öne çıkmıştır. Böylece MAS, kurumsal organizasyonun yapısını dönüştürerek, dijital dönüşümün karakteristiğini sergilemektedir (Çelik, 2023:75). Buna ek olarak, MAS

gibi sistemler yalnızca bilgiye erişimi hızlandırmakla kalmamakta, aynı zamanda suç önleme stratejilerinin şekillendirilmesinde de etkili olmaktadır (Ekinci, 2011:92).

MAS, özellikle şehir merkezlerinde sıklaşan güvenlik kontrollerinde, araçların kriminal geçmişinin hızla tespit edilmesi, aranan şahısların yakalanması, kaçakçılık faaliyetlerinin engellenmesi gibi çok çeşitli alanlarda kullanılmaktadır. Bu bağlamda, araç plakalarının anlık olarak sorgulanması, plaka tanıma sistemleri (PTS) ile entegre çalışarak sahada gerçek zamanlı karar destek imkânı sunar (Zhuang vd., 2018:312). Ayrıca, MAS sistemleri üzerinden elde edilen veriler, merkezî veri analiz sistemlerine entegre edilerek suç örüntülerinin tespitinde kullanılmaktadır (Bülbül, 2019:66).

Ancak MAS sistemlerinin yaygınlaşması, bazı etik ve hukuki sorunları da beraberinde getirmiştir. Özellikle kişisel verilerin korunması açısından, araç sahibiyle ilişkilendirilen bilgilerin erişim sınırlarının net tanımlanması, yetkisiz erişimlerin önlenmesi ve veri saklama sürelerinin belirlenmesi gibi konular gündeme gelmektedir (Ün, 2022:421). Dijital teknolojilerin güvenlik politikalarında artan kullanımı, kamusal güvenlik ile bireysel özgürlükler arasındaki dengeyi daha karmaşık ve hassas bir hâle getirmektedir. Bu durum, özellikle Mekânsal Adli Sistemler (MAS) gibi ileri düzey dijital gözetim araçlarının tasarımında, yalnızca teknik işlevselliğin değil; aynı zamanda etik denetim mekanizmalarının da sistematik biçimde gözetilmesini zorunlu kılmaktadır. Bireyin mahremiyetini tehdit edebilecek müdahale biçimlerinin önüne geçilmesi ve toplumsal meşruiyetin sağlanması adına, bu tür teknolojik çözümlerin şeffaf, hesap verebilir ve hak temelli bir yaklaşımla yapılandırılması gerekmektedir (Hayta, 2021:931, 934–935).

Mobil Araç Sorgulama Sistemleri, dijital çağın güvenlik stratejilerinde önemli bir yer edinmiştir. Sahadaki güvenlik personelinin araçlara dair bilgilere hızlı ve doğru biçimde ulaşmasını sağlayan bu sistemler, dijitalizasyon, dijitalleşme ve dijital dönüşüm süreçlerini somut bir örnekle ortaya koymaktadır. MAS uygulamaları, yalnızca teknolojik bir yenilik değil, aynı zamanda kurumsal işleyişi yeniden biçimlendiren bir dönüşüm aracıdır. Bununla birlikte, veri güvenliği ve bireysel mahremiyetin korunması konularında geliştirilmesi gereken yönleri de mevcuttur. Gelecekte MAS sistemlerinin, yapay zekâ ve büyük veri analizleriyle daha da bütünleşmiş hâle gelmesi beklenmekte; bu da kamu güvenliğinin dijitalleşme sürecinde yeni bir evreye işaret etmektedir.

2.2.1.6. Muhtarlık Otomasyon Sistemi (MOS)

Kamu yönetiminde dijital teknolojilerin artan rolü, yerel yönetim birimlerinin yeniden yapılandırılmasını zorunlu hale getirmiştir. Bu dönüşümün temelinde dijitalleşme ve buna bağlı uygulamalar yatmaktadır. Türkiye’de muhtarlık kurumu, yerel yönetimlerin en alt düzeydeki temsilcisi olarak, dijital kamu hizmetleriyle entegre edilmesi gereken önemli bir yapıdır. Bu bağlamda, İçişleri Bakanlığı tarafından geliştirilen *Muhtarlık Otomasyon Sistemi (MOS)*, muhtarlıkların kurumsal işleyişini çağın gereklerine uygun hale getirmek amacıyla geliştirilmiştir. Sistem, hem devlet ile muhtarlar arasındaki bilgi akışını kolaylaştırmakta hem de kamu hizmetlerinin daha etkin, hızlı ve denetlenebilir bir biçimde yürütülmesini amaçlamaktadır. MOS’un potansiyel olarak bu dönüşüme öncülük etmesi hedeflenmektedir.

MOS, muhtarların taleplerini, önerilerini ve şikâyetlerini doğrudan iletebildiği bir platform sunmakta ve valilik ile belediyelere bu iletileri hızlı şekilde aktararak geri bildirim sürecini kısaltmaktadır (T.C. İçişleri Bakanlığı, 2015). Bunun yanında, muhtarların görev alanlarına ilişkin bilgi ve belgeleri tek bir sistem üzerinden yürütebilmeleri, bürokratik işlemlerde zaman ve kaynak tasarrufu sağlamaktadır. Ancak bu yapının sürdürülebilirliği, sadece teknik altyapı ile değil, aynı zamanda kullanıcıların dijital okuryazarlığı ve kurumsal destekle mümkündür (Yıldırım ve Öner, 2004:49).

Burdur ili Gölhisar ilçesinde yapılan araştırmada (Koç, Gündoğar ve Teke, 2023:9), muhtarların büyük çoğunluğunun MOS’u ya hiç kullanmadığı ya da sınırlı şekilde kullandığı görülmektedir. Kullanım oranının düşük olması, birkaç temel nedene dayanmaktadır: birincisi, kırsal bölgelerde internet altyapısının yetersiz oluşu; ikincisi, muhtarların çoğunlukla ilkököl ve ortaokul mezunu olmaları nedeniyle dijital uygulamalara yabancı olmaları; üçüncüsü ise sistemden alınan geri dönüşlerin yetersizliği nedeniyle motivasyon eksikliğidir. Bu durum, sistemin teknik olarak var olmasının yeterli olmadığını, kullanıcı deneyimi ve memnuniyetinin de dijital dönüşümde belirleyici olduğunu göstermektedir (Çukurçayır, 2012:142).

MOS, teknik olarak mobil uygulamalarla desteklenmiş, Android ve iOS işletim sistemlerinde çalışabilir bir formda tasarlanmıştır. Ancak teknolojik araçların varlığı,

onların etkili kullanımı anlamına gelmemektedir. Gölhisar örneğinde olduğu gibi, sistemin kapsayıcılığı donanım, yazılım ve insan kaynağı açısından eşgüdümlü bir şekilde düşünülmelidir. Muhtarların bireysel sosyal medya hesapları üzerinden iletişim kurması, MOS'un kurumsal anlamda yeterince benimsenmediğini de ortaya koymaktadır (Koç, 2018:89). Bu durum, teknolojinin sadece varlığıyla değil, aynı zamanda kültürel ve yönetsel kabullerle desteklenmesi gerektiğini göstermektedir.

Sonuçta, MOS, Türkiye'de yerel yönetim sisteminin dijital dönüşüm hedeflerine ulaşmasında önemli bir adımdır. Ancak sistemin etkili ve yaygın kullanımı, sadece teknik altyapının iyileştirilmesiyle değil, aynı zamanda muhtarların dijital becerilerinin geliştirilmesi ve sistemin işlevselliğinin artırılmasıyla mümkündür. MOS'un başarıya ulaşabilmesi için kullanıcı merkezli bir yaklaşım benimsenmeli; muhtarların yaş, eğitim ve bölgesel koşulları göz önünde bulundurularak eğitim programları, teknik destek ve sistemsal geri bildirim mekanizmaları güçlendirilmelidir. Aksi halde, bu tür dijitalleşme hamleleri yalnızca yüzeyde kalacak ve kamu hizmetlerinde eşitsizlikleri artıracaktır. Yerel hizmetlerin kalitesini artırmak ve kamu yönetiminde katılımı desteklemek için MOS gibi sistemlerin geliştirilerek, işlevsel hale getirilmesi kritik öneme sahiptir.

2.3. Türkiye'de Dijital Güvenlik Sistemlerinin Evrimi

Bu kısımda, Türkiye'de dijital güvenlik sistemlerinin geçirdiği dönüşüm süreci çok yönlü bir yaklaşımla ele alınacaktır. Öncelikle, hukuki ve kurumsal çerçeve üzerinden dijital güvenlik altyapısının yasal temelleri incelenecek; ardından, dijitalleşme sürecinde benimsenen güvenlik politikaları değerlendirilecektir. Son olarak, KGYS ve MOBESE sistemlerinin entegrasyon süreci mercek altına alınarak, Türkiye'de dijital güvenlik yönetiminin kurumsal evrimi kapsamlı biçimde ortaya konacaktır.

2.3.1. Dijitalleşmede Güvenlik Politikaları: Hukuki ve Kurumsal Çerçeve

Türkiye'de dijitalleşme süreci, yalnızca teknolojik altyapıların dönüşümü ile sınırlı kalmamış; aynı zamanda güvenlik, mahremiyet ve temel haklara ilişkin sorunların hukuki ve kurumsal düzenlemelerle ele alınmasını da beraberinde getirmiştir. Dijital güvenlik, teknik yönünün ötesinde toplumsal, yönetsel ve hukuksal

katmanlarıyla çok boyutlu bir politika alanı hâline gelmiştir. Özellikle 2000’li yıllardan itibaren, uluslararası normlarla uyumlu bir dijital güvenlik altyapısı inşa edilmeye çalışılmış; bu kapsamda çıkarılan yasalar, oluşturulan kurumlar ve geliştirilen strateji belgeleri, dijitalleşmenin güvenlik boyutunu şekillendirmiştir.

Bu çerçevede, Türkiye’de dijital güvenlik alanındaki en temel düzenlemelerden biri 2007 yılında yürürlüğe giren 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” olmuştur. Bu yasa, çevrimiçi suçlara karşı koruyucu önlemler getirmiş ve içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcı gibi yeni sorumluluk alanları tanımlamıştır (Erdoğan, 2021:73). Yasa ile birlikte kurulan Bilgi Teknolojileri ve İletişim Kurumu (BTK), internet içeriklerinin denetiminde ve erişimin engellenmesinde merkezi bir aktör hâline gelmiştir.

Kurumsal yapılanma açısından dijital güvenlik yalnızca BTK ile sınırlı kalmamış; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Siber Suçlarla Mücadele Daire Başkanlığı gibi kurumlar aracılığıyla çok katmanlı bir yapıya kavuşmuştur. Bu kurumlar hem önleyici hem de müdahale edici roller üstlenerek dijital suçlarla mücadelede önemli görevler icra etmektedir (Çukurçayır, 2012:136). Ancak bu çok başlı yapı, zaman zaman yetki karmaşasına ve koordinasyon sorunlarına yol açabilmektedir.

2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu (KVKK), dijital güvenliğin hak temelli yönünü güçlendirmiştir. Kanun, kişisel verilerin işlenmesini rızaya dayalı hâle getirmiş ve bu alanda bireylere koruyucu bir hukuki çerçeve sunmuştur. Kanunla kurulan Kişisel Verileri Koruma Kurumu, hem kamu hem de özel sektörde denetleyici bir rol üstlenmiştir. Ancak uygulamada kurumun etkisinin sınırlı kaldığı, özellikle büyük teknoloji şirketlerinin veri toplama ve işleme pratiklerinin yeterince denetlenemediği yönünde eleştiriler gündeme gelmiştir (Koç, 2018:90).

Türkiye’de dijital güvenlik politikalarının bir diğer boyutu siber güvenlik stratejileri olmuştur. Siber saldırıların yalnızca bireyleri değil, kamu kurumlarını ve kritik altyapıları hedef alması üzerine, Türkiye Siber Güvenlik Stratejisi ve Eylem Planı gibi belgeler hazırlanmıştır (Demirel, 2021). Bu belgeler, dijital güvenliği ulusal güvenlik meselesi olarak ele almış; ancak somut uygulama mekanizmalarının eksikliği

nedeniyle sıklıkla temenni düzeyinde kaldığı eleştirileri yapmıştır (Yıldırım ve Öner, 2004:51).

Uluslararası gelişmelerin de Türkiye'deki dijital güvenlik politikaları üzerinde etkisi olmuştur. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemeler, iç hukukta ve uygulamalarda önemli ölçüde yönlendirici olmuştur. Bununla birlikte, bazı akademik çevrelerde Batı merkezli normların yerel ihtiyaçlara göre uyarlanması gerektiği yönünde tartışmalar gündeme gelmiştir (Şahin ve Korkmaz, 2021:65).

Genel olarak değerlendirildiğinde, Türkiye'nin dijital güvenlik politikaları, dijitalleşmenin hızına yetişmeye çalışan bir nitelik taşımaktadır. Hukuki düzenlemeler çoğunlukla reaktif şekilde, yani sorunlar ortaya çıktıktan sonra hayata geçirilmiş; kurumsal yapı ise çok aktörlü fakat dağınık bir karakter göstermiştir. Gelecekte daha etkin bir dijital güvenlik politikası için, normatif çerçevenin güçlendirilmesine, kurumlar arası iş birliğinin artırılmasına ve kamuoyunun dijital farkındalığının geliştirilmesine ihtiyaç duyulmaktadır.

2.3.2. KGYS ve MOBESE Sistemlerinin Entegrasyon Süreci

Dijital dönüşüm, kamu güvenliği alanında önemli yapısal değişimlere yol açmıştır. Türkiye'de kent güvenliği ve kamu düzeninin sağlanmasında etkin rol oynayan MOBESE (Mobil Elektronik Sistem Entegrasyonu) ve KGYS gibi dijital sistemlerin entegrasyonu, güvenlik hizmetlerinin dijitalleşmesinin en somut örneklerinden birini oluşturmaktadır. Bu süreç, hem teknolojik gelişmelere hem de güvenlik stratejilerindeki paradigmatik değişimlere bağlı olarak şekillenmiştir.

MOBESE, 2000'li yılların başında suçla mücadele, olaylara hızlı müdahale ve kent genelinde izleme kapasitesinin artırılması amacıyla devreye alınmıştır. Ancak sınırlı altyapısı ve yerel farklılıkları nedeniyle sistem, zamanla bütünlük ve koordinasyon açısından yetersiz kalmıştır (Erdoğan, 2021:75). Bu eksiklikleri gidermek amacıyla geliştirilen KGYS, yalnızca görüntüleme değil; haberleşme, plaka tanıma, veri analizi ve karar destek mekanizmalarını içeren çok katmanlı bir yapıyla öne çıkmıştır. İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü koordinasyonunda 2008

sonrası dönemde yaygınlaştırılan KGYS, zamanla MOBESE bileşenlerini de bünyesine dâhil etmiştir (Kocaoğlu, 2017).

Bu entegrasyon sürecinde, MOBESE'nin görüntüleme odaklı yapısı KGYS'nin çok yönlü dijital altyapısıyla birleştirilmiş; anlık veri toplama, analiz ve karar verme süreçleri hızlandırılmıştır. Plaka Tanıma Sistemi (PTS), yüz tanıma teknolojileri ve Coğrafi Bilgi Sistemleri (CBS) gibi ileri düzey uygulamaların sisteme entegre edilmesiyle güvenlik kapasitesi önemli ölçüde genişlemiştir (Demirel, 2021).

Dijital dönüşüm bağlamında, entegrasyon yalnızca teknik bir adaptasyon değil; aynı zamanda kurumsal işleyişin dönüşümü olarak da değerlendirilmelidir. Analog görüntüleme sistemlerinden dijital altyapıya geçiş, verilerin analiz edilebilir hâle getirilmesi ve bu verilerin karar destek sistemleri aracılığıyla yönetsel süreçlere dâhil edilmesi, sürecin temel evrelerini oluşturmuştur (Yıldız, 2020:113).

Bununla birlikte, entegrasyon süreci etik ve toplumsal tartışmaları da beraberinde getirmiştir. Özellikle mahremiyet, veri güvenliği ve şeffaflık konuları kamuoyunda gündeme gelmiş; demokratik denetimden uzak işleyişin bireysel özgürlükler üzerinde potansiyel tehditler yaratabileceği dile getirilmiştir (Şahin ve Korkmaz, 2021:68). Bu nedenle entegrasyonun yalnızca teknik değil, aynı zamanda etik ve hukuksal boyutlarıyla da ele alınması gerektiği açıktır.

Sonuç olarak, KGYS ve MOBESE sistemlerinin entegrasyonu, Türkiye'de dijital güvenlik politikalarının kurumsallaşma sürecinde bir dönüm noktası olmuştur. Görüntüleme temelli güvenlik anlayışından, veri odaklı ve stratejik güvenlik yönetimine geçişin önünü açan bu dönüşüm; gelecekte daha şeffaf, hesap verebilir ve hak temelli güvenlik yaklaşımlarını zorunlu kılmaktadır.

BÖLÜM III

KENT GÜVENLİĞİ UYGULAMALARINA YÖNELİK SAHA ARAŞTIRMASI

3.1. Araştırmanın Amacı, Kapsamı ve Yöntemi

Bu bölümde, kent güvenliği uygulamalarına yönelik olarak yürütülen saha araştırmasının kapsamı, yöntemi ve elde edilen bulgular ayrıntılı biçimde ele alınacaktır. İlk aşamada, araştırmanın amacı, yöntemi ve veri toplama süreci açıklanacak; ardından, MAXQDA yazılımı kullanılarak gerçekleştirilen nitel veri analiz süreci adım adım ortaya konacaktır.

Ayrıca, Kütahya il merkezinde gerçekleştirilen ikili görüşmelere dayalı olarak, dijital güvenlik sistemlerine yönelik toplumsal algılar ve uygulama sürecinde karşılaşılan sorunlar nitel bir çerçevede ele alınacaktır. Son bölümde ise, ulaşılan bulgular derinlemesine yorumlanarak, mevcut literatürle karşılaştırmalı biçimde çok yönlü bir değerlendirmeye tabi tutulacaktır.

3.1.1. Araştırmanın Amacı ve Önemi

Bu çalışmada, kent güvenliğinin sağlanmasında dijital teknolojilerin artan rolünü anlamak ve özellikle KGYS çerçevesinde bu sistemlerin nasıl algılandığı, kullanıldığı ve değerlendirildiği üzerine kapsamlı bir analiz sunulması amaçlanmaktadır. Dijitalleşme çağında gözetim sistemlerinin güvenlik politikaları bu araştırmanın merkezinde yer almaktadır. Özellikle dijital gözetim teknolojilerinin polis memurları tarafından nasıl kullanıldığı, araştırmanın temel sorunsalını oluşturmaktadır.

Bu bağlamda, çalışmanın bilimsel katkısı, dijital güvenlik sistemlerinin yalnızca teknik boyutuyla değil, aynı zamanda sosyo-kültürel, yönetsel ve etik etkileriyle değerlendirilmesini sağlayarak, dijitalleşmenin kent güvenliği pratiklerini nasıl dönüştürdüğünü ortaya koymasıdır (Koç, 2018:91). Yönetsel açıdan, dijital güvenlik sistemlerinin uygulayıcılar (polis memurları) üzerindeki etkileri, iş yükü, karar alma mekanizmaları ve dijital veriyle çalışma biçimleri üzerinden analiz edilerek, uygulama süreçlerine dair eleştirel bir perspektif sunulmuştur. Toplumsal düzeyde ise, bireylerin mahremiyet algısı, güvenlik ile özgürlük arasındaki dengeyi

nasıl yorumladıkları ve bu sistemlere ne düzeyde dâhil oldukları sorgulanarak, dijital vatandaşlık kavramına katkı sağlanması hedeflenmiştir.

Araştırmada, literatürde çoğunlukla teknik yönleriyle ele alınan Kent Güvenlik Yönetim Sistemi'nin (KGYS), bireylerin öznel deneyimleri ve toplum nezdindeki algısal yansımaları çerçevesinde değerlendirilmesi hedeflenmiştir. Bu yönüyle çalışma, dijital güvenlik sistemleri üzerine var olan teknik merkezli çalışmalardan farklılaşarak, insan merkezli bir yaklaşım sunmaktadır.

3.1.2. Veri Toplama Yöntemleri ve Katılımcı Profili

Bu araştırma kapsamında, nitel araştırma desenlerinden “fenomenolojik¹⁰” yaklaşım benimsenmiş ve veri toplama sürecinde yarı yapılandırılmış derinlemesine görüşmeler temel yöntem olarak tercih edilmiştir. Görüşmelerin tümü, Kütahya il merkezinde görev yapan polis memurlarıyla, yüz yüze gerçekleştirilmiştir. Görüşme tekniği olarak ikili görüşmeler uygulanmış, her bir görüşme belirli bir soru formuna bağlı kalınarak yapılandırılmıştır.

Bu araştırmada, KGYS'ye ilişkin deneyimlerin ve algıların derinlemesine incelenebilmesi amacıyla, 20 polis memuruyla yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Katılımcıların belirlenmesinde amaçlı örnekleme yöntemi tercih edilmiş; özellikle yaş, eğitim düzeyi, görev birimi, cinsiyet ve mesleki kıdem gibi değişkenlerde çeşitlilik sağlanmasına dikkat edilmiştir. Katılımcılar, önleyici hizmetler, asayiş, trafik ve karakol gibi farklı operasyonel birimlerde görev yapmakta olup, bu durum araştırmanın çoklu perspektifler içermesini mümkün kılmıştır.

Görüşme formu, toplamda 22 sorudan oluşmaktadır. Bu soruların 17'si nitel veri toplamaya yönelik açık uçlu sorulardan, 5'i ise katılımcıların yaş, eğitim durumu, hizmet süresi, görev birimi ve cinsiyet bilgilerini kapsayan demografik niteliktedir.

Görüşmeler, her bir katılımcının açık rızası doğrultusunda, gizlilik esaslarına uygun biçimde dijital ses kayıt cihazı aracılığıyla kaydedilmiş; daha sonra bu kayıtlar

¹⁰ **Fenomenoloji:** Kökeni Edmund Husserl'in felsefi yaklaşımına dayanan fenomenoloji, bireylerin yaşantılarını ve bu yaşantılara yükledikleri anlamları öznel bir perspektiften incelemeyi amaçlayan bir felsefi ve bilimsel yöntemdir. Temel amacı, bireylerin deneyimlerini olduğu gibi betimleyerek, olguların özünü (fenomenlerin özsel yapısını) açığa çıkarmaktır. Nitel araştırmalarda, katılımcıların yaşadıkları deneyimlerin anlamını derinlemesine analiz etmeyi ve bu deneyimlerin ortak yönlerini ortaya koymayı hedefleyen bir yaklaşım olarak kullanılmaktadır.

doğrudan transkript yöntemi ile yazılı hâle getirilmiştir. Görüşme süreleri, katılımcıların yanıtlarının kapsamına göre değişiklik göstermiş; bu süreler 10 ile 25 dakika arasında farklılık göstermiştir. Ortalama görüşme süresi ise yaklaşık 20 dakikadır.

Elde edilen nitel veriler, MAXQDA 2022 nitel veri analiz yazılımı aracılığıyla çözümlenmiştir. Analiz sürecinde içerik analizi yöntemi benimsenmiş; ilk aşamada veriler üzerinden açık kodlama gerçekleştirilmiş, sonrasında ise bu kodlar temalar ve alt temalar etrafında anlamlı gruplar hâline getirilerek kavramsal bir çerçeve oluşturulmuştur.

Araştırmanın bulguları yalnızca tematik düzeyde frekans analizleriyle değil, aynı zamanda katılımcıların kendi ifadelerinden yapılan doğrudan alıntılar ile desteklenmiştir. Bu yaklaşım sayesinde, hem verilerin sayısal temsiliyeti korunmuş, hem de elde edilen nitel verilerin derinliği ortaya çıkarılmıştır. Katılımcılar, etik ilkelere uygun şekilde K1, K2... K20 şeklinde kodlanarak anonimleştirilmiş, böylece hem mahremiyet korunmuş hem de her görüşün özgünlüğü muhafaza edilmiştir.

Bu metodolojik yapı sayesinde, dijital güvenlik sistemlerine ilişkin algıların yalnızca istatistiksel bir temsille değil; aynı zamanda bireysel deneyim ve algılar ışığında çok boyutlu biçimde anlaşılması hedeflenmiştir.

3.1.3. Sınırlılıklar

Bu araştırmanın bulguları, belirli mekânsal, zamansal ve yöntemsel çerçevelerle sınırlandırılmıştır. Çalışma yalnızca Kütahya il merkezi sınırlarında gerçekleştirilmiş olup, elde edilen veriler bu yerel bağlama özgü sosyal, yönetsel ve kültürel dinamikler ışığında değerlendirilmiştir. Dolayısıyla, bulguların daha geniş ölçekli kentsel yapılar veya farklı sosyo-kültürel çevrelerle doğrudan genellenebilirliği sınırlıdır.

Araştırmada veri toplama aracı olarak nitel görüşme tekniği benimsenmiş ve yalnızca polis memurları (20 kişi) ile derinlemesine görüşmeler yapılmıştır. Sayıca sınırlı olan bu örneklem, çalışmanın nitel doğasına uygun olmakla birlikte, tüm yerel toplumu temsil etme iddiası taşımamaktadır.

Yapılan görüşmeler 2025 Yılı Haziran ayı içerisinde gerçekleştirilmiştir. Bu durum, elde edilen verilerin döneme özgü politik, teknolojik veya güvenlik uygulamalarındaki değişkenlikten etkilenme olasılığını beraberinde getirmektedir. Ayrıca, görüşmelerin tamamı yüz yüze yapılmış olup, katılımcıların yanıtlarında sosyal kabul görme isteği ya da kurumsal baskı hissi gibi faktörlerin etkili olabileceği göz önünde bulundurulmalıdır.

Yöntemsel açıdan, MAXQDA yazılımı ile kodlanan görüşme verileri üzerinden tematik analiz gerçekleştirilmiş; ancak bu analiz, yorumlayıcının öznel değerlendirme sürecine bağlı olarak şekillenmiştir. Dolayısıyla, araştırma sonuçlarında sınırlı da olsa yorumlayıcı yanlılığı olasılığı mevcuttur.

Son olarak, çalışma kapsamında yalnızca KGYS uygulamaları üzerine odaklanılmış; diğer dijital güvenlik araçları (ör. mobil devriye uygulamaları, sosyal medya analiz sistemleri vb.) kapsam dışı bırakılmıştır. Bu da dijital güvenlik alanındaki bütüncül değerlendirmelerin kapsamını sınırlayan bir başka unsur olarak değerlendirilmelidir.

3.2. MAXQDA Yazılımı ile Nitel Veri Analizi

Günümüzde toplumsal gerçekliğin katmanlı yapısını anlamlandırmak adına başvurulan yöntemlerden biri olan nitel araştırma, artık yalnızca kelimelerle değil, yazılım temelli destekleyici araçlarla da yürütülmektedir. Bu bağlamda, araştırmacılara veri üzerinde bütüncül bir kontrol ve analitik esneklik sunan yazılımların başında MAXQDA gelmektedir. Söz konusu yazılım, hem klasik nitel veri analizinde hem de karma yöntem tasarımlarında araştırma süreçlerini derinleştirme potansiyeline sahiptir (Guetterman ve James, 2023).

Nitel veri analizinin özünde, verinin bağlamsal anlamlarının ortaya çıkarılması ve tematik örüntülerin keşfedilmesi yer alır. Ancak özellikle geniş hacimli veri setleriyle çalışıldığında, araştırmacının analitik sezgisine dayalı olarak elle yürütülen analizler yetersiz kalabilmektedir. İşte bu noktada, MAXQDA gibi yazılımlar, verinin sistematik biçimde kodlanmasını, kategorilere ayrılmasını ve ilişkilendirilmesini mümkün kılar. Kod sistemleri, araştırmacının kavramsal çerçevesiyle eşgüdümlü biçimde yapılandırılabilir ve böylece teori-inşa süreci daha sağlam bir temele oturtulabilir (Bazeley, 2018:345).

MAXQDA'nın sunduğu etkileşimli alıntı matrisi (Interactive Quote Matrix) özelliği, araştırmacıya yalnızca kod frekanslarını göstermekle kalmaz; aynı zamanda hangi gruba ait katılımcının ne söylediğini doğrudan görselleştirerek, karma yöntem yaklaşımında meta-çıkarma üretimini kolaylaştırır (Guetterman ve James, 2023). Bu yaklaşım, nitel verilerin yalnızca betimlenmesiyle sınırlı kalınmaksızın, anlam katmanlarının derinlemesine çözümlenmesini ve veriler arasında içsel bir etkileşim kurulmasını mümkün kılmaktadır. Bu sayede, katılımcı anlatıları arasında anlamlı bağlar oluşturularak daha bütüncül ve rafine yorumlara ulaşılabilmektedir.

Yazılımın bir diğer önemli yönü, araştırma sürecini tekrarlanabilir ve şeffaf bir hale getirmesidir. Kodlama süreçlerinin dijital olarak izlenebilir olması, araştırma etiği açısından da belirleyici bir unsurdur. Zira analiz sürecinin belgelenirliği, özellikle hakemli dergilerde yapılan değerlendirmelerde güvenilirliğin temelidir (Kuckartz ve Rädiker, 2021:542). Öte yandan, bazı eleştiriler de yazılımın araştırmacının sezgisel analiz yetisini bastırabileceği yönündedir. Ancak bu eleştiriler, yazılımın bilinçli ve yaratıcı bir şekilde kullanılmadığı durumlar için geçerlidir. Nitel analiz her zaman araştırmacının kavrayışıyla şekillenir; yazılım ise bu süreci hızlandıran ve düzenleyen bir araçtır, yerini alan değil.

Sonuç olarak, MAXQDA'nın sunduğu araçlar, yalnızca teknik bir kolaylaştırma değil, aynı zamanda analitik bir düşünme biçimi de sunmaktadır. Yazılım aracılığıyla yürütülen nitel veri analizi, hem yapısal şeffaflık hem de analitik derinlik açısından araştırmalara yeni bir soluk getirmektedir. Ancak burada belirleyici olan, yazılımın ne kadar gelişmiş olduğundan çok, araştırmacının epistemolojik tutumu ve analitik merakıdır.

3.3. Analiz Sonuçları ve Raporlama Süreci

Nitel araştırmalar kapsamında yürütülen analiz süreçlerinin güvenilir ve anlamlı sonuçlar üretebilmesi, yalnızca teknik doğruluğa değil; aynı zamanda düşünsel bütünlüğün sistematik biçimde sürdürülmesine bağlıdır. Bu bağlamda, verilerin çok katmanlı yapısının dikkatle çözümlenmesi ve elde edilen bulguların kavramsal bir zeminde yorumlanması hedeflenmektedir. MAXQDA yazılımı ise, özellikle temalar, kodlamalar ve doğrudan alıntılar üzerinden gerçekleştirilen derinlemesine analizlerde araştırmacıya önemli bir işlevsellik sunmaktadır (Guetterman ve James, 2023).

Raporlama Sürecinde Anlamın Yapılandırılması: Analiz bulgularının yalnızca betimleyici bir şekilde sunulması yeterli değildir; elde edilen verilerin hangi bağlamlarda ne tür anlamlar ürettiği, bu anlamların katılımcı deneyimleriyle nasıl örtüştüğü ve araştırma sorularına nasıl yanıt verdiği açık biçimde ortaya konulmalıdır. Bu çerçevede raporlama süreci, yalnızca kodların ya da temaların sıralanması değil; aynı zamanda bu unsurların etkileşimli biçimde yeniden yapılandırıldığı bir yorumlama alanıdır (Creswell ve Poth, 2018).

Entegrasyonun Katmanlılığı - Veriler Arası Diyalog: Nitel ve nicel veriler arasında sağlıklı bir entegrasyon sağlandığında, analiz süreci çok daha güçlü bir teorik çerçeveye kavuşmaktadır. MAXQDA'nın "Interactive Quote Matrix" ve "Joint Display" gibi araçları, nicel bulgularla nitel anlatılar arasında diyalogu olanaklı kılmakta; böylelikle araştırmacıya meta-çıkarımlar üretme fırsatı sunmaktadır (Guetterman vd., 2015).

Eleştirel ve Refleksif Yaklaşımın Gerekliliği: Analiz süreci boyunca elde edilen sonuçların "mutlak" olarak sunulmasından kaçınılmalı; yorumlar, bağlamsal koşullarla ve katılımcı ifadeleriyle desteklenmelidir. Bu noktada eleştirel bir refleksiyonla, araştırmacının kendi pozisyonunu ve olası önyargılarını gözden geçirmesi, analiz sonuçlarının geçerliliğini artıracaktır (Saldaña, 2021).

Yapılandırılmış ve Şeffaf Bir Sunum Dili: Elde edilen bulguların okuyucuya aktarıldığı raporlama aşamasında, açıklık ve sistematiklik en temel ilkeler arasında yer almaktadır. Her bir tema, hem teorik çerçevesiyle hem de temsil gücü yüksek alıntılarla desteklenerek sunulmalı; okuyucunun analiz sürecini adım adım takip edebilmesi sağlanmalıdır. Bu bağlamda temalar, alt temalar, katılımcı görüşleri ve kod frekansları ayrı başlıklar altında detaylandırılmalı, her veri kümesinin özgün katkısı açık biçimde ortaya konulmalıdır.

3.3.1. Temalar ve Alt Temalar

Veri analiz süreci boyunca elde edilen bulguların yapılandırılması süreci, yalnızca içerik temelli bir sınıflandırma pratiği olmanın ötesinde, araştırmacının teorik arka planı ve metodolojik yönelimiyle doğrudan ilişkilidir. MAXQDA yazılımı üzerinden yürütülen nitel veri analizi kapsamında, temalar ve alt temalar çok katmanlı

bir biçimde oluşturulmuş; her bir tematik yapı, katılımcı görüşlerinin yoğunlaştığı anlam kümeleri temel alınarak inşa edilmiştir.

1. Dijital Sisteme Yönelik Algı: Bu ana tema altında, KGYS'nin dijital bir güvenlik sistemi olarak mesleki yaşama entegrasyonu ve polislerin teknolojiye yönelik tutumları irdelenmiştir. Katılımcıların önemli bir kısmı, dijitalleşmenin mesleki rutinlere hız ve verimlilik kazandırdığını belirtirken; bazı ifadelerde sistemin soğuk, mekanik ve insan temasını azaltan yönlerine dikkat çekilmiştir. Bu noktada, “uyum sağlama” ve “eleştirel mesafe” kavramları temanın alt başlıklarını oluşturmuştur.

Alt Tema: Uyum Sağlama Eğilimi: Polis memurlarının önemli bir kısmı, teknolojik sistemleri mesleki işleyişin ayrılmaz bir parçası olarak görmektedir. Bu durum, dijitalleşme ile kurulan faydacı ilişkiyi ve operasyonel kolaylık beklentisini yansıtmaktadır.

Alt Tema: Eleştirel Mesafe ve Duygusal Yabancılaşma: Bazı katılımcılar ise sistemin insanî dokunuşu azaltan yapısından duydukları rahatsızlığı dile getirmiştir. Bu görüşler, mesleki aidiyet ve etik değerlere ilişkin daha derin bir sorgulamayı beraberinde getirmiştir.

2. Sistemin Etkinliği ve İşlevselliği: Bu tema altında KGYS'nin günlük görevlerin yerine getirilmesindeki pratik katkıları ve sistemsel kısıtları ele alınmıştır. Katılımcı ifadeleri, sistemin caydırıcılık, delil toplama, olay takibi gibi yönlerden önemli bir işlev gördüğünü ortaya koymaktadır.

Alt Tema: Operasyonel Verimlilik ve Hız: KGYS'nin olaylara müdahale süresini kısaltması ve olayların dijital olarak izlenebilmesi, sistemin operasyonel değerine işaret eden temel unsurlar arasında yer almıştır.

Alt Tema: Teknik Aksaklıklar ve İş Yükü Artışı: Buna karşın, sistemin zaman zaman işlevsel sınırlarla karşılaştığı, teknik hataların görev sürecini aksattığı ve memurlar üzerinde ek yük oluşturduğu yönünde eleştirel görüşler de sıkça dile getirilmiştir.

3. İletişim ve Denetim Bağlamında Sistem: Katılımcıların büyük bir bölümü, KGYS'nin yalnızca güvenlik sağlamakla kalmadığını, aynı zamanda vatandaşlarla kurulan iletişimi ve denetim süreçlerini dönüştürdüğünü ifade etmiştir.

Alt Tema: Vatandaşla İlişkide Görünürlük ve Hesap Verebilirlik: Kameraların varlığı, bazı memurlar tarafından kamuya karşı daha dikkatli bir davranış sergilenmesine yol açan bir faktör olarak değerlendirilmiştir.

Alt Tema: Denetim Aracı Olarak Sistem: Aynı zamanda sistem, üst düzey yöneticiler açısından bir denetim aracı olarak algılanmakta ve bu durum, memurlar üzerinde zaman zaman baskı yaratan bir kontrol mekanizması olarak yorumlanmaktadır.

4. Etik, Mahremiyet ve Hukuki Boyut: KGYS'nin kullanımında en fazla tartışılan temalardan biri de mahremiyet, etik ve hukuki sınırlar olmuştur. Katılımcı görüşleri bu konularda oldukça farklılaşmakta ve derin bir farkındalık düzeyine işaret etmektedir.

Alt Tema: Mahremiyet Endişesi ve Kişisel Alan: Bazı polis memurları, kameraların sürekli kayıt yapmasının kişisel mahremiyet alanlarını tehdit ettiğini belirtmiştir. Bu durum, sistemin insan hakları boyutuyla da sorgulanmasına yol açmaktadır.

Alt Tema: Hukuki Sınırlılıkların Belirsizliği: Yasal mevzuatın uygulanma biçimi ve sistemin sınırlarının belirsizliği, etik ikilemler doğurmakta ve uygulamada yorum farklılıklarına neden olmaktadır.

3.3.2. Katılımcı Görüşleri

KGYS'ye dair polis memurlarının düşüncelerini yansıtan çeşitli katılımcı ifadeleri, hem bireysel deneyimlerin hem de ortak algıların çözümlenmesine olanak sağlamıştır.

Dijitalleşmenin Etkisi Üzerine Görüşler: Katılımcıların büyük bölümü, dijital sistemlerin iş süreçlerine olan katkısını olumlu bir biçimde değerlendirmiştir. Özellikle kayıt alma, olay takibi ve kanıt toplama gibi görevlerin dijital araçlar sayesinde daha sistematik hâle geldiği vurgulanmıştır:

“KGYS sayesinde artık birçok olayın ne zaman, nasıl gerçekleştiğini kayıt altına alabiliyoruz. Eskiden tamamen şahsi kanaatle ilerliyorduk, şimdi görüntülerle destekleyebiliyoruz.” (K.17)

Bununla birlikte, bazı katılımcılar, dijital sistemlerin mesleki refleksleri baskıladığına ve insanî unsurların geriye itildiğine dikkat çekmiştir:

“Her şeyin kayıt altında olması, bizi doğal davranmaktan alıkoyuyor. Sürekli izleniyor olmak, mesleki inisiyatifi azaltıyor.” (K.04)

KGYS'nin Operasyonel İşlevselliği: Operasyonel kolaylık ve olaylara daha hızlı müdahale edebilme açısından sistemin avantajları sıkça dile getirilmiştir. Özellikle anlık yönlendirme ve geçmiş görüntülerin incelenebilmesi, sistemin somut faydaları arasında görülmüştür:

“KGYS ile sahaya çıkmadan önce olay yerinin genel durumu hakkında bilgi sahibi oluyoruz. Bu, müdahale biçimimizi de şekillendiriyor.” (K.09)

Ancak bu işlevselliğin, bazı durumlarda teknik aksaklıklar nedeniyle sekteye uğradığı da ifade edilmiştir:

“Kameraların çoğu çalışmıyor ya da kör noktaları var. Sisteme güvenmek istiyoruz ama teknik altyapı yetersiz.” (K.12)

İletişim, Denetim ve Toplumsal Etki: Sistemin vatandaşla iletişimde görünürlük yarattığı ve hesap verebilirliği artırdığı yönündeki görüşler belirginleşmiştir. Bu yönüyle KGYS, yalnızca suçla mücadele değil, aynı zamanda kamu güveni açısından da bir araç olarak görülmektedir:

“Vatandaş da artık her şeyin kayıta olduğunu bildiği için daha dikkatli davranıyor. Bizim için de bir güvenlik duvarı gibi.” (K.03)

Ancak aynı bağlamda, sistemin bir denetim aracına dönüşerek içsel baskı yarattığı görüşü de dikkat çekicidir:

“Biz vatandaşları korurken, bir yandan da yönetim tarafından izleniyoruz. Bu, mesleki özerkliği zedeliyor.” (K.08)

Etik Sınırlar ve Mahremiyet Endişeleri: KGYS'nin sürekli kayıt yapma kapasitesi, bazı memurlar tarafından etik sınırların ihlali olarak değerlendirilmiştir. Özellikle istirahat anlarında ya da iç mekân görevlerinde kameraların varlığı, kişisel alanın ihlal edildiği hissini doğurmuştur:

“Dinlenme alanlarımızda dahi kameralar var. Hangi görüntünün nerede kullanılacağı belli değil. Bu, güvensizlik yaratıyor.” (K.14)

Buna karşın bazı katılımcılar, sistemin etik açıdan gerekli olduğu görüşünü savunmuştur:

“Biz devlet adına görev yapıyoruz. Şeffaflık önemli. KGYS bu şeffaflığı sağlıyor.” (K.01)

3.3.3. Kod Frekans Tablosu ve Kod Matrisi

Nitel araştırmalarda, doğrudan alıntılar yalnızca betimleme işlevi görmekle kalmayıp; aynı zamanda bireysel algıların, ortak eğilimlerin ve kurumsal deneyimlerin çözümlenmesinde derinlik sağlayan temel bir veri kaynağı olarak değerlendirilmektedir. Bu bağlamda, KGYS uygulamasına dair elde edilen katılımcı görüşleri, dijitalleşmenin etkisi, operasyonel işlevsellik, iletişim ve denetim boyutu ile etik-mesleki sınırlar çerçevesinde tematik olarak sınıflandırılmıştır.

Dijitalleşmenin İş Süreçlerine Etkisi: Katılımcıların büyük çoğunluğu, KGYS'nin dijital olanaklarının günlük görev rutinine olumlu katkı sunduğu yönünde görüş bildirmiştir. Özellikle görüntülü kayıt sistemlerinin sağladığı kanıta dayalı işlem yapabilme imkânı, katılımcılar tarafından güçlü biçimde vurgulanmıştır. Bu durum, dijital dönüşümün yalnızca teknolojik bir yenilik değil, aynı zamanda karar alma süreçlerinde şeffaflık ve nesnellik sağlayan bir araç olarak benimsendiğini göstermektedir.

Katılımcılardan biri bu görüşü şu sözlerle dile getirmiştir: *“KGYS sayesinde artık birçok olayın ne zaman, nasıl gerçekleştiğini kayıt altına alabiliyoruz. Eskiden tamamen şahsi kanaatle ilerliyorduk, şimdi görüntülerle destekleyebiliyoruz.” (K17)* Benzer biçimde bir başka katılımcı, sistemin olay anına ilişkin görsel delil sunması nedeniyle hata payının azaldığını belirtmiştir: *“Görüntüler olmasa bazı şeyleri açıklamak çok zor olurdu, artık kimse lafla birini suçlayamıyor.” (K10)*

Buna karşılık, bazı katılımcılar dijital gözetimin mesleki refleksleri ve doğal davranışı baskıladığına dikkat çekmiştir. *“Her şeyin kayıt altında olması, bizi doğal davranmaktan alıkoyuyor. Sürekli izleniyor olmak, mesleki inisiyatifi azaltıyor.” (K4)* ifadesi, teknolojik müdahalenin olumsuz yan etkilerine işaret etmektedir.

KGYS'nin Operasyonel İşlevselliği: KGYS'nin operasyonel süreçlere olan katkısı, katılımcılar tarafından özellikle hızlı müdahale, olay öncesi bilgiye ulaşma ve anlık yönlendirme bağlamında öne çıkarılmıştır.

Örneğin, bir katılımcı “KGYS ile sahaya çıkmadan önce olay yerinin genel durumu hakkında bilgi sahibi oluyoruz. Bu, müdahale biçimimizi de şekillendiriyor.” (K9) şeklinde sistemin olay öncesi analiz avantajına dikkat çekmiştir. Benzer şekilde, “Kameralar sayesinde olay yerine gitmeden durumu görebiliyoruz, bu ciddi zaman kazandırıyor.” (K2) görüşü de müdahale sürecine olan somut katkıyı yansıtmaktadır.

Ancak teknik sorunlar nedeniyle sistemin işlevselliğinin zaman zaman sekteye uğradığı da ifade edilmiştir. “Kameraların çoğu çalışmıyor ya da kör noktaları var. Sisteme güvenmek istiyoruz ama teknik altyapı yetersiz.” (K12) ifadesi, altyapı eksikliklerinin uygulama başarısını doğrudan etkilediğini göstermektedir.

İletişim, Denetim ve Toplumsal Etki: KGYS'nin sadece olay çözümü değil, aynı zamanda vatandaşla iletişimde görünürlük ve hesap verebilirlik yarattığı da vurgulanmıştır.

“Vatandaş da artık her şeyin kayıta olduğunu bildiği için daha dikkatli davranıyor. Bizim için de bir güvenlik duvarı gibi.” (K3) ifadesi, sistemin çift yönlü bir denetim mekanizması hâline geldiğini göstermektedir.

Bununla birlikte, bazı katılımcılar bu durumun kurum içi gözetim aracı olarak kullanılmasından duydukları rahatsızlığı dile getirmiştir.

“Biz vatandaşları korurken, bir yandan da yönetim tarafından izleniyoruz. Bu, mesleki özerkliği zedeliyor.” (K8) ifadesi, içsel baskının kurum kültürü üzerindeki etkisini ortaya koymaktadır.

Bu durum, Foucault'nun panoptikon¹¹ modeline dayalı gözetim toplumları yaklaşımıyla da örtüşmektedir.

Etik Sınırlar ve Mahremiyet Endişeleri: KGYS'nin her an ve her yerde kayıt alabilme kapasitesi, bazı katılımcılar tarafından etik sınırların ihlali olarak değerlendirilmiştir.

“Dinlenme alanlarımızda dahi kameralar var. Hangi görüntünün nerede kullanılacağı belli değil. Bu, güvensizlik yaratıyor.” (K14) şeklindeki ifade, teknolojik izleme karşısında duyulan mahremiyet kaygısının açık bir yansımasıdır.

¹¹ Panoptikon modeli: Michel Foucault tarafından geliştirilmiş bir gözetim teorisidir. Kişilerin sürekli izlenip izlenmediğini bilmemesine rağmen gözetleniyor olma ihtimaliyle kendi davranışlarını kontrol altına alması esasına dayanır.

Diğer yandan, sistemin şeffaflık ve hesap verebilirlik açısından gerekliliğini savunan görüşler de mevcuttur.

“Biz devlet adına görev yapıyoruz. Şeffaflık önemli. KGYS bu şeffaflığı sağlıyor.” (K1) ifadesi, sistemin kurumsal etikle uyumlu bir denetim mekanizması olarak da algılandığını göstermektedir.

KGYS sistemine ilişkin yapılan nitel analizde, dijitalleşmenin hem işlevsel katkılar hem de mesleki sınırlamalar yarattığı görülmüştür. Katılımcıların çoğunluğu, sistemin güvenlik, hız ve delil temelli çalışma açısından büyük kolaylıklar sağladığını belirtmiştir. Ancak bu avantajların, mahremiyet, teknik yeterlilik ve mesleki özerklik gibi alanlarda bazı risklerle birlikte var olduğu da açıkça ifade edilmiştir.

Bu bulgular, Lyon (2003) ve Zuboff (2019) gibi araştırmacıların gözetim teknolojilerine dair tespitleriyle benzerlik göstermektedir. Aynı şekilde, Foucault'nun panoptikon modeli¹ de polis memurlarının izlenme hissiyle kurduğu ilişkiyi açıklamada kuramsal bir dayanak sunmaktadır.

3.3.4. Örnek Kod Ağaçları (KGYS Üzerine)

Nitel analiz sürecinde, KGYS uygulamalarının mesleki yaşantıya etkilerini görünür kılmak amacıyla oluşturulan kod ağaçları, açık kodlama sonrası ortaya çıkan veri parçalarının anlamlı temalar etrafında gruplandırılmasıyla yapılandırılmıştır. Her bir tema, kendi içinde bütünlük taşıyan alt kodlara ayrılmıştır.

Mesleki Faaliyetlerde Dönüşüm: Bu tema altında özellikle görev tanımlarındaki değişim, müdahale süreçlerinde yaşanan hızlanma ve bürokratik işlemlerin dijital sistemle hafifletilmesi gibi boyutlara dikkat çekilmiştir. Katılımcılardan biri, “Eskiden müdahaleye gitmeden önce detaylı bilgi alamıyorduk. Şimdi kameradan önce bir bakıyoruz, neyle karşılaşacağımızı biliyoruz” (K3) şeklinde ifade kullanarak KGYS'nin olaylara müdahale sürecinde zaman kazandırdığını vurgulamıştır. Benzer biçimde, bir başka katılımcı, “Rapor işi çok uzun sürüyordu. Şimdi görüntü varsa dosya daha kolay kapanıyor” (K11) sözleriyle, sistemin bürokratik yükü azalttığını belirtmiştir. Bu doğrultuda, kod ağaçlarında “Müdahale Sürecinde Hızlanma” ve “Bürokratik Yükün Azalması” alt kodları öne çıkmıştır.

Gözetim ve Denetim: Bu temada, katılımcıların sistemin izleme kapasitesi karşısında geliştirdikleri algılar öne çıkmıştır. Bir katılımcı, *“Kimin ne yaptığı her an görülebiliyor. Sürekli izleniyoruz gibi hissediyoruz”* (K6) diyerek “Sürekli İzlenme Algısı” kodunun tipik örneğini sunmuştur. Bazı katılımcılar, bu gözetim halinin karar alma özgürlüğünü kısıtladığını ifade etmiştir: *“Kamera olduğu için bazen inisiyatif almak yerine genelgeye bakıyoruz”* (K15). Ayrıca, *“Amirler artık ekran başında takip ediyor, sahada ne yaptığımızı anında biliyorlar”* (K5) şeklindeki ifade ile “Amir Denetiminin Artması” alt koduna katkı sağlanmıştır.

Vatandaşla İletişim ve Etkileşim: Bu tema altında, KGYS'nin vatandaşla kurulan iletişim üzerindeki etkileri değerlendirildiğinde farklı yönlü algılar gözlenmiştir. Bazı katılımcılar, sistemin şeffaflık sağladığını vurgulamış; *“Vatandaş da her şeyin kayıta olduğunu biliyor, davranışları değişiyor”* (K2) diyerek “Şeffaflık Algısında Artış” temasına katkı sunmuştur. Diğer yandan, bazı katılımcılar iletişimin doğallığını kaybettiğini belirtmiştir: *“Vatandaşla konuşurken bile kayıt altında olmak rahatsız ediyor”* (K19). Görsel kayıtların caydırıcılığına dikkat çeken bir ifade ise şu şekildedir: *“Kamera olduğunu görünce vatandaş hemen sakinleşiyor”* (K8).

Kod Ağaçları ile Analitik Derinleşme: Kod ağaçları sayesinde sadece temalar değil, bu temalar arasındaki örtüşmeler ve gerilim alanları da belirginleşmiştir. Örneğin, *“Dinlenme alanlarımızda bile kamera var. Bazen mahremiyet ihlali gibi hissediliyor”* (K14) ifadesi, hem “Mahremiyet” hem de “Etik Sınırlar” temalarına aynı anda hizmet eden çoklu ilişkilere işaret etmektedir.

Bu çerçevede, sistemin teknik, etik ve psikososyal yönleri arasında kesişimsel bir yapı kurulduğu; bu yapının da kod ağaçları aracılığıyla kavramsal olarak görünür kılındığı ifade edilebilir. MAXQDA'nın “Code Map” ve “Code System” araçları sayesinde bu temalar görselleştirilmiş; benzer kodların birlikte geçtiği örüntüler üzerinden kavramsal yoğunluklar ortaya çıkarılmıştır. Örneğin, “Gözetim” ve “Mesleki Özerklik” temalarının sıkça birlikte anıldığı belirlenmiştir.

Sonuç olarak, katılımcıların deneyimleri, KGYS'nin yalnızca teknolojik bir denetim aracı değil; aynı zamanda mesleki rutinleri yeniden şekillendiren, toplumsal ilişki biçimlerini etkileyen ve etik sınırların sorgulanmasına neden olan çok boyutlu bir yapı olduğunu göstermektedir. Kod ağaçları, bu çoklu boyutların sistematik olarak

çözümlemesine olanak tanımış; böylece elde edilen bulgular, bireysel ifadelerden soyutlanan kavramsal bir bütünlük içinde sunulabilmiştir.

3.4. Kütahya İl Merkezindeki Emniyet Personeline Yönelik Görüşme Verileri

Bu bölümde, Kütahya il merkezinde görev yapan emniyet personeliyle gerçekleştirilen saha araştırmasına dayalı nitel veriler ele alınmakta ve sistematik bir biçimde değerlendirilmektedir. Araştırmada kullanılan yarı yapılandırılmış görüşme ve ikili mülakat teknikleri aracılığıyla, katılımcıların KGYS'ye ilişkin algı, tutum ve deneyim düzeyleri çok boyutlu bir analiz sürecine tabi tutulmuştur.

Elde edilen bulgular doğrultusunda, sistemin kentsel güvenliğe sağladığı katkılar kadar, uygulama sürecinde karşılaşılan yapısal ve etik sınırlılıklar da ayrıntılı şekilde ortaya konmuştur. Analize, katılımcıların yaş, eğitim durumu ve görev birimi gibi demografik değişkenleri tanımlayan betimsel verilerle başlanmış; bu değişkenlerin KGYS algısı üzerindeki olası yansımaları üzerine çözümlenmeler yapılmıştır.

Sisteme ilişkin deneyim düzeyine göre görüş ayrılıklarının da dikkate değer olduğu gözlemlenmiştir. Özellikle KGYS ile aktif biçimde çalışan katılımcılar ile dolaylı temas kuran personel arasında, sistemin işlevselliği ve etkilerine yönelik algıların anlamlı ölçüde farklılaştığı belirlenmiştir. Bu bağlamda, deneyim değişkeninin KGYS'ye yönelik tutumsal ve bilişsel farkındalık üzerinde belirleyici bir rol oynadığı sonucuna ulaşılmıştır.

Ayrıca, kent güvenliğinin dijitalleşme süreciyle nasıl yeniden biçimlendiği, tematik analiz yöntemiyle değerlendirilmiştir. Suçun önlenmesi, caydırıcılık, hızlı müdahale kapasitesi, toplumsal farkındalık, veri güvenliği ve mahremiyet gibi temalar etrafında yapılan çözümlenelerde, dijital güvenlik teknolojilerinin yalnızca teknik değil, aynı zamanda psikolojik, sosyal ve etik düzeyde etkiler yarattığı görülmüştür.

Bu kapsamda, KGYS'nin etkililik düzeyi, iş yükünü azaltma potansiyeli ve kentsel yaşamın düzenlenmesine sağladığı katkılar detaylı biçimde analiz edilmiş; aynı zamanda sistemin kullanımı bağlamında ortaya çıkan etik, hukuki ve mahremiyet temelli tartışmalara da yer verilmiştir. Böylece KGYS'nin sadece güvenlik sağlama kapasitesi değil, aynı zamanda sosyal sürdürülebilirlik bağlamındaki yeri de tartışmaya açılmıştır.

İzleyen alt bölümlerde, bu temalara ilişkin bulgular, katılımcı görüşlerinden alınan doğrudan alıntılarla desteklenerek sunulacak; verilerin, çalışmanın kuramsal çerçevesi ve literatürle olan ilişkisi çerçevesinde kapsamlı bir şekilde yorumlanmasına olanak tanınacaktır.

3.4.1. Deneyim Temasına İlişkin Bulgular

Görüşmelerden elde edilen nitel veriler doğrultusunda, polis memurlarının KGYS ile kurdukları ilişki biçimleri, “deneyim düzeyi” teması altında kategorize edilmiştir. Bu kapsamda, sisteme doğrudan bütünleşmiş biçimde çalışan katılımcılar ile dolaylı yoldan etkileşim kuran personel arasında anlamlı farklar gözlemlenmiştir.

Bazı katılımcılar, KGYS’ye yönelik operasyonel bilgiye ve uygulama pratiğine sahip olduklarını açıkça ifade etmiştir. Örneğin, “*KGYS sayesinde olay yerine varmadan önce kamera kayıtlarından sahadaki durumu görüyoruz*” (K5) ifadesi, sistemle doğrudan teması olan personelin teknik kapasiteyi etkin biçimde kullandığını göstermektedir. Benzer şekilde, “*Kayıtlara bakıp olayın oluş biçimini net olarak çözümlenebiliyoruz*” (K12) görüşü, uygulamaya aktif katılımın sistem hakkındaki algıları nasıl şekillendirdiğini ortaya koymaktadır.

Bununla birlikte, bazı katılımcıların sistemle olan ilişkisi gözlem ve dolaylı deneyimler yoluyla oluşmuştur. Örneğin, “*Birebir kullanmıyoruz ama olay çözümlenmede yardımcı olduğunu görüyoruz*” (K3) ifadesi, dolaylı sistem deneyimi kodunu destekleyen tipik bir örnek olarak değerlendirilmiştir. Ayrıca, “*KGYS bizden çok amirler tarafından kullanılıyor, biz sadece sonuçlarına tanık oluyoruz*” (K8) sözleri, görev pozisyonunun etkileşim biçimini belirlediğini göstermektedir.

Bu doğrultuda, katılımcıların sistem algılarının yalnızca bilgi düzeyine değil; aynı zamanda kurumsal konum ve görev sorumluluklarına göre şekillendiği anlaşılmaktadır. Örneğin, “*Ben kameraları yönlendirmiyorum ama kayıtları inceleyen birimde çalıştım, nasıl işlediğini biliyorum*” (K16) şeklindeki bir ifade, sistemle dolaylı etkileşim kuran personelin teknik bilgiye de sahip olabileceğini göstermektedir. Buna karşılık, “*Sahada kullanmadığım için detayları bilmiyorum*” (K1) görüşü, sınırlı temasın sistem değerlendirmelerine olan yansımalarına işaret etmektedir.

Kodlama sürecinde bu ifadeler, “doğrudan sistem kullanımı”, “dolaylı gözlem”, “uygulama bilgisi” ve “teknik değerlendirme” gibi alt başlıklar etrafında gruplandırılmış; her bir kod, katılımcıların KGYS ile kurduğu deneyimsel ilişki biçimlerini kavramsal düzeyde yansıtmıştır.

Kod Haritası ve Kavramsal Örüntüler: Kod haritası oluşturulurken, içeriksel benzerlik gösteren ifadeler açık kodlama yöntemiyle MAXQDA yazılımına aktarılmış; buradan hareketle, tematik kümelenmelere ulaşılmıştır. Aşağıda, elde edilen başlıca kod kümeleri ve katılımcı ifadeleri örnekleriyle birlikte sunulmuştur:

1. Suç Önleme ve Caydırıcılık: Katılımcıların çoğunluğu, KGYS’nin önleyici ve caydırıcı bir güvenlik aracı olduğuna inandığını belirtmiştir. “*Kameraları görünce vatandaş davranışlarını değiştiriyor, bir tür baskı unsuru oluşturuyor*” (K9) ve “*Suç işlemeyi düşünen biri için kamera büyük engel*” (K7) gibi ifadeler bu kodu destekleyen örneklerdir.

2. Anlık İzleme ve Hızlı Müdahale: KGYS’nin olaylara anında müdahale etme kapasitesini artırdığı yönündeki görüşler sıklıkla dile getirilmiştir. “*Olay çıkmadan önce merkeze bilgi düşüyor, sahaya geçmeden haberdar oluyoruz*” (K14) ve “*KGYS sayesinde olay yerine daha hazırlıklı gidiyoruz*” (K5) görüşleri, bu yönüyle sistemin operasyonel etkinliğine vurgu yapmaktadır.

3. Kamera Sistemlerine Güven: Sistemin teknik altyapısına yönelik güveni yansıtan ifadeler arasında, “*Kayıtlar olay çözümlemede en büyük yardımcımız*” (K13) ve “*Delil konusunda artık elimiz çok daha güçlü*” (K6) gibi değerlendirmeler yer almıştır.

4. Toplumsal Farkındalık ve Şeffaflık: Katılımcıların bazıları, KGYS’nin toplumsal görünürlüğü artırdığını ve vatandaş davranışlarını biçimlendirdiğini belirtmiştir. Örneğin, “*Vatandaş artık her şeyin kayıt altında olduğunu biliyor ve daha dikkatli davranıyor*” (K2) ifadesi, bu başlık altında değerlendirilmiştir.

5. Veri Güvenliği ve Mahremiyet: Sistemle ilgili mahremiyet kaygısı ve veri güvenliğine ilişkin endişeler, dikkat çeken temalar arasında yer almıştır. “*Dinlenme alanlarında bile kamera var. Sürekli izleniyoruz hissi psikolojik baskı yaratıyor*” (K11) ve “*Hangi görüntünün nerede kullanılacağı belli değil*” (K18) gibi görüşler, sistemin bireysel alana müdahale ettiği yönündeki algıyı yansıtmaktadır.

6. Yapay Zekâ ve Yüz Tanıma Sistemleri: Bazı katılımcılar, gelişmiş teknolojik bileşenlerin sisteme bütünleşmiş edilmesini olumlu karşılarken, bazıları ise bu durumun etik sınırlara yaklaşabileceğini belirtmiştir. *“Yüz tanıma sistemleri işlerimizi kolaylaştırıyor ama aynı zamanda tedirginlik yaratıyor”* (K10) şeklindeki ifade, teknolojik ilerlemelerin çelişkili algılara neden olabileceğini göstermektedir.

Elde edilen bulgular, KGYS ile kurulan deneyimsel ilişkinin yalnızca teknolojik bilgiye değil; aynı zamanda kurumsal roller, görev dağılımı ve bireysel reflekslere bağlı olarak çeşitlendiğini ortaya koymuştur. Kod haritası yardımıyla, yalnızca içerik temelli değil; kavramsal yoğunluklara dayalı ilişkisel örüntüler de görünür kılınmıştır. Bu yönüyle, sistemin teknik işlevlerinin yanı sıra, etkileşimsel, sosyal ve psikolojik boyutları da kapsamlı biçimde değerlendirilmiştir.

3.4.2. Dijitalleşmenin Kent Güvenliğine Etkisine İlişkin Bulgular

Katılımcı anlatıları doğrultusunda, kent güvenliğine ilişkin dijitalleşme süreçlerinin çok katmanlı bir yapıya sahip olduğu anlaşılmıştır. Elde edilen veriler, MAXQDA yazılımı kullanılarak tematik düzeyde analiz edilmiş; dijital güvenlik sistemlerine yönelik algıların görev tanımı, kurumsal pozisyon ve uygulama pratiklerine bağlı olarak anlamlı bir çeşitlilik gösterdiği ortaya konmuştur.

Olumlu Değerlendirme teması çerçevesinde, dijital güvenlik sistemlerinin özellikle kamu güvenliği açısından işlevsellik taşıdığına ilişkin ifadelerin yoğunlaştığı belirlenmiştir. Bazı katılımcılar, sistemin sunduğu operasyonel olanakları doğrudan deneyimlemiş; bazıları ise daha çok kurumsal işleyiş üzerinden değerlendirmelerde bulunmuştur.

1. Suçun Önlenmesi ve Caydırıcılık: Dijital gözetim sistemlerinin yalnızca olay sonrası müdahale için değil; aynı zamanda önleyici bir güvenlik aracı olarak algılandığı saptanmıştır. Özellikle kamusal davranışların şekillendirilmesinde bu sistemlerin önemli rol oynadığı vurgulanmıştır:

- *“Kameraların varlığı bile çoğu zaman yeterli oluyor. Suç işlenmeden caydırıyor. İnsanlar bilmeden bile davranışlarını değiştiriyor.”* (K6)
- *“Yalnızca kameranın orada olduğunu bilmek bile olayları azaltıyor.”* (K14)

Bu ifadeler, Foucault'nun panoptikon yaklaşımıyla da örtüşmektedir; bireyin sürekli gözetlenmese bile gözetlenme ihtimali karşısında davranışlarını içselleştirmesi şeklindeki etki açıkça görülmektedir.

2. Mahremiyet ve Veri Güvenliği: KGYS gibi gözetim sistemlerinin yarattığı görünürlük ve izlenebilirlik durumu, bazı katılımcılar tarafından mahremiyetin ihlali olarak yorumlanmıştır:

- *“Her an izleniyor olmak rahatsız edici. Nerede olduğumuz, ne yaptığımız birileri tarafından görülebiliyor. Bu, bana kendimi güvende değil, kısıtlanmış hissettiriyor.”* (K10)

- *“Dinlenme alanlarımızda bile kamera var. Sürekli kontrol altındayız.”* (K18)

Bu değerlendirmeler, dijital gözetim teknolojilerinin fiziksel güvenlik sağlama amacının ötesinde, bireylerin psikolojik sınırlarına da etki ettiğini göstermektedir.

3. Güvende Hissetme: Bazı katılımcılar ise izleniyor olma durumunu, bireysel güvenlik hissini artıran bir unsur olarak değerlendirmiştir:

- *“Gece geç saatte eve dönerken kameralı sokaklardan gitmeye çalışıyorum. Orada izleniyor olmak içimi rahatlatıyor.”* (K3)

- *“Sokakta devriye olmasa bile kameranın varlığı bize güven veriyor.”* (K9)

Bu ifadeler, gözetim teknolojilerinin yalnızca fiziki değil, aynı zamanda psikolojik koruma hissi oluşturduğunu ortaya koymaktadır.

4. Kamera Sistemlerine Güven: Katılımcıların bir kısmı, teknik eksikliklere rağmen KGYS'nin genel işleyişine yönelik olumlu bir güven geliştirmiştir:

- *“Sistemin her noktayı göremeyeceğini biliyorum ama genel olarak işliyor. O yüzden insanlar daha dikkatli davranıyor.”* (K1)

- *“Kayıtlar bazen eksik olabilir ama genel olarak delil konusunda elimiz güçlendi.”* (K5)

Bu görüşler, sistemin tam kapsayıcı olmamasına rağmen davranışsal düzenleme işlevini sürdürdüğünü göstermektedir.

5. Teknolojik Uyum ve Alışkanlıklar: Görüşmelerde, dijital teknolojilerin kurumsal rutinelere entegre oluşu ve buna bağlı gelişen alışkanlıkların da önemi vurgulanmıştır:

- *“Artık her şey dijital. Aıştık. Eski sistemler geri gelse büyük karmaşa olur. Teknolojiyle birlikte çalışmak şart.”* (K2)

- “Dijital sistemler sayesinde işler daha düzenli. Kalemle tutulan tutanaklar devri kapandı.” (K15)

Bu ifadeler, dijitalleşmenin yalnızca güvenlik boyutunda değil; aynı zamanda kurumsal hafızanın yeniden yapılandırılmasında da etkili olduğunu göstermektedir.

6. Yapay Zekâ ve Yüz Tanıma Sistemleri: Bazı katılımcılar, gelişen teknolojik bileşenlere ihtiyatla yaklaşmakla birlikte, bunların işlevsel boyutlarını da göz ardı etmemektedir:

- “Ne kadar iyi çalışıyor bilemiyoruz ama çok şeyin artık yazılıma bağlı olduğunu fark ediyorum. Hata yaparsa geri dönüşü zor olur.” (K7)
- “Yüz tanıma sistemleri hızlı çözüm sağlıyor ama bazen hatalı eşleşme yaparsa sıkıntı büyük olabilir.” (K17)

Bu görüşler, yapay zekâ temelli uygulamalara duyulan güven ile ihtiyatlı yaklaşım arasındaki dengeyi yansıtmaktadır.

Toplanan anlatılar, dijital güvenlik sistemlerine yönelik algının tek yönlü olmadığını; bu algının görev deneyimleri, sistemle temas düzeyi ve bireysel tutumlara göre değişiklik gösterdiğini ortaya koymuştur. Sistemler bir yandan güvenliği artıran araçlar olarak görülmekte; diğer yandan mahremiyet, bireysel alan ve psikolojik baskı gibi konularda çeşitli sorgulamalara neden olmaktadır.

Sonuç olarak, dijitalleşmenin kent güvenliği üzerindeki etkisinin yalnızca teknik verimlilik düzeyinde değil; aynı zamanda etik, duygusal ve sosyal katmanlarda da derinlemesine analiz edilmesi gerektiği ortaya konmuştur. Katılımcı ifadeleri, bu çok boyutlu yapıyı anlamada önemli bir veri kaynağı olarak değerlendirilmiştir.

3.4.3. Dijital Güvenlik Sistemlerine İlişkin Bulgular

Katılımcı anlatılarına dayanarak, dijital güvenlik sistemlerine yönelik algılar ve deneyimler toplam **on bir alt temada** bütünleştirilmiştir. Bu temalar; güvenliğe dair teknik ve operasyonel boyutlar, psikososyal etkiler, etik sınırlar ve kent yaşamına ilişkin yansımalar gibi çok yönlü alanları kapsamaktadır.

Kodlar Arası Tematik Geçişlilik: Kod haritası üzerinde yapılan ilişkiyel çözümler, bazı kodların birden fazla tema ile eşzamanlı ilişkili olduğunu göstermiştir. Örneğin:

- “Kamera sistemlerine güven” ve “güvende hissetme” ifadeleri, birçok katılımcı söyleminde iç içe geçmiş biçimde yer almıştır. Bir katılımcı bu konuda şöyle belirtmiştir:

“Her yeri göremese de kameraların olması insanı güvende hissettiriyor. O yüzden sistemin çalıştığını bilmek bile yetiyor.” (K8)

- Benzer şekilde, “mahremiyet” temasının hem “veri güvenliği” hem de “yapay zekâ” uygulamalarıyla kesiştiği gözlemlenmiştir. Özellikle yüz tanıma teknolojileri ile ilgili olarak bir katılımcı şöyle demiştir:

“Nereye kayıt alındığı belli değil. Her şey sistemde. Yüz tanıma işi biraz özel alanı zorluyor.” (K14)

Bu çoklu ilişkililik durumu, katılımcı algılarında bazı kavramların sadece teknik değil, aynı zamanda etik ve psikolojik düzeyde de anlam kazandığını göstermektedir.

Belirlenen Temalar ve Yapısal Dağılım: Kodlamalar sonucunda elde edilen temalar aşağıda sıralanmıştır. Her bir tema altında birden fazla alt kod ve katılımcı ifadesi yer almaktadır:

- **Suç Önleme ve Caydırıcılık**

“Kamera varsa suç olmuyor. İnsanlar kendilerini denetliyor gibi.” (K5)

- **Anlık İzleme ve Hızlı Müdahale**

“Anlık görüntüyle müdahale zamanında yapılıyor. Beklemeye gerek kalmıyor.” (K9)

- **Güvende Hissetme**

“Görev sırasında kameraların çalıştığını bilmek içimizi rahatlatıyor.” (K1)

- **Toplumsal Farkındalık ve Davranışsal Etkiler**

“Vatandaş bile artık kamera göre hareket ediyor.” (K3)

- **Kamera Sistemlerine Güven**

“Kameralar çalıştığında sorun az oluyor. Görüntü varsa herkes daha dikkatli.” (K6)

- **Veri Güvenliği ve Mahremiyet**

“Verilerin nasıl saklandığını bilmiyoruz. Özel alanlarımızda kamera olmamalı.” (K12)

- **Yapay Zekâ ve Yüz Tanıma Teknolojileri**

“Yüz tanıma işi güzel ama yanlış tanı olursa sıkıntı büyük olur.” (K17)

- **Dijitalleşme ile Bütünleşme**

“Artık dijital sistemler olmadan işler yürümüyor. Alıştık.” (K11)

- **İş Yükü Azaltma**

“Olaylara daha çabuk müdahale ediliyor. Evrak işleri azaldı.” (K15)

- **Yaşanabilir Kent Algısı**

“Daha düzenli bir kent yapısı oluştu. Vatandaş da kurallara uymaya başladı.” (K13)

- **Sistem Etkinliği ve Verimlilik**

“Dijital sistemler işlerimizi hızlandırdı. Eskiden üç kişiyle yaptığımız işi bir kişi hallediyor.” (K10)

Kod Haritasının Katkısı

Kod haritası yalnızca bu tematik yapıların sınıflandırılmasını değil, aynı zamanda temalar arası geçişkenlikleri de görünür kılmıştır. Örneğin, “veri güvenliği” ile “güvende hissetme” arasındaki gerilim bazı katılımcılar tarafından çelişkili biçimlerde ifade edilmiştir:

“Kameralar hem güven veriyor hem de izleniyoruz hissi uyandırıyor. Bazen huzur bazen tedirginlik.” (K7)

Bu durum, dijital güvenlik sistemlerine yönelik algının sabit ve yekpare değil; görev tipi, deneyim düzeyi ve bireysel değer yargılarına bağlı olarak değişken olduğunu göstermektedir.

Kod haritası aracılığıyla yapılan çözümleme, dijital güvenlik teknolojilerinin yalnızca işlevsel değil; aynı zamanda **algısal, etik ve toplumsal boyutlarıyla** da nasıl değerlendirildiğini ortaya koymuştur. Temalar arasında belirlenen bu çok katmanlı ilişkiler, katılımcı söylemlerinin derinliğini artırmakta ve KGYS'nin kolluk personeli üzerindeki etkisini yalnızca teknik düzlemde değil, aynı zamanda kültürel ve psikolojik bağlamda da anlamlandırmayı mümkün kılmaktadır.

Tema 1: Suç Önleme ve Caydırıcılık: *“Kameraların varlığı başlı başına yeterli oluyor. Suç işlenmeden önleniyor; insanlar artık daha dikkatli davranıyor.” (K5)*

Katılımcı ifadesi, gözetim sistemlerinin yalnızca müdahale aracı değil, aynı zamanda önleyici bir kontrol mekanizması olduğunu ortaya koymaktadır. Dijital sistemlerin, birey davranışları üzerinde caydırıcı bir etkisi olduğu vurgulanmıştır.

Tema 2: Anlık İzleme ve Hızlı Müdahale: *“Eskiden olay olduktan sonra bilgi alınabiliyordu, şimdi sistem anında uyarı veriyor. Zaman kaybı yaşanmıyor.”* (K9)
Bu görüş, dijitalleşmenin müdahale süreçlerindeki zaman maliyetini azaltarak operasyonel verimliliği artırdığına işaret etmektedir.

Tema 3: Güvende Hissetme: *“Sokakta yürürken izleniyor olmak bazen rahatsız etse de, bir olay yaşandığında kayıt altına alındığını bilmek güven veriyor.”* (K1)

İfade, izleme sistemlerinin çelişkili iki etkisini aynı anda yansıtmaktadır: Hem koruyucu hem de psikolojik baskı yaratan yönleri.

Tema 4: Kamera Sistemlerine Güven: *“Her şey kayda alınıyor. Bu durum, hem bizi koruyor hem de olayların gerçekliğini ortaya koyuyor.”* (K8)
Bu söylem, kayıtların hem iç denetim hem de hukuki süreçlerde nesnellik sağlama işlevini öne çıkarmaktadır.

Tema 5: Veri Güvenliği ve Mahremiyet: *“Sistem oldukça faydalı ama bazen özel bilgilerin kimlerin erişimine açık olduğunu düşünmeden edemiyor insan.”* (K14)
Görüş, teknik güvenlik kadar kişisel veri güvenliğinin de dijitalleşme sürecinde temel bir endişe unsuru olduğunu göstermektedir.

Tema 6: Yapay Zekâ ve Yüz Tanıma: *“Yapay zekâ birçok süreci hızlandırıyor ama her hareketin izlenmesi bazen sınırların belirsizleştiği hissini yaratıyor.”* (K17)
İfade, otomatik izleme sistemlerinin bireysel alanı tehdit edebileceğine dair etik bir sorgulama içermektedir.

Tema 7: Dijitalleşme ve Teknolojiyle Bütünleşme: *“Artık eski yöntemlerle bu işler yürütülemez. Teknoloji hem süreci hem de görev uygulamalarını hızlandırıyor.”* (K11)

Bu söylem, teknolojik dönüşümün mesleki uygulamalarda yaygınlaştığını ve zorunlu hâle geldiğini ortaya koymaktadır.

Tema 8: Sistem Etkinliği ve Verimlilik: *“Olaylara müdahale süresi ciddi biçimde azaldı. Eskiden saatler alan işlemler artık dakikalar içinde tamamlanıyor.”* (K13)

İfade, dijital güvenlik sistemlerinin iş akışı üzerindeki somut etkilerini vurgulamakta; zaman tasarrufu ve süreç iyileştirmesi sağladığına işaret etmektedir.

Temalar Arası İlişki Modeli: Kavramsal Örgü ve Geçişlilik: MAXQDA'nın tematik görselleştirme araçları kullanılarak oluşturulan ilişki haritasında, temalar arasında **örüntüsel ve geçişli bağların** olduğu tespit edilmiştir. Bu yapılar, yalnızca kavramsal yakınlıkla değil, aynı zamanda katılımcı anlatılarındaki **duygusal ve bilişsel geçişler** üzerinden modellenmiştir.

- “**Suç önleme ve caydırıcılık**” teması, modelin merkezinde konumlandırılmış; özellikle “**anlık müdahale**”, “**kamera güveni**” ve “**verimlilik**” temaları ile doğrudan bağlantılı şekilde yapılandırılmıştır. Bu etkileşim, sistemin sadece izleme değil, aynı zamanda hızlı eyleme geçme ve kamusal düzen kurma işlevleriyle birleştiğini göstermiştir.
- “**Veri güvenliği**” ve “**mahremiyet**” temaları, sistemin fayda boyutuna gölge düşüren **etik duyarlılık kümeleri** olarak ortaya çıkmıştır. Katılımcıların büyük bölümü, sistemlerin etkinliğini kabul etmekle birlikte, kişisel sınırların bulanıklaştığına dair endişeler taşımaktadır.
- “**Güvende hissetme**” teması, bu iki uç arasında **köprü niteliği** taşımaktadır. Bir grup katılımcı, kameraların görünürlüğünü güvenlik göstergesi olarak değerlendirirken; diğer bir grup, bu görünürlüğün izlenme baskısına dönüştüğünü ifade etmiştir.

“*Kamera beni koruyor ama aynı zamanda her an izlendiğimi bilmek bazen huzursuzluk veriyor*” (K4). Bu örnek, güvenlik ve özgürlük arasında ortaya çıkan psikolojik ikiliği yansıtmaktadır.

Tematik ilişki modeli, KGYS ve benzeri dijital güvenlik sistemlerinin yalnızca teknik bir altyapı olmadığını; aynı zamanda toplumsal anlam üretiminin bir parçası hâline geldiğini göstermektedir. Katılımcı ifadeleri, bu sistemlere yönelik algının işlevsellik, etik, psikolojik etki ve kurumsal dönüşüm boyutlarında şekillendiğini ortaya koymuştur.

Bu çerçevede, dijital gözetim sistemleri bir yandan kurumsal verimliliği ve kamu güvenliğini artıran araçlar olarak değerlendirilirken; diğer yandan bireysel haklar, mahremiyet ve sosyal denge açısından eleştirel bir okuma alanı yaratmaktadır.

3.4.4. Dijital Dönüşümün Kent Güvenliğine Etkisine İlişkin Bulgular

Yürütülen nitel analiz süreci neticesinde, kent güvenliğine yönelik dijital dönüşümün çok katmanlı etkilerini ortaya koyan temalar belirlenmiştir. Polis memurlarının bireysel deneyimlerinden, mesleki yargılarından ve kurumsal değerlendirmelerinden elde edilen veriler, dijital güvenlik sistemlerinin yalnızca teknik değil; aynı zamanda psikolojik, sosyolojik ve etik düzeyde çok yönlü bir etkileşim alanı oluşturduğunu göstermektedir. Özellikle *suç önleme*, *anlık müdahale* ve *sistem etkinliği* gibi temalar sistemlerin işlevsel yönlerini öne çıkarırken; *mahremiyet*, *yapay zekâ* ve *güvende hissetme* temaları, dijitalleşmenin bireysel sınırlılıklar ve toplumsal duyarlılıklarla ilişkisini görünür kılmıştır.

Tematik Yapı ve Üst Başlıklar: Kodlama süreci sonunda belirlenen temalar aşağıdaki başlıklarda sınıflandırılmıştır:

- Suç önleme ve caydırıcılık
- Anlık izleme ve hızlı müdahale
- Güvende hissetme
- Toplumsal farkındalık ve davranışsal değişim
- Kamera sistemlerine güven
- Veri güvenliği ve mahremiyet
- Yapay zekâ ve yüz tanıma teknolojileri
- Dijitalleşme ve teknolojik adaptasyon
- İş yükü azaltma ve operasyonel kolaylık
- Yaşanabilir/düzenli şehir algısı
- Sistem etkinliği ve verimlilik

Tema Bazlı Bulgular ve Katılımcı Söylemleri

Suç Önleme ve Caydırıcılık: Dijital gözetim teknolojilerinin kamuya açık alanlarda suç işleme eğilimlerini büyük ölçüde sınırladığı gözlemlenmiştir. Katılımcıların çoğu, gözetim sistemlerinin varlığının bireylerin davranışlarını doğrudan etkilediğini ve suçların daha oluşmadan engellendiğini belirtmiştir. Bu bağlamda, bir katılımcı, “*Kameraların varlığı bile çoğu zaman yeterli oluyor. Suç işlenmeden caydırıyor.*” (K2) ifadesiyle sistemin norm üretici rolüne dikkat çekmiştir.

Anlık İzleme ve Hızlı Müdahale: KGYS gibi dijital güvenlik sistemlerinin olaylara anlık müdahaleyi mümkün kıldığı ve bu sayede operasyonel süreçlerde önemli bir zaman avantajı sağlandığı görülmüştür. *“Eskiden olaydan saatler sonra müdahale edilirdi. Şimdi daha olayın içindeyken müdahale başlıyor.”* (K7) ifadesi, dijital sistemlerin sahadaki karar alma mekanizmalarına katkısını örneklemektedir.

Güvende Hissetme: Dijital izleme sistemleri, yalnızca fiziksel güvenlik sağlamamakta; aynı zamanda psikolojik güven hissini de güçlendirmektedir. Ancak, bu hissin bazı durumlarda “sürekli gözetlenme” algısıyla birlikte rahatsızlık yarattığı da dile getirilmiştir. *“Kamera olduğunu bildiğim yerlerde yürürken daha az tedirgin oluyorum, ama bazen izlenmek baskı gibi de geliyor.”* (K3) yorumu, bu ikili hissiyatı yansıtmaktadır.

Toplumsal Farkındalık ve Davranışsal Etkiler: Katılımcı görüşleri, gözetim sistemlerinin bireylerin kamusal davranışlarını biçimlendirdiğini, toplumsal normları yeniden ürettiğini ve güvenlik algısını daha görünür kıldığını ortaya koymaktadır. *“Vatandaş da artık her şeyin kayıta olduğunu bildiği için daha dikkatli davranıyor.”* (K3)

Kamera Sistemlerine Güven: Kamera sistemlerinin olayların çözümüne katkı sağladığı, delil oluşturma kapasitesinin güveni artırdığı ifade edilmiştir. Ancak bazı katılımcılar, sistemlerin teknik açıdan zaman zaman yetersiz kalabileceğini vurgulamıştır. *“Her zaman yeterli mi emin değilim ama çoğu zaman işe yarıyor.”* (K12)

Veri Güvenliği ve Mahremiyet: Sürekli gözetim altında bulunma hâlinin psikolojik baskı yarattığı; bireysel mahremiyet alanlarının belirsizleştiği yönünde güçlü bir eleştirel söylem geliştirilmiştir. Katılımcılar, bu sistemlerin etik sınırlarının belirsizliğinden rahatsızlık duymakta ve kişisel verilerin nasıl işlendiğine dair kaygı taşımaktadır:

“Teknoloji çok ilerledi ama özel alanımızın nerede başladığını artık kestiremiyoruz.” (K14)

Yapay Zekâ ve Yüz Tanıma Teknolojileri: Yeni nesil güvenlik uygulamaları olan yüz tanıma sistemleri ve yapay zekâ algoritmaları, bazı katılımcılarca olumlu karşılanırsa da, hata payları ve etik sorumluluklar bakımından ciddi kaygılar da dile getirilmiştir. *“Bir yanlışlık olsa kim sorumluluk alacak?”* (K18)

Dijitalleşme ve Teknolojik Adaptasyon: Katılımcıların büyük bölümü, dijitalleşmenin artık geri döndürülemez bir süreç olduğunu ve kurumların bu dönüşüme uyum sağlamak zorunda olduğunu ifade etmiştir. Aynı zamanda, teknolojinin denetim altında tutulması gerektiği de sıkça vurgulanmıştır.

İş Yükü Azaltma ve Operasyonel Kolaylık: Dijital sistemler, belge yönetiminden müdahale süreçlerine kadar birçok operasyonel faaliyeti kolaylaştırmış, iş gücü üzerindeki yükü azaltmıştır. “Eskiden evrak işleri çok yoğundu. Şimdi sistem sayesinde birçok şey hızlandı.” (K9)

Yaşanabilir ve Düzenli Şehir Algısı: Kameralarla donatılmış bölgelerin daha düzenli, daha güvenli ve daha huzurlu olduğu yönünde yaygın bir kanaat oluşmuştur. Ancak bu düzen duygusunun aynı zamanda bir kontrol hissi yarattığı da belirtilmiştir.

Sistem Etkinliği ve Verimlilik: Teknik altyapının güçlendirilmesiyle birlikte, sistemlerin karar alma süreçlerini hızlandırdığı ve hata oranlarını azalttığı yönünde değerlendirmeler yapılmıştır. “Sistem çok iş görüyor. Müdahale hızlandı, hata payı azaldı.” (K11)

Temalar Arası İlişkisel Yapı ve Analitik Çözümleme: MAXQDA yazılımı aracılığıyla gerçekleştirilen tematik analiz sürecinde, temalar arasındaki içeriksel ve bağlamsal ilişkiler bütüncül bir yapı hâlinde modellenmiştir. Bulgular doğrultusunda iki ana tematik küme ortaya konmuştur:

1. **Güvenlik Odaklı Temalar:** *Suç önleme, anlık müdahale, kamera güvenliği ve sistem verimliliği* temaları, güvenlik üretimi açısından merkezî bir pozisyon üstlenmiştir. Bu temalar, dijital sistemlerin meşrulaştırılmasında teknik başarı ve operasyonel yeterlilik temelinde önemli bir dayanak oluşturmuştur.
2. **Etik ve Bireysel Sınırlılık Temaları:** *Veri güvenliği, mahremiyet, yüz tanıma teknolojileri ve izlenme baskısı*, daha çevresel bir konumda yer almakla birlikte sistemin eleştirel boyutlarını temsil etmektedir. Bu temalar, güvenlik ile özgürlük, izlenme ile özel alan arasındaki gerilimleri göz önüne sermektedir.

Güvende hissetme teması ise her iki küme arasında geçişsel bir alan olarak konumlanmış; bireylerin hem korunduğunu hissettiği hem de gözetlendiğini düşündüğü bir alan olarak temalar arası çok yönlü bağ kurmuştur.

Yapılan analiz, dijital güvenlik sistemlerinin yalnızca teknolojik araçlar değil; aynı zamanda toplumsal normlar, kurumsal yapı ve bireysel psikolojiyle etkileşim

içinde olan bir dönüşüm aracı olduğunu ortaya koymaktadır. Katılımcı anlatıları, dijitalleşmenin kent güvenliğine katkı sunduğu kadar; etik, hukuki ve sosyolojik sınırları da zorlayan çok boyutlu etkiler yarattığını göstermektedir. Bu bağlamda, güvenlik sistemlerinin başarısı yalnızca teknik yeterlilikle değil; aynı zamanda toplumsal kabul, etik meşruiyet ve bireysel hakların korunmasıyla da ölçülmelidir.

3.4.5. Dijital Sistemlere Yönelik Algı ve Tutuma İlişkin Bulgular

Bu bölümde, dijital güvenlik sistemlerine yönelik algı ve tutumlar, yalnızca kolluk kuvvetleri bağlamında, nitel veri analizine dayalı olarak değerlendirilmiştir. Görüşme verilerinden elde edilen bulgular, teknolojik sistemlerin yalnızca teknik araçlar olarak değil; aynı zamanda psikolojik, kurumsal ve sosyal dinamiklerle iç içe geçmiş yapılar olarak algılandığını ortaya koymaktadır.

Katılımcılar tarafından dijital sistemler, kent güvenliğinin sağlanmasında işlevsel ve destekleyici bir unsur olarak tanımlanmıştır. Özellikle suçla mücadelede, müdahale süreçlerinin hızlandırılmasında ve kamu düzeninin korunmasında önemli katkılar sunduğu yönünde ortak bir kanaat oluşmuştur:

“Kameraların varlığı insanları düşündürüyor. Eskisi kadar rahat davranılmıyor artık.” (K1)

Sistemin görünür varlığının birey davranışlarını doğrudan etkilediği; potansiyel risklerin önlenmesi açısından caydırıcı bir rol üstlendiği ifade edilmiştir. Dijital izleme sistemlerinin, olaylara zamanında müdahale edilmesini kolaylaştırdığı yönündeki değerlendirmeler öne çıkmıştır:

“Bir olay çıktığında anında müdahale ediliyor. Eskiden bu kadar hızlı olunmazdı.” (K2)

Katılımcı anlatılarında, kamera altyapısının olay anına dair hızlı bilgi aktarımını sağladığı ve karar alma süreçlerini desteklediği sıkça dile getirilmiştir. Bu bağlamda sistem, yalnızca gözleme amacıyla değil; aynı zamanda olay yönetimini yönlendirme işleviyle de değerlendirilmektedir.

Katılımcıların büyük kısmı, dijital izleme sistemlerinin bulunduğu alanlarda görev yürütmenin, yalnızca fiziksel güvenlik değil; aynı zamanda psikolojik bir güven hissi sağladığını belirtmiştir:

“Kamera olduğunu bildiğim yerlerde yürürken daha az tedirgin oluyorum, ama bazen izlenmek baskı gibi de geliyor.” (K3)

Bu güvenlik algısının, dijital varlığın kendisi kadar, o varlığa yüklenen simgesel anlamla da ilişkili olduğu görülmektedir. Ayrıca sistemin kamuya açık alanlarda yaygın biçimde kullanılmasıyla, bireylerde kurallara uyum ve davranışsal farkındalığın arttığı yönünde değerlendirmeler yapılmıştır:

“İnsanlar davranışlarını değiştirdi. Çünkü artık her yerde kamera var.” (K4)

Bu durum, dijital güvenlik teknolojilerinin yalnızca teknik değil, aynı zamanda toplumsal davranışları yönlendiren bir kontrol mekanizması olarak da işlev gördüğünü göstermektedir. Katılımcı ifadelerinde sıkça vurgulanan bir diğer unsur ise sistemin verimliliğe olan katkısıdır:

“Sistem çok iş görüyor. Müdahale hızlandı, hata payı azaldı.” (K11)

Güvenlik süreçlerinin dijital altyapı aracılığıyla daha hızlı, koordineli ve hatasız yürütülebildiği; görevlerin sistematik biçimde dağıtıldığı ve zaman yönetiminin etkinleştiği ifade edilmiştir. Bu görüşler, dijital sistemlerin operasyonel faydalarının yanı sıra kurumsal işleyişe sağladığı katkıları da vurgulamaktadır:

“Eskiden evrak işleri çok yoğundu. Şimdi sistem sayesinde birçok şey hızlandı.” (K9)

Sistem sayesinde delil toplama ve olay kayıt süreçlerinde kolaylık sağlandığı; özellikle sahada görev yapan personelin iş yükünün azaldığı belirtilmiştir. Bununla birlikte, fiziksel yükte azalma sağlansa da, zihinsel yükte zaman zaman artış yaşandığı yönünde değerlendirmelere de rastlanmıştır. Bu durum, dijitalleşmenin getirdiği avantajlarla birlikte, yeni türden mesleki dinamikler oluşturduğunu göstermektedir.

Öte yandan, sistemin olumlu yönlerinin yanı sıra etik ve kişisel sınırlar bağlamında çeşitli sorgulamalar da yapılmıştır. Katılımcılar, dijital izleme kapasitesinin genişlemesinin mahremiyet sınırlarını zorlayabileceğine ve bireysel özgürlük alanında bazı belirsizlikler yaratabileceğine dikkat çekmiştir:

“Güvenlik için izleniyoruz ama bilgilerimiz nerede, kimde bilemiyoruz. Bu biraz rahatsız edici.” (K6)

Özellikle yüz tanıma sistemlerine ilişkin değerlendirmelerde, hatalı eşleşme ihtimalinin yaratabileceği sonuçlara dair temkinli bir tutum benimsenmiştir:

“Yüz tanıma sistemleri etkileyici ama riskli. Yanlış eşleşme olursa telafisi zor olur.” (K7)

Bazı katılımcılar ise dijitalleşme sürecinin geri döndürülemez bir noktada olduğunu kabul etmekle birlikte, bu dönüşümün sağlıklı yönetilmesi gerektiğini vurgulamıştır:

“Artık dijital olmadan bir iş yürütülmüyor. Ama bu kadar izleniyor olmak da düşündürücü.” (K8)

Dijital güvenlik sistemlerinin yalnızca güvenlik değil, aynı zamanda kent yaşamına ilişkin düzen ve estetik arayışlara da katkı sunduğu yönünde görüşler bildirilmiştir:

“Kameralı bölgeler daha düzenli. Huzur veriyor insana, ama biraz da kontrol hissi var.” (K10)

Bu doğrultuda sistem, yalnızca riskleri bertaraf eden bir araç değil; aynı zamanda şehir yaşamını biçimlendiren bir yapısal unsur olarak da tanımlanmıştır.

Genel olarak değerlendirildiğinde, dijital güvenlik sistemlerine yönelik algıların çok boyutlu, dinamik ve bağlamsal bir yapıya sahip olduğu söylenebilir. Katılımcıların bu sistemlerle kurduğu ilişki, teknik etkinliğin yanı sıra etik duyarlılıklar, mesleki pratikler ve psikolojik tepkiler çerçevesinde şekillenmektedir. Bu bağlamda, KGYS gibi uygulamaların yalnızca teknik değil; aynı zamanda toplumsal bir dönüşüm sürecinin de parçası olduğu sonucuna ulaşılmıştır.

3.4.6. Sistemin Etkinliği ve Karşılaşılan Sorunlara İlişkin Bulgular

Örnek olarak, “sistem etkinliği ve verimlilik” teması, görev süreçlerinde hız, koordinasyon ve karar alma kolaylığına yapılan atıflar üzerinden yapılandırılmış; “iş yükü azaltma” teması ise sahadaki uygulamalardan kaynaklanan operasyonel rahatlamalara odaklanan anlatılarla desteklenmiştir. “Veri güvenliği ve mahremiyet” teması, izlenme algısı, kişisel sınırların belirsizleşmesi ve özellikle yüz tanıma sistemlerine dair etik değerlendirmeler üzerinden yapılandırılmıştır.

Bazı temalar, içerdiği kavramların kesişim noktalarında birbiriyle bağ kurarak çok boyutlu bir ağ yapısı oluşturmuştur. Örneğin, “yaşanabilir/düzenli şehir” ve “toplumsal farkındalık” temaları arasında kurulan normatif ilişki, dijital güvenlik

sistemlerinin yalnızca denetim sağlayan bir yapı değil; aynı zamanda toplumsal davranışları yönlendiren bir işlev üstlendiğini göstermektedir.

Farklı görev kademelerindeki katılımcılar tarafından ifade edilen anlatılarda, sistemin teknik, yönetsel ve psikolojik etkilerine dair çeşitlenen değerlendirmeler dikkat çekmiştir. Bazı ifadelerde sistemin operasyonel yeterliliği ön plana çıkarken; bazılarında bireysel alanın sınırlarına yönelik değerlendirmeler öne çıkmıştır. Bu durum, mesleki deneyim çeşitliliğinin değerlendirme biçimleri üzerinde belirleyici bir etkisi olduğunu düşündürmektedir.

Kod haritasının genel yapısı incelendiğinde, dijital güvenlik sistemlerinin teknik, etik, psikolojik ve sosyolojik boyutları arasında bütüncül bir örüntü kurulduğu görülmektedir. Temalar arası geçişkenlikler, içeriksel yoğunluklar ve anlatı derinlikleri dikkate alınarak oluşturulan bu yapı, verinin yalnızca tanımlanmasını değil; aynı zamanda eleştirel bir çerçevede değerlendirilmesini de mümkün kılmıştır.

“Sistemin varlığı bize bir adım önde olma imkânı veriyor. Olay yaşanmadan önce bile fark edilmesi mümkün oluyor artık. Eski usulde böyle bir şey yoktu.” (K6). Bu ifade, dijital güvenlik sistemlerinin önleyici kapasitesine ve kriz öncesi erken müdahale imkânlarına vurgu yapmaktadır. Sistem, yalnızca olay sonrası kayıt değil; olay öncesi risk analizi açısından da işlevsel görülmektedir.

“Kameraların her yerde olduğunu bilmek güven veriyor ama bazen göz önünde olmak da rahatsız edebiliyor. Özellikle kalabalık yerlerde daha fazla izleniyor hissi oluşuyor.” (K11). Burada, güvenlik hissi ile izlenme algısı arasındaki ikili duygu yapısı dikkat çekmektedir. Sistemin sunduğu koruyucu çerçeve olumlu karşılanırken, sürekli gözetim hâlinin kişisel alan üzerinde baskı oluşturduğu da dile getirilmektedir.

“Eskiden sahada daha çok yoruluyorduk. Şimdi bazı şeyleri oturduğumuz yerden takip edebiliyoruz. Zaman kazanıyoruz ama ekrana bakmaktan da yoruluyoruz aslında.” (K4). Bu görüş, dijital sistemlerin fiziksel yükü azalttığını ancak zihinsel dikkat yoğunluğunu artırdığını göstermektedir. Ekran temelli çalışma biçimi, farklı türden bir yorgunluk biçimi üretmektedir.

“Yüz tanıma sistemleriyle ilgili endişelerim var. Her an izlenmek tedirgin edici olabiliyor. Nerede durduğumu, ne kadar izlendiğimi bilmiyorum”. (K9). Bu ifade, yüz tanıma teknolojisinin sınırlarına ve bireysel mahremiyet üzerindeki etkilerine dair etik

sorgulamayı içermektedir. Gözetimin sürekliliği, sistemin sınırlarının belirgin olmaması hâlinde tedirginlik yaratabilmektedir.

“Teknolojiyle işler kolaylaştı ama hâlâ bazı boşluklar var. Her şey kayıt altına alınıyor, peki ya bu kayıtlar sonra ne oluyor? Bu sistemin sınırlarını da bilmek istiyoruz” (K8). Bu alıntı, dijital sistemlerin işlevselliğine yönelik olumlu değerlendirmeyi içerirken, aynı zamanda sistemin şeffaflık ve veri yönetimi konularındaki açıklık beklentisini de ortaya koymaktadır.

“**Sistem etkinliği ve verimlilik**” ile “**iş yükü azaltma**” temaları arasında doğrudan bir işlevsel ilişki tespit edilmiştir. Dijital sistemlerin operasyonel süreçlerde sunduğu hız, düzen ve müdahale kolaylığı; hem verimliliği artırmakta hem de sahada yürütülen görevlerde fiziksel yükü azaltmaktadır. Bu ilişki, teknolojinin yalnızca destekleyici değil; aynı zamanda görev süreçlerini dönüştürücü bir araç olarak algılandığını göstermektedir.

“**Veri güvenliği ve mahremiyet**” ile “**yapay zekâ ve yüz tanıma**” temaları arasında da güçlü bir bağlantı belirlenmiştir. Katılımcılar, teknolojik sistemlerin sunduğu imkânlara rağmen, bu sistemlerin kişisel veriler üzerindeki etkilerine ve kullanım sınırlarına dair belirsizlikler konusunda kaygılarını dile getirmiştir. Mahremiyetin, yalnızca bireysel alan değil; aynı zamanda sistemin meşruiyetini etkileyen bir unsur olarak değerlendirildiği görülmektedir.

“**Güvende hissetme**”, “**toplumsal farkındalık**” ve “**yaşanabilir şehir**” temaları arasında normatif bir geçişkenlik gözlemlenmiştir. Dijital sistemlerin kent genelinde görünür hâle gelmesi, davranışsal düzeyde farkındalık oluşturmakta; kamusal alanda daha dikkatli hareket edilmesine zemin hazırlamaktadır. Böylece güvenlik sistemlerinin yalnızca teknik değil; aynı zamanda toplumsal düzeni teşvik eden bir yapıya dönüştüğü anlaşılmaktadır.

Ayrıca, “**etik kaygılar**” ve “**hukuki sınırlar**” temalarının, diğer tüm temaların değerlendirilmesinde belirleyici bir arka plan işlevi üstlendiği saptanmıştır. Katılımcılar, sistemin yalnızca operasyonel yönleriyle değil, aynı zamanda nasıl uygulandığı, hangi sınırlar içinde kullanıldığı ve ne tür denetim mekanizmalarına tabi olduğu konularında da değerlendirme yapmıştır.

Genel Değerlendirme: Temalar arasında kurulan bu çok katmanlı ilişki ağı, dijital güvenlik teknolojilerinin yalnızca bir güvenlik aracı değil; aynı zamanda kent

yaşamının psikolojik, etik ve toplumsal katmanlarını etkileyen çok boyutlu bir yapı olarak algılandığını göstermektedir. Katılımcı ifadeleri, bu sistemlerin yalnızca sahaya yönelik değil; aynı zamanda bireyin gündelik deneyimine, karar alma biçimlerine ve toplumsal normlara yönelik etkilerini de görünür kılmıştır.

3.5. TARTIŞMA

Dijital güvenlik sistemlerinin kent güvenliği bağlamında nasıl algılandığı, deneyimlendiği ve değerlendirildiği polis memurlarının anlatıları üzerinden anlamlandırıldığında, dijitalleşmenin güvenlik hizmetlerinin işleyişinde çok yönlü bir dönüşüm yarattığı görülmektedir. Katılımcıların değerlendirmeleri, dijital altyapıların hem operasyonel süreçlerde hem de bireysel ve yönetsel deneyimlerde belirleyici bir unsur hâline geldiğini göstermektedir.

İlk olarak, dijital sistemlerin operasyonel etkinlik, karar alma süreçlerine katkı ve görev planlamasında sağladığı düzen, öne çıkan temalar arasında yer almıştır. Polis memurları tarafından yaygın biçimde dile getirilen değerlendirmeler, teknolojik altyapının geleneksel güvenlik uygulamalarına kıyasla daha hızlı, eşgüdümlü ve tutarlı bir işleyiş sunduğu yönündedir. Bu durum, sistemin yalnızca işlevsel bir araç değil; aynı zamanda yapısal bir dönüşüm mekanizması olarak benimsendiğini göstermektedir.

Teknik boyutun ötesinde, dijital sistemlere yönelik değerlendirmeler; mahremiyet, kişisel alan, gözetlenme hissi ve etik sınırlar gibi kavramları da içerecek şekilde geniş bir çerçevede şekillenmiştir. Polis memurlarının bazı anlatılarında, güvenlikle birlikte gelen izlenme hâlinin, bireysel psikolojide bir tür baskı unsuru oluşturabileceği yönünde görüşler ortaya çıkmıştır. Bu da, dijital güvenlik sistemlerinin yalnızca dışsal bir denetim mekanizması olarak değil; aynı zamanda güvenlik ile kontrol arasında birey tarafından kurulan içsel dengenin bir parçası olarak deneyimlendiğini göstermektedir.

Dijital sistemlerin, hem güvenlik sağlayıcı hem de bireysel sınırları zorlayıcı bir yapı olarak algılanması; katılımcı ifadelerinde sıkça vurgulanan çelişkili bir duruma işaret etmektedir. Güvenliğin tesisine katkı sağlarken, izlenme hissini sürekliliği; bireyde zaman zaman kontrol altında tutulma algısının ağır basmasına

neden olabilmektedir. Bu bağlamda, sistemin kent yaşamındaki yeri yalnızca fiziksel değil; aynı zamanda psikolojik ve toplumsal düzeylerde de yeniden düşünülmelidir.

Toplumsal farkındalık ve davranışsal dönüşüm temaları da dikkat çekici biçimde öne çıkmıştır. Polis memurları tarafından aktarılan görüşlerde, dijital sistemlerin kent genelinde görünürlük kazanmasıyla birlikte, vatandaş davranışlarında belirgin bir değişim gözlemlendiği ifade edilmiştir. Daha temkinli, daha kurallı ve daha dikkatli bir kamusal tutumun geliştiği yönündeki gözlemler, sistemin yalnızca suçla mücadele değil; aynı zamanda normatif düzenin pekiştirilmesinde de rol üstlendiğini göstermektedir. Ancak bu durum, bireylerde sürekli denetleniyor olma hissini yarattığı psikolojik baskı ile iç içe geçmekte; içsel denetim mekanizmalarının aşırı aktifleşmesine neden olabilmektedir.

Dijital güvenlik sistemlerinin kent yaşamına katkısı, yalnızca güvenlik bağlamında değil; aynı zamanda düzen ve yaşam kalitesi ekseninde de değerlendirilmiştir. Sistemin, kent estetiğine ve yapısal bütünlüğe katkı sunduğu, mekânsal kontrolün artmasıyla birlikte kentte daha yaşanabilir bir ortam hissi oluşturduğu yönünde görüşler dile getirilmiştir. Ancak bu olumlu değerlendirmenin yanında, izlenebilirliğin sürekliliği nedeniyle bireyin özne konumundan edilerek pasif birer denetim nesnesine dönüşme riskine de dikkat çekilmiştir. Bu çift yönlü algı, dijital güvenlik politikalarının yalnızca teknoloji merkezli değil; insan merkezli, hak temelli ve katılımcı bir perspektifle de şekillendirilmesi gerektiğini ortaya koymaktadır.

Katılımcılar tarafından dile getirilen önemli bir diğer husus, sistemin hukuki sınırlarına dair belirsizliktir. Gözetim sistemlerinin hangi yasal zeminde faaliyet gösterdiği, elde edilen verilerin nasıl işlendiği ve kimler tarafından ne amaçla kullanıldığı gibi sorular, sistemin teknik yeterliliğinin ötesinde, meşruiyet zemininin tartışılmasını da gerekli kılmaktadır. Şeffaflık ve hesap verebilirliğe duyulan ihtiyaç, yalnızca teknolojik yeterlilik değil; aynı zamanda yönetim ilkeleri açısından da sistemin desteklenmesi gerektiğine işaret etmektedir.

Araştırmanın sınırlılıkları arasında, veri toplama sürecinin tek bir ilde yürütülmüş olması yer almaktadır. Kütahya ilinde görev yapan polis memurlarının anlatılarına dayanan bu çalışma, bulguların farklı coğrafi ya da yönetsel bağlamlara genellenmesini sınırlamakla birlikte; yerel güvenlik deneyimlerinin özgün doğasını

anlamak açısından derinlemesine bir bakış sunmaktadır. Mikro ölçekte elde edilen nitel veriler, geniş ölçekli nicel araştırmaların ulaşamayacağı içeriksel zenginlik üretmiş; kent güvenliğiyle ilgili bireysel algıların ve uygulama pratiklerinin daha iyi anlaşılmasına katkı sağlamıştır.

Dijital güvenlik sistemlerinin **teknik boyutu**, polis memurlarının aktardığı anlatılar üzerinden değerlendirildiğinde, operasyonel işleyişte sağladığı hız, koordinasyon ve doğruluk açısından önemli bir işlev gördüğü anlaşılmaktadır. Kamera sistemlerinden veri analiz yazılımlarına kadar uzanan dijital araçların, olaylara müdahale süresini azalttığı, görev dağılımını daha verimli hale getirdiği ve karar alma süreçlerini daha rasyonel biçimde yönlendirdiği ifade edilmiştir. Bu sistemlerin, sahada görev yapan güvenlik personelinin olaylara anlık ve bütüncül erişimini mümkün kıldığı görülmektedir. Teknik yeterliliğin bu şekilde yüksek bir işlevsellik düzeyi sunması, dijital altyapının kent güvenliği açısından vazgeçilmez bir araç haline gelmesini beraberinde getirmiştir.

Ancak dijital sistemlerin etkisi, yalnızca teknik performansla sınırlı kalmamaktadır; **sosyo-kültürel düzeyde** de belirgin dönüşümler yaratmaktadır. Polis memurlarının anlatılarında, sistemlerin kent genelindeki görünürlüğünün vatandaş davranışları üzerinde düzenleyici bir etki oluşturduğu, bireylerin kamusal alandaki tutumlarında daha dikkatli ve kurallara uygun davranışlar sergilemeye yöneldiği belirtilmiştir. Bu gözlemler, kentte hâkim olan kültürel normların, dijital gözetim algısıyla yeniden şekillendiğini göstermektedir. Ancak bu durum, aynı zamanda sürekli denetim altında olduğu hissini pekiştirerek bireylerde psikolojik bir baskı ve içsel kontrol mekanizmalarının aşırı aktivasyonu gibi sonuçlara da yol açabilmektedir. Bu çelişkili yapı, dijital güvenlik sistemlerinin toplumsal yaşantı üzerindeki kültürel etkilerini görünür kılmaktadır.

Bunun yanında, dijital güvenlik sistemlerinin **yönetimsel etkileri** de polis memurlarının değerlendirmelerinde önemli bir yer tutmaktadır. Teknolojik sistemler sayesinde görev takibinin daha sistematik hâle geldiği, denetim süreçlerinin hızlandığı ve yöneticiler ile saha personeli arasında veri akışının daha etkin kurulduğu ifade edilmiştir. Bu bağlamda, dijitalleşmenin kent güvenliği yönetiminde merkezi bir rol üstlendiği, özellikle karar verme süreçlerini şeffaflaştırarak yönetsel etkililiği artırdığı söylenebilir. Ancak bazı anlatılarda, artan dijital denetimin, özellikle personel

üzerinde sürekli izlenme baskısı yaratarak görev motivasyonunu olumsuz etkileyebildiğine de dikkat çekilmiştir. Bu durum, yönetsel verimliliğin, insan faktörü gözetilmeden yürütülmesinin çeşitli riskler barındırabileceğini göstermektedir.

Dijital güvenlik sistemlerinin değerlendirilmesinde **etik boyut** ise üzerinde hassasiyetle durulması gereken bir diğer önemli katmandır. Katılımcıların bir kısmı, bireylerin özel yaşam alanlarının gözetlenme ihtimalinin, sistemin güvenlik işlevi kadar tartışmalı bir yönünü de ortaya çıkardığını vurgulamıştır. Gözetim araçlarının hangi yasal zeminde çalıştığı, elde edilen verilerin kimler tarafından ne şekilde kullanıldığı gibi sorular, sistemin teknik başarısından ziyade meşruiyetine dair sorgulamaları beraberinde getirmiştir. Etik sınırların belirsizliği, bireylerin dijital sistemleri yalnızca güvenlik sağlayan araçlar olarak değil; aynı zamanda kontrolü elinde bulunduran güç mekanizmaları olarak da algılamasına neden olmaktadır. Bu da teknolojinin insan hakları, mahremiyet ve özgürlükler bağlamında yeniden tartışılmasını zorunlu kılmaktadır.

Bu araştırmada, dijital güvenlik sistemlerinin kent güvenliği bağlamında yalnızca teknik etkinlik düzeyinde değil; aynı zamanda **sosyo-kültürel, yönetsel ve etik boyutlarıyla birlikte** nasıl algılandığı, deneyimlendiği ve anlamlandırıldığı derinlemesine incelenmiştir. Teknik olarak hızlı müdahale, verimli planlama ve yüksek operasyonel koordinasyon sağladığı görülse de; sistemlerin toplumsal yaşantıya etkisi, birey psikolojisi ve yönetim anlayışı üzerinde çok katmanlı sonuçlar doğurduğu ortaya konmuştur.

Dijital güvenlik sistemlerinin, vatandaş davranışlarını şekillendiren, toplumsal normları dönüştüren ve hatta kamusal alan algısını yeniden inşa eden bir araç haline geldiği anlaşılmıştır. Yönetsel düzeyde verimliliği artırırken, aynı zamanda çalışanlar üzerinde sürekli izlenme algısı oluşturduğu; etik düzlemde ise bireysel mahremiyet, veri güvenliği ve sistemin meşruiyeti gibi önemli sorgulamaları beraberinde getirdiği görülmüştür.

Sonuç olarak, dijital güvenlik sistemlerinin kent güvenliğine katkısı, yalnızca teknik işlevsellikle sınırlı kalmamakta; aynı zamanda toplumsal yapı, yönetsel süreçler ve bireysel haklar üzerinde çok boyutlu bir etki üretmektedir. Bu nedenle, sistemin değerlendirilmesi, sadece teknoloji merkezli bir bakışla değil; insan merkezli, hak temelli ve katılımcı bir güvenlik paradigmasıyla yapılmalıdır. Dijitalleşmenin kent

güvenliği pratiklerinde yol açtığı dönüşüm, salt bir teknolojik ilerleme olarak değil; aynı zamanda yeni bir yönetim biçimi ve toplumsal sözleşme anlayışı olarak kavranmalı; bu dönüşümün yönetimi, güvenlik ile özgürlük arasında sağlıklı bir denge kuran etik bir zemin üzerine inşa edilmelidir.

3.5.1. KGYS'nin Etkililiğine Dair Görüşler

Dijital dönüşüm olgusu, yalnızca teknolojik araçların kurumlara entegrasyonu ile sınırlı kalmayıp, aynı zamanda çalışan deneyimlerini, iş yapış biçimlerini ve kurumsal dinamikleri kökten etkileyen bir dönüşüm olarak değerlendirilmelidir. Bu bağlamda, özellikle kent güvenliği gibi yüksek hassasiyet gerektiren alanlarda kullanılan dijital sistemlerin, çalışanlar nezdinde nasıl algılandığı ve bu sistemlerin örgütsel yapıya etkileri önemli bir araştırma konusu hâline gelmiştir.

KGYS gibi dijital denetim ve yönetim mekanizmalarının sahada görev yapan memurlar üzerindeki etkilerinin anlaşılabilmesi için, uygulayıcı aktörlerin doğrudan deneyimlerinden beslenen niteliksel veri setlerine ihtiyaç duyulmaktadır. Bu ihtiyaç doğrultusunda gerçekleştirilen görüşmeler aracılığıyla, kamu çalışanlarının KGYS sistemine ilişkin algıları, deneyimleri ve değerlendirmeleri sistematik biçimde analiz edilmiştir.

Yapılan analizde; teknolojik uyum, görev tanımlarının dijitalleşme sürecinde aldığı biçim, yönetsel iletişim yapıları, iş yükü dönüşümü, psikolojik etkiler ve kurumsal aidiyet gibi temalar ön plana çıkmıştır. Katılımcıların dile getirdiği görüşler, dijital sistemlerin yalnızca işlevsel değil, aynı zamanda sosyo-psikolojik sonuçlar da doğurduğunu açıkça ortaya koymuştur. Bu çerçevede, dijital güvenlik sistemlerinin başarısının teknik yeterlilikten ziyade, insan odaklı bir dönüşüm stratejisiyle ne ölçüde bütünleştiğiyle doğrudan ilişkili olduğu söylenebilir.

Tablo 1.***Dijital Dönüşüm ve KGYS Bağlamında Görüşlerin Tematik Analizi***

Tema	Görüş Özeti	Katılımcı(lar)
Teknolojik Altyapı ve Uyum	KGYS ile birlikte teknolojik dönüşüme uyum sağlandığı belirtilmiştir.	K1, K4, K9, K14
	Sistemin teknik aksaklıklar ve kullanıcı zorlukları barındırdığı ifade edilmiştir.	K2, K6, K11, K17
Görev Tanımı ve Rol Netliği	Dijital sistemlerle birlikte görevlerin daha net hale geldiği belirtilmiştir.	K3, K12, K18
	Görevlerin teknolojiyle daha karmaşıklaştığı ve belirsizleştiği vurgulanmıştır.	K5, K7, K10, K15
Yönetimsel İletişim ve Koordinasyon	Amirlerle iletişimin KGYS sonrası daha sistematik hale geldiği aktarılmıştır.	K1, K8, K13
	Dijital raporlama ve izleme süreçlerinin iletişim kopukluklarına yol açtığı belirtilmiştir.	K2, K3, K17, K20
İş Yükü ve Performans	Otomasyonun iş yükünü azalttığı ifade edilmiştir.	K4, K9, K16
	Sistemin iş yükünü artırdığı, sürekli raporlamaya dönüştüğü belirtilmiştir.	K6, K11, K15, K19
Psikolojik Etkiler	Dijital sistemin denetim duygusu yarattığı ve çalışanı baskı altında hissettirdiği bildirilmiştir.	K7, K10, K18, K20
	Sistem sayesinde güvenlik algısının yükseldiği ve görev bilincinin arttığı vurgulanmıştır.	K5, K12, K14
Kurumsal Aidiyet ve Sahiplenme	Dijitalleşme ile birlikte modernleşen yapının aidiyet hissini artırdığı ifade edilmiştir.	K1, K9, K13, K19
	Sürekli değişen sistemlerin yabancılaşmaya neden olduğu dile getirilmiştir.	K2, K6, K8, K17

a. Teknolojik Altyapı ve Uyum

Dijital dönüşüm süreciyle birlikte KGYS sisteminin işleyişe entegrasyonu, birçok katılımcı tarafından olumlu bir gelişme olarak değerlendirilmiştir. Özellikle teknolojik altyapının, olaylara müdahale sürecini hızlandırdığı, iş akışını daha sistematik hâle getirdiği ve kurumun modern bir yapıya kavuştuğu belirtilmiştir. Nitekim “*KGYS ile olaylara müdahale süremiz azaldı, sistem hızlı çalışıyor*” (K1) ve “*KGYS ile daha çağdaş bir yapıda çalıştığımızı hissediyoruz*” (K14) ifadeleri, bu olumlu algıyı yansıtmaktadır.

Bununla birlikte, sistemin teknik altyapısına ilişkin bazı eleştirilerin de dile getirildiği görülmektedir. Katılımcılar tarafından sistemin zaman zaman yavaşladığı, donma ve veri kaybı gibi problemler yaşandığı ifade edilmiştir. Bu durum, “*Sistem sık sık donuyor, kayıtlar eksik çıkıyor*” (K2) ve “*Veri yoğunluğu olunca sistem çok yavaşlıyor*” (K17) gibi görüşlerle açıkça ortaya konmuştur. Ayrıca bazı kullanıcıların

sistemi etkin kullanmakta zorlandıkları da belirtilmiştir “*Bazı arkadaşlar sistemi kullanmakta zorlanıyor*” (K6). Dolayısıyla, teknolojik entegrasyonun olumlu yönlerine karşın, altyapısal sürdürülebilirliğin henüz yeterince sağlanamadığı anlaşılmaktadır.

b. Görev Tanımı ve Rol Netliği

KGYS sisteminin görevlere getirdiği yapısal düzenlemeler, bazı çalışanlar tarafından iş tanımlarının daha netleşmesi yönünde değerlendirilmiştir. Özellikle “*KGYS ile birlikte görevlerimiz daha sistematik hale geldi*” (K3) ve “*Görevim ekran başında daha anlamlı hâle geldi*” (K12) şeklindeki ifadeler, sistemin görevleri belirginleştirme işlevine sahip olduğunu ortaya koymaktadır.

Buna karşılık, görev tanımındaki dijitalleşmenin bazı çalışanlar tarafından karmaşa ve belirsizlik yaratıcı bir unsur olarak algılandığı da dikkat çekmektedir. “*Sahada görev yaparken daha netti, şimdi karışıklaştı*” (K5) ve “*Bir gün sahadayız, ertesi gün sistem başında. Net değil*” (K15) ifadeleri, teknolojik geçişin görevlerin içeriği ve kapsamı üzerinde kafa karışıklığına yol açabileceğini göstermektedir. Bu bağlamda, görev tanımlarının dijital dönüşüm süreciyle yeniden yapılandırılmasının gerekliliği ortaya çıkmaktadır.

c. Yönetsel İletişim ve Koordinasyon

Katılımcıların önemli bir kısmı, KGYS sisteminin yönetsel iletişim süreçlerini daha sistematik ve kayıt altına alınabilir kıldığı yönünde değerlendirmelerde bulunmuştur. Örneğin “*Yöneticilerle iletişimimiz daha net, çünkü her şey sistemde yazılı*” (K1) ve “*Artık talimatlar dijital geliyor, takip etmesi kolay*” (K8) şeklindeki ifadeler, yönetsel koordinasyonun şeffaflaştığını ortaya koymaktadır.

Ancak öte yandan, sistem temelli iletişimin yüz yüze etkileşimi azalttığı ve bazı durumlarda iletişim kopukluklarına neden olduğu da dile getirilmiştir. “*Sadece sistem mesajları geliyor, insan teması azaldı*” (K17) ve “*Yöneticinin sesini duymayı unuttuk neredeyse*” (K20) ifadeleri, bu teknolojik yabancılaşma durumuna işaret etmektedir. Bu durum, dijitalleşme ile birlikte yönetsel etkileşimde insani unsurların kaybolma riskine dikkat çekmektedir.

d. İş Yükü ve Performans

Otomasyon sistemlerinin iş yükünü azalttığı yönündeki algılar, bazı katılımcılar tarafından vurgulanmıştır. Özellikle “*Saha koşturması azaldı, sistem işleri*

üstleniyor” (K9) ve *“Raporlar otomatik geliyor, zaman kazanıyoruz”* (K16) ifadeleri, sistemin zaman yönetimi ve görev dağılımı açısından avantajlar sunduğunu göstermektedir.

Bununla birlikte, dijital sistemlerin getirdiği sürekli raporlama zorunluluğunun iş yükünü artırdığına dair görüşler de mevcuttur. *“Sürekli rapor isteniyor, yorucu oluyor”* (K6) ve *“Sistem işimizi artırdı, kolaylaştırmadı”* (K19) gibi ifadeler, bu çelişkili durumu gözler önüne sermektedir. Ayrıca, *“Hem sahada hem sistemde çalışmak bizi zorluyor”* (K11) görüşü, dijitalleşmenin yükü ikiye katladığı algısını pekiştirmektedir. Bu bağlamda, sistem performansının çalışanlara etkisinin kişisel deneyimlere göre oldukça değişkenlik gösterdiği anlaşılmaktadır.

e. Psikolojik Etkiler

Katılımcıların önemli bir bölümü, KGYS sisteminin denetleyici yapısı nedeniyle psikolojik baskı unsuru oluşturduğunu belirtmiştir. *“Sürekli izleniyor olmak tedirgin edici”* (K7) ve *“Her adımımızı izliyorlar, bu baskı yaratıyor”* (K20) gibi görüşler, dijital gözetimin çalışanlar üzerinde sürekli bir stres ortamı oluşturduğunu göstermektedir. Bu tür denetim algısı, özellikle sahadaki performans üzerinde olumsuz etkilere neden olabilmektedir.

Buna karşın, bazı katılımcılar sistemin güvenlik algısını artırarak görev bilincini yükselttiğini ifade etmiştir. *“İşimi ciddiyetle yapıyorum çünkü kayıt altındayım”* (K12) ve *“Görev bilincim arttı, çünkü her şey sistemde görünür”* (K14) ifadeleri, dijital izlemenin kimi zaman isteklendirme artırıcı bir unsur hâline de gelebileceğini ortaya koymaktadır. Bu bağlamda, sistemin psikolojik etkilerinin kişisel algı farklılıklarına göre değiştiği sonucuna varılabilir.

f. Kurumsal Aidiyet ve Sahiplenme

Dijital sistemlerin kuruma olan aidiyet duygusunu pekiştirdiği yönünde bazı değerlendirmeler yapılmıştır. Özellikle *“Modern sistemlerde çalışmak kuruma olan güvenimi artırdı”* (K1) ve *“Bu sistem sayesinde kuruma daha bağlı hissediyorum”* (K19) gibi ifadeler, dijital dönüşümün kurumsal sahiplenmeye katkı sunduğunu göstermektedir.

Ancak öte yandan, sistemin sık sık değişmesi, çalışanlar üzerinde yabancılaşma duygusu oluşturabilmektedir. *“Sistem sürekli değişiyor, yabancılaşıyoruz”* (K2) ve *“İnsan yerine sistemle muhatapız, bu uzaklaştırıyor”* (K6) gibi ifadeler,

dijitalleşmenin kurumsal aidiyeti zedeleyebileceğine işaret etmektedir. Bu nedenle, sistemlerin sürdürülebilirliği kadar, kullanıcı dostu olması ve çalışanla etkileşimi desteklemesi de önemli hâle gelmektedir.

Katılımcılar tarafından KGYS'ye ilişkin etkililik algılarının genel olarak olumlu olduğu görülmekle birlikte, sistemin pratikteki işleyişine ve toplumsal yansımalarına dair çeşitli eleştiri ve önerilerin de dile getirildiği tespit edilmiştir. Yapılan nitel çözümleme sonucunda sistemin; suçun önlenmesi, olayların aydınlatılması, müdahale hızının artırılması ve güvenlik hissini güçlendirilmesi gibi çok yönlü işlevlere sahip olduğu ifade edilmiştir. Bu bulgular, KGYS'nin sadece teknik değil, aynı zamanda sosyo-psikolojik etkileri olan bir güvenlik aygıtı olduğunu göstermektedir.

Katılımcıların önemli bir kısmı, sistemin olaylara erken müdahale imkânı sunduğunu belirtmiş; özellikle olayların gerçekleşme anında ya da hemen sonrasında hızlı çözüm sağlayan bir yapı oluşturduğuna dikkat çekilmiştir. Örneğin bir katılımcı, *“Zabita veya polis olay yerine gelmeden önce kameralar sayesinde müdahale ediliyor”* (K1) ifadesiyle zaman tasarrufuna ve sistemin anlık müdahale kapasitesine vurgu yapmıştır. Benzer şekilde, *“Geçen gün bir olay oldu, kamera sayesinde kim olduğu anlaşıldı”* (K4) şeklindeki bir diğer değerlendirme, sistemin olay çözümleme süreçlerinde oynadığı destekleyici rolü ortaya koymaktadır. Bu tür görüşlerin, gözetim teknolojilerinin özellikle olay öncesi ve sonrası kayıtlarla delil üretme ve hızlı tespit sağlama potansiyelini literatürde savunan çalışmalarla örtüştüğü görülmektedir (Lyon, 2003; Murakami Wood & Graham, 2006).

Katılımcı ifadeleri, yalnızca sistemin pratik yararlarına değil, aynı zamanda bu yararların bireysel haklar ve mahremiyet üzerinde oluşturabileceği baskıya da işaret etmektedir. Bu bağlamda, bazı katılımcılar sistemin sürekli izleme özelliğinden kaynaklı tedirginliğe dikkat çekmiştir. Örneğin, *“Mahremiyeti ne kadar ihlal ediyor bilmiyoruz ama gerekli bir sistem”* (K20) ifadesi, güvenlik ile özgürlük arasındaki hassas dengeye yönelik bir farkındalığı ortaya koymaktadır. Benzer biçimde, *“Her adımımızı izliyorlar, bu baskı yaratıyor”* (K20) ve *“Kameralar hep açık, hata yaparsak cezalandırılıyor”* (K10) gibi ifadeler, KGYS'nin sadece denetleyici değil, aynı zamanda psikolojik baskı yaratan bir mekanizma olarak da deneyimlendiğini göstermektedir. Zuboff (2019), bu durumu dijital gözetim sistemlerinin aynı anda hem

güvenlik üretmesi hem de bireylerin davranışlarını sürekli izlenebilir kılacak biçimde yapılandırılmasıyla açıklamaktadır.

Sistemin caydırıcılık etkisi de sıkça dile getirilen bir diğer temayı oluşturmaktadır. Katılımcılardan biri, “*Orada kamera olduğunu görünce kendine çeki düzen veriyor*” (K5) ifadesiyle birey davranışlarında oluşan dönüşüme dikkat çekmiş; sistemin pasif bir izleme aracı olmaktan öte, davranışsal bir düzenleyici rol üstlendiğini ima etmiştir. Bu tür değerlendirmeler, Foucault’nun (1975) panoptikon kavramsallaştırmasıyla doğrudan ilişkilendirilebilecek niteliktedir. Foucault, gözetimin sürekli değil, olasılık dâhilinde olduğunda bile birey davranışlarını disipline edeceğini savunmuştur. Bu bağlamda KGYS, modern gözetim araçlarının yalnızca fiziksel değil, aynı zamanda zihinsel bir düzen oluşturduğu mekanizmalar arasında konumlanmaktadır.

Öte yandan, sistemin teknik altyapısına yönelik bazı eleştiriler de dile getirilmiştir. Katılımcılardan biri, “*Köşe başına koymuşlar, birçok olayı görmüyor*” (K2) ifadesiyle kameraların mekânsal konumlandırmasına ilişkin eksiklikleri vurgulamıştır. Benzer eleştiriler “*Kamera görüntülerini açarken sistem kilitlenebiliyor*” (K11) ya da “*Veri yoğunluğu olunca sistem çok yavaşlıyor*” (K17) gibi görüşlerle de desteklenmiştir. Bu bulgular, sistemin sadece varlığıyla değil, erişilebilirliği ve etkinliğiyle de sorgulanması gerektiğini ortaya koymaktadır. Smith (2007) tarafından da vurgulandığı üzere, gözetim sistemlerinin genellikle "riskli" görülen alanlara yoğunlaştırılması, mekânsal adalet bağlamında dengesizlikler yaratabilmektedir.

Sonuç olarak, KGYS’ye ilişkin katılımcı değerlendirmeleri, sistemin işlevsel boyutlarının yanı sıra, teknik yeterlilik, bireysel mahremiyet, psikolojik etkiler ve kurumsal güven algısı gibi çok katmanlı unsurları da içeren kapsamlı bir bakış açısı sunmaktadır. Sistem, kamu düzeninin sağlanmasında önemli avantajlar sunmakla birlikte, özgürlük-güvenlik ikilemi başta olmak üzere çeşitli etik ve yapısal sorunları da beraberinde getirmektedir. Bu bağlamda, KGYS gibi dijital güvenlik uygulamalarının etkililiği yalnızca olay çözümü kapasitesiyle değil, aynı zamanda toplumun değerleri, hak arayışları ve teknolojiye olan güveniyle birlikte değerlendirilmelidir. Bu değerlendirme, hem mevcut literatürle tutarlılık göstermekte

hem de dijital güvenlik sistemlerinin gelecekteki tasarım süreçlerine ışık tutabilecek niteliktedir.



SONUÇ VE ÖNERİLER

Bu araştırmada, dijitalleşme sürecinin kent güvenliği politikaları üzerindeki etkileri, (KGYS) örneği ekseninde nitel yöntemler aracılığıyla irdelenmiştir. Bu bağlamda, katılımcıların kişisel deneyimleri, sistem algıları ve bu teknolojik yapıların toplumsal düzeydeki yansımaları çok katmanlı bir perspektifle değerlendirilmiştir. Araştırma kapsamında elde edilen veriler, dijital güvenlik sistemlerinin yalnızca teknik bir altyapı unsuru olmakla kalmayıp, aynı zamanda birey-devlet ilişkilerini dönüştüren, toplumsal denetim mekanizmalarını yeniden şekillendiren, mahremiyet algısını etkileyen ve etik tartışmaları gündeme taşıyan çok boyutlu araçlar olduğunu ortaya koymuştur.

Görüşme verilerine dayanarak, KGYS'nin kentteki güvenlik uygulamalarında organize, hızlı ve etkin müdahalelere imkân tanıyan bir sistem olarak algılandığı belirlenmiştir. Katılımcılar, söz konusu sistemin suçun önlenmesi, olaylara anlık müdahale imkânı sağlama, delil toplama süreçlerine katkı sunma ve kamusal alanlarda caydırıcılığı artırma gibi işlevsel açılardan önemli faydalar sunduğunu ifade etmiştir. Ancak bununla birlikte, sistemin kamusal alanda bireylerin davranışlarını dönüştürdüğüne, sürekli gözetlenme duygusunun bireylerde psikolojik ve sosyolojik etkiler yarattığına yönelik bulgular da dikkate değerdir. Bu durum, güvenliğin sağlanması sürecinde özgürlük alanlarının nasıl daraltılabileceğine ilişkin kritik bir sorgulamayı da beraberinde getirmektedir.

Çalışmada, “güvende olma” ve “izlenme” duygularının sıklıkla iç içe geçtiği deneyimlerin öne çıktığı ve bu durumun güvenlik ile özgürlük arasındaki kırılgan dengeyi görünür kıldığı belirlenmiştir. Elde edilen bulgular, dijital gözetim sistemlerinin bireylerin kamusal alandaki davranışlarını yalnızca güvenlik algısı üzerinden değil; aynı zamanda sürekli denetlenme hissiyle şekillendirdiğini göstermektedir. Bu durum, dijital güvenlik teknolojilerinin tarafsız araçlar olmaktan ziyade, toplumsal ilişkiler ve güç dinamikleri üzerinde dönüştürücü bir etkiye sahip yapılar olarak değerlendirilmesi gerektiğine işaret etmektedir. Dolayısıyla, söz konusu sistemlerin güvenliği sağlama işlevinin ötesinde, bireysel mahremiyet algısı ve toplumsal denge üzerinde belirleyici bir rol oynadığı sonucuna ulaşılmıştır.

Kuramsal düzeyde çalışma, gözetim toplumuna dair literatürle güçlü bir etkileşim kurmuştur. Michel Foucault'nun panoptikon modeliyle ifade ettiği denetim biçimi ile Shoshana Zuboff'un dijital gözetim kapitalizmine yönelik eleştirileri, KGYS örneğinde somut karşılıklarını bulmuştur. Elde edilen veriler, bu sistemlerin yalnızca güvenliği sağlamaya yönelik teknik araçlar olmadığını, aynı zamanda bireylerin davranışlarını disipline eden ve normatif uyumu sağlayan bir iktidar mekanizması işlevi gördüğünü ortaya koymuştur. Bu çerçevede araştırmanın teorik özgünlüğü, dijital güvenlik teknolojilerinin teknik faydalarına odaklanmakla yetinmeyip, onların toplumsal yapı, iktidar ilişkileri ve etik sorumluluklarla nasıl iç içe geçtiğini somut biçimde analiz etmesinde yatmaktadır.

Araştırma sürecinde uygulamaya yönelik bazı yapısal sorunların da mevcut olduğu belirlenmiştir. Özellikle kameraların konumlandırılmasındaki düzensizlik, görüntü erişiminde yaşanan gecikmeler ve veri yönetimi süreçlerindeki şeffaflık eksikliği, sistemin bütünsel verimliliğini zayıflatan unsurlar olarak öne çıkmıştır. Katılımcılar, kişisel verilerin nasıl işlendiği, kimlerin bu verilere erişebildiği ve veri güvenliğine dair yasal altyapının ne ölçüde tanımlandığı konularında bilgi eksikliği yaşadıklarını ifade etmiştir. Bu durum, sistemin toplumsal meşruiyeti ve bireysel güven duygusu açısından potansiyel bir tehdit olarak değerlendirilmiştir.

Sonuç itibarıyla, KGYS benzeri dijital güvenlik sistemlerinin yalnızca operasyonel düzeyde değil; aynı zamanda etik, hukuki, psikolojik ve sosyolojik açılardan da ele alınmasının gerekliliği bu çalışmayla bir kez daha vurgulanmıştır. Bu doğrultuda, söz konusu araştırma, hem uygulayıcı kurumlara hem de akademik çevrelere yönelik olarak önemli çıkarımlar sunmaktadır. Özellikle dijital güvenlik teknolojilerinin kent yaşamına entegrasyonu sürecinde; toplumsal meşruiyetin sağlanması, bireylerin veri güvenliği endişelerinin giderilmesi ve mahremiyet hakkının yeniden tanımlanması, hem politika yapıcılar hem de sosyal bilim araştırmacıları için kaçınılmaz bir sorumluluk alanı olarak öne çıkmaktadır.

Bu doğrultuda, hem araştırma bulgularından hem de ilgili literatürden hareketle aşağıdaki önerilere yer verilmiştir:

Öneriler

Mahremiyetin Korunmasına Yönelik Hukuki ve Etik Önlemlerin Güçlendirilmesi: Dijital güvenlik sistemlerinin, bireylerin özel yaşam alanlarını ihlal

etmeyecek şekilde düzenlenmesi, temel bir gereklilik olarak öne çıkmaktadır. KGYS benzeri gözetim teknolojilerinin uygulama alanlarında, kişisel mahremiyetin korunmasına yönelik açık ve bağlayıcı düzenlemelerin hayata geçirilmesi zorunluluk arz etmektedir. Avrupa Birliği'nin yürürlüğe koyduğu Genel Veri Koruma Tüzüğü (GDPR), bu konuda kapsamlı bir örnek teşkil etmekte olup; gözetim sistemlerine dair veri toplama, işleme ve saklama süreçlerinin açık, denetlenebilir ve kullanıcı merkezli esaslara göre yapılandırılmasını sağlamaktadır. Türkiye özelinde ise kişisel verilerin korunmasına dair mevcut yasal çerçevenin güncellenmesi; gözetim sistemleri için hesap verebilirlik, şeffaflık ve etik sınırların açıkça tanımlandığı, bağlayıcı politika belgelerinin oluşturulması ile desteklenmelidir. Bu bağlamda, ilgili kurumlar nezdinde etik kurul mekanizmalarının devreye alınması ve karar süreçlerine toplumsal paydaşların katılımının sağlanması önem arz etmektedir.

Toplumun Dijital Gözetim Konusunda Bilinçlendirilmesine Yönelik Yaygınlaştırıcı Stratejiler: Gözetim sistemlerinin etkili ve meşru bir biçimde işlemesi, yalnızca teknik yeterlilikle değil; aynı zamanda kamuoyunun konuya ilişkin bilgi düzeyiyle de doğrudan ilişkilidir. Bu nedenle, toplumun farklı kesimlerinin dijital gözetim teknolojileri hakkında bilinçlendirilmesine yönelik çok yönlü stratejilerin geliştirilmesi gerekmektedir. Nitekim Amerika Birleşik Devletleri'nde bazı eyaletlerde gözetim sistemlerinin kurulumu öncesinde halkın katılımıyla bilgilendirme toplantıları düzenlenmesi zorunlu tutulmuştur. Benzer bir yaklaşımın Türkiye'de de benimsenmesi; kamuoyunu aydınlatan iletişim kampanyalarının yaygınlaştırılması, yerel halkla yürütülecek danışma süreçlerinin sistematikleştirilmesi ve dijital vatandaşlık bilincini temel alan eğitim programlarının müfredata dâhil edilmesiyle mümkün olabilecektir. Böylece, gözetim teknolojilerine yönelik toplumsal kabullenişin rızaya dayalı biçimde oluşması sağlanabilecektir.

Toplumsal Temelli Etki Analizlerinin Derinleştirilmesi: Araştırma bulguları, dijital gözetim sistemlerinin bireyler üzerindeki etkilerinin homojen olmadığını ve farklı algısal tepkiler doğurabildiğini ortaya koymuştur. Gözetim teknolojilerine yönelik yaklaşımın, kullanıcıların deneyimsel geçmişleri ve sistemle kurdukları etkileşim biçimleri doğrultusunda çeşitlilik arz ettiği görülmüştür. Bu durum, söz konusu sistemlerin yalnızca güvenlik eksenli değerlendirilmesinin yetersiz olduğunu; aynı zamanda toplumsal yapıyla, bireysel algılarla ve psikososyal

faktörlerle olan etkileşimlerinin de dikkate alınması gerektiğini göstermektedir. Avrupa’da bazı ülkelerde bu kapsamda kurulan bağımsız araştırma birimleri aracılığıyla, gözetim teknolojilerinin toplumsal etkilerine yönelik çok boyutlu değerlendirme süreçlerinin kurumsallaştırıldığı görülmektedir. Benzer şekilde, farklı toplumsal grupların dijital güvenlik sistemleriyle kurdukları ilişkilere dair psikolojik, davranışsal ve sosyolojik yönelimlerin ayrıntılı biçimde analiz edilmesi; elde edilecek verilerin politika oluşturma süreçlerine bilgi temelli katkı sunması açısından önem arz etmektedir.

Kentsel Doku ile Uyumlu Bir Sistem Entegrasyonu Sürecinin Benimsenmesi: Dijital güvenlik sistemlerinin kent mekânına entegre edilmesi sürecinde, yalnızca teknik gerekliliklerin değil; aynı zamanda estetik, mekânsal adalet ve kullanım yoğunluğu gibi unsurların da dikkate alınması gerekmektedir. Fiziksel kent dokusuyla uyumlu bir kamera yerleşim planlaması, hem görsel bütünlüğün korunmasını hem de kamusal alanlarda hissedilen güvenliğin artırılmasını mümkün kılacaktır. İngiltere’de uygulanan CPTED (Çevresel Tasarımla Suç Önleme) yaklaşımı doğrultusunda, gözetim sistemleri yalnızca teknik değil; aynı zamanda sosyokültürel ve psikolojik etkileri göz önünde bulundurularak planlanmaktadır. Türkiye’de de benzer bir yöntem benimsenmeli; kamusal alanlarda kamera yerleşimi kararları, görünürlük, mahremiyet algısı ve alan kullanım sıklığı gibi değişkenlerle birlikte çok disiplinli bir yaklaşımla ele alınmalıdır.

Veri Yönetimi Süreçlerinde Şeffaflık ve Denetim Esaslı Kurumsal Yapıların Tesisi: Dijital güvenlik sistemlerinde toplanan verilerin hangi aktörler tarafından, hangi amaçlarla kullanıldığına dair bilgiye erişimin sınırlı olması, sistemin meşruiyeti açısından ciddi bir sorun teşkil etmektedir. Bu nedenle, veri yönetimine dair süreçlerin bağımsız gözetim mekanizmaları aracılığıyla denetlenebilir hâle getirilmesi elzemdir. ABD’nin çeşitli eyaletlerinde bu amaçla oluşturulmuş bağımsız denetim kurulları, gözetim sistemlerinin veri kullanımı konusunda kamuoyunu bilgilendiren yıllık raporlar yayımlamaktadır. Türkiye’de de benzer bir modelin hayata geçirilmesi; düzenli raporlama, kamuya açık şeffaflık beyanları ve veri sorumlularına dair açık tanımlar yoluyla güven ilişkisini güçlendirecektir. Böylelikle hem bireysel hakların korunması hem de kamu güvenliği uygulamalarının toplumsal meşruiyeti sağlanabilecektir.

Uygulanabilir Etik Rehberlerin Oluřturulması ve Eđitimle Desteklenmesi:

Yasal çerçevenin ötesine geçen, uygulayıcıların karar alma süreçlerine rehberlik edecek etik ilkelerin oluşturulması büyük önem arz etmektedir. Avrupa Konseyi ve OECD gibi uluslararası kuruluşlar tarafından yayımlanan etik ilkeler, dijital güvenlik teknolojilerinin insan haklarına duyarlı bir şekilde kullanımını teşvik etmektedir. Türkiye’de de bu doğrultuda hareket edilerek, sahada görev yapan kolluk kuvvetleri ve ilgili personelin etik kodlar çerçevesinde yönlendirilmesini sağlayacak kapsamlı rehber belgeler hazırlanmalıdır. Bu belgeler, yalnızca teorik çerçeve sunmakla kalmamalı; aynı zamanda uygulamalı eğitimlerle desteklenerek, dijital gözetim pratiklerinin etik ilkeler doğrultusunda şekillendirilmesine katkı sağlamalıdır. Söz konusu eğitimler hizmet içi programlara entegre edilmeli ve düzenli olarak güncellenmelidir.

KAYNAKÇA

- Ackerman, W. V. (1998). Socioeconomic correlates of increasing crime rates in smaller communities. *The Professional Geographer*, 50(3), 372-387.
- Akmeşe, S. (2020). Kamuda dijital dönüşümün siber güvenlik ve dijital güvence boyutları ve iç denetimin rolü. *Denetim*, (20), 108-119.
- Aksoy, E. (2007). Suç ve kent güvenliği yaklaşımı. *TMMOB Ankara Şubesi Bülteni*, (55), 11-16.
- Alacadağlı, E. (2020). Güvenli kent ve kent güvenliği üzerine bir irdeleme. *Giresun Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 6(2), 152-167.
- Al-Khedher, M. A. (2012). Hybrid GPS-GSM localization of automobile tracking system. *arXiv*. <https://arxiv.org/abs/1201.2630>
- Anagnostopoulos, C. N. E., Anagnostopoulos, I. E., Loumos, V., & Kayafas, E. (2006). A license plate-recognition algorithm for intelligent transportation system applications. *IEEE Transactions on Intelligent Transportation Systems*, 7(3), 377-392.
- Aslan, M. M., & Bulut, Y. (2019). Akıllı kent uygulamalarının kentsel güvenlik açısından önemi. *ASSAM Uluslararası Hakemli Dergi*, 13, 52-60.
- Ayhan, İ., & Çubukçu, K. M. (2007). Suç ve kent ilişkisine ampirik bakış: Literatür taraması. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 3(5), 30-55.
- Bahar, F. (2013). Küresel güvenlik tedbirleri: Gözetleme olgusu bağlamında özel güvenlik ve mobese kameraları. *Sosyologca*, 6, 197-207.
- Bazeley, P. (2021). Using NVivo for mixed methods research. In A. Onwuegbuzie & R. B. Johnson (Eds.), *The Routledge Reviewer's Guide to Mixed Methods Analysis* (pp. 343-354). Routledge.
- Balachandar, S., & Chinnaiyan, R. (2021). Secure solutions for smart city command control centre using AIOT. *CoRR*, [abs/2108.00003](https://arxiv.org/abs/2108.00003). <https://arxiv.org/abs/2108.00003>
- Beşe, N., & Geleri, G. (2013). Kent güvenlik yönetim sistemleri. In F. M. Harmancı, M. Gözübenli, & C. Zengin (Eds.), *Güvenlik sektöründe temel stratejiler* (s. 243-276). Nobel Yayıncılık.

- Bimay, M., & Kaypak, Ş. (2019). Küreselleşme sürecinde kamu politikalarında yaşanan değişimler. *ASSAM Uluslararası Hakemli Dergi*, 6(15), 24–40.
- Bozkurt, A., Hamutoğlu, N. B., Liman Kaban, A., Taşçı, G., & Aykul, M. (2021). Dijital bilgi çağı: Dijital toplum, dijital dönüşüm, dijital eğitim ve dijital yeterlilikler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi (AUAd)*, 7(2), 35–63. <https://doi.org/10.51948/auad.911584>
- Bülbül, B. (2019). Kamusal Mekânlardan Akıllı Kent Teknolojileri ile Veri Elde Edilmesi ve Kamusallığın Değerlendirilmesi. *Yapı Bilgi Modelleme*, 1(2), 62–73.
- Ceritli, İ. (2003). *Kentleşme sürecinin ekonomi politiği ve bir Türkiye uygulaması*. Yargı Yayınları.
- Chambliss, W. J. (1996). Toward a political economy of crime. In E. J. Muncie & G. Hughes (Eds.), *Criminological perspective* (2nd ed., ss. 249–256). Sage.
- Çatal, M. (2019). Mobil emniyet uygulamalarına yönelik bir inceleme: METE örneği. *Dijital Çağda Güvenliğin Dönüşümü ve Bir İç Güvenlik Aktörü Olarak Polis Sempozyumu*, 79–93.
- Çelik, D. (2023). Kamu yönetiminde dijital dönüşümde bir sorun alanı: Dijital kültüre yönelik direnç. *Kamu Yönetimi ve Teknoloji Dergisi*, 5(1), 69–86.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Çukurçayır, M. A. (2012). Yönetim Süreçlerinde Açıklık: “Open Government” Ve Yerel Yönetimler. *Yerel Politikalar*, (1).
- Dardour, A., El Haji, E., & Begdouri, M. A. (2025, June). Video surveillance and artificial intelligence for urban security in smart cities: A review of a selection of empirical studies from 2018 to 2024. In *Computer Sciences & Mathematics Forum* (Vol. 10, No. 1, p. 15). MDPI. <https://doi.org/10.3390/csmf10010015>
- Demirbaş, T. (2005). *Kriminoloji*. Seçkin Yayıncılık.
- Demirel, M. (2021). *Türkiye’de dijital güvenlik politikaları*. Güvenlik Araştırmaları Yayınları.
- Doğan, A., & Ustakara, F. (2013). Kamu yönetiminde dijitalleşme ve e-devlet uygulamaları. *Akademik Yayıncılık*.

- EGM (Emniyet Genel Müdürlüğü). (2013). *Emniyet Genel Müdürlüğü 2013 faaliyet raporu*. <https://www.egm.gov.tr>
- Ekinci, C. (2011). *Kent güvenlik yönetim sistemleri*. Emniyet Genel Müdürlüğü Yayınları.
- Erdem, E. İ. (2016). İnsani güvenlik kavramı bağlamında çevre güvenliği. *Akademik Bakış Dergisi*, 10(19), 255–281.
- Erdil, A. (2023). *Kamu hizmetlerinin dijitalleşmesi: E-devlet uygulamalarının etkileri*. Kamu Politikaları Enstitüsü Yayınları.
- Erdoğan, B. (2021). *Kamu yönetiminde dijitalleşme ve güvenlik*. Kamusal Politika Yayınları.
- Erkek, M. (2017). Kent ulaşımında teknolojik denetim sistemleri. In A. Kaya (Ed.), *Kent, suç ve güvenlik* (ss. 55–74). Dora Yayıncılık.
- Foucault, M. (1975). *Surveiller et punir: Naissance de la prison*. Édition Gallimard.
- Gündem. (2010). Ankara KGYS açılış töreni ve iç güvenlik zirvesi. Ankara Emniyet Müdürlüğü Basın Arşivi.
- Gündüzöz, A. (2016). Suçun önlenmesine yönelik kent tasarımı yaklaşımları. In A. Gündüzöz & M. H. Cengiz (Eds.), *Kent güvenliği ve güvenlik yönetimi* (ss. 327–350). Seçkin Yayıncılık.
- Gürbüz, A. (2019). Vatandaş odaklı kamu hizmet yönetimi. *Erzincan Binali Yıldırım Üniversitesi İİBF Dergisi*, 1(2), 34–41.
- Guetterman, T. C., & James, T. G. (2023). A software feature for mixed methods analysis: The MAXQDA interactive quote matrix. *Methods in Psychology*, 8, Article 100116. <https://doi.org/10.1016/j.metip.2023.100116>
- Gültekin Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *INTERNET POLICY REVIEW: JOURNAL ON INTERNET REGULATION*, 13(3).
- Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., ... & Chiroma, H. (2016). The role of big data in smart city. *International Journal of information management*, 36(5), 748-758.
- Hayta, Y. (2021). Akıllı Kent Uygulamalarında Kişisel Verilerin Gizliliği Ve Güvenliği. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 31(2), 929-941.

- Hongliang, B., & Changping, L. (2004, August). A hybrid license plate extraction method based on edge statistics and morphology. In *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.* (Vol. 2, pp. 831-834). IEEE.
- Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance.*
- Huang, H., Li, R., Wang, W., Qin, T., Zhou, R., & Fan, W. (2023). Concepts, models, and indicator systems for urban safety resilience: A literature review and an exploration in China. *Journal of Safety Science and Resilience, 4*(1), 30–42. <https://doi.org/10.1016/j.jnlssr.2022.12.001>
- Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers, 24*(2), 393-414.
- Karaağaçlı, M. (2022). Türkiye’de güvenlik hizmetlerinde dijitalleşme: Kent Güvenlik Yönetim Sistemi (KGYS) ve MOBESE üzerine bir inceleme. *CBÜ Sosyal Bilimler Dergisi, 20*(2), 739–756. <https://doi.org/10.18026/cbusos.18498>
- Kaypak, Ş. (2016). Kentsel bir sorun olarak kentsel güvenlik. *The Journal of Academic Social Science, 33*, 35–50.
- Khan, I. R., Ali, S. T. A., Siddiq, A., Khan, M. M., Ilyas, M. U., Alshomrani, S., & Rahardja, S. (2022). Automatic license plate recognition in real-world traffic videos captured in unconstrained environment by a mobile camera. *Electronics, 11*(9), 1408.
- Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. *Sensors, 23*(7), 3681. <https://doi.org/10.3390/s23073681>
- Kocaoğlu, A. (2017). *Bilgi toplumunda hukuk ve güvenlik.* Adalet Yayınevi.
- Koç, M. (2018). Dijital çağın etkisinde kent, yönetim, siyaset. In V. Şeker & N. Bilgili (Eds.), *Mahalle muhtarlarının yönetime katılımında yeni iletişim teknolojilerini kullanımı: Muğla ili üzerinden bir değerlendirme* (ss. 89–102). Detay Yayıncılık.

- Koç, M. (2023). Dijitalleşen dünyada mahalle yönetimi: Dijital mahalle ve muhtarlık. In M. Koç, N. Bilgili, & B. Gündoğar (Eds.), *Dijitalleşme ve mahalle yönetimi: Kavramlar, kuramlar, uygulamalar* (ss. 3–18). Gazi Kitabevi.
- Koç, M., Gündoğar, B. N., & Teke, M. E. (2023). Muhtarların yeni iletişim araçlarını kullanımı: Gölhisar örneği. *Ünye İktisadi ve İdari Bilimler Fakültesi Dergisi*, 5(2), 1–11.
- Kuckartz, U., & Rädiker, S. (2022). Using MAXQDA for integration in mixed methods research. In J. H. Hitchcock & A. J. Onwuegbuzie (Eds.), *The Routledge Handbook for Advancing Integration in Mixed Methods Research* (pp. 540–562). Routledge.
- Li, B., Tian, B., Li, Y., & Wen, D. (2013). Component-based license plate detection using conditional random field model. *IEEE Transactions on Intelligent Transportation Systems*, 14(4), 1690–1699.
- Lyon, D. (2003). Surveillance as social sorting.
- Marchment, Z., Clemmow, C., & Gill, P. (2025). PROTOCOL: Situational Crime Prevention Measures to Prevent Terrorist Attacks Against Soft Targets and Crowded Places: An Evidence and Gap Map. *Campbell Systematic Reviews*, 21(2), e70040. <https://doi.org/10.1002/cl2.70040>
- Matsueda, R. L., & Grigoryeva, M. S. (2014). Social inequality, crime, and deviance. In *Handbook of the social psychology of inequality* (pp. 683-714). Dordrecht: Springer Netherlands.
- McClain, P. D. (2001). Urban crime in USA and Western Europe: A comparison. In R. Paddison (Ed.), *Handbook of Urban Studies* (pp. 220–240). Sage.
- Murakami, W., Ball, K., Graham, S., Lyon, D., Norris, C., & Raab, C. (2006). A report on the surveillance society: For the information commissioner by the surveillance studies network.
- Nomura, S., Yamanaka, K., Katai, O., Kawakami, H., & Shiose, T. (2005). A novel adaptive morphological approach for degraded character image segmentation. *Pattern Recognition*, 38(11), 1961–1975.
- Othman, F., Yusoff, Z. M., & Salleh, S. A. (2020). The impact of physical features and environment on crime in urban neighbourhood areas. *Planning Malaysia*, 18.

- Öner, S., & Çam, M. (2022). Çocuk parklarında güvenlik uygulamaları: Ankara örneği. *Uluslararası Toplum Araştırmaları Dergisi*, 18(28), 1167–1191. <https://doi.org/10.26466/opusjsr.1051045>
- Özen, A., & Gürel, F. N. (2020). Kamu denetiminde dijital dönüşüm: Dijital ikiz yöntemi. *İzmir Sosyal Bilimler Dergisi*, 2(1), 16–23.
- Özhan, M. Z. (2014). İzmir KGYS uygulaması ve yazılım entegrasyonu. In F. M. Harmancı, M. Gözübenli, & C. Zengin (Eds.), *Güvenlik sektöründe temel stratejiler* (pp. 243–276). Nobel Yayıncılık.
- Özdemir, A. (2022). Data-and knowledge-driven smart city strategies: research on implementation challenges of local governments in Turkey. *Yönetim ve Ekonomi Araştırmaları Dergisi*, 20(3), 152-169.
- Palma-Borda, J., Guzmán, E., & Belmonte, M. V. (2025). A digital shadow for modeling, studying and preventing urban crime. *IEEE Access*.
- Portakal, N. (1999). *Bursa BEMTAP Projesi ve sayısal entegrasyon uygulamaları*. Bursa Emniyet Müdürlüğü Yayınları.
- Pustu, Y. (2006). Küreselleşme sürecinde kent: “Antik site’den dünya kentine”. *Sayıştay Dergisi*, 60, 129–151.
- Quiros, A. R. F., Bedruz, R. A., Uy, A. C., Abad, A., Bandala, A., Dadios, E. P., Fernando, A., & Salle, D. L. (2017). A kNN-based approach for the machine vision of character recognition of license plate numbers. *IEEE TENCON*, 1081–1086. <https://doi.org/10.1109/TENCON.2017.8228018>
- Redo, S. (2008). Six United Nations guiding principles to make crime prevention work. In *International perspectives of crime prevention: Contributions from the 1st Annual International Forum* (pp. 5-22). Mönchengladbach: Forum Verlag Godesburg.
- Reis, J., & Melão, N. (2023). Digital transformation: A meta-review and guidelines for future research. *Heliyon*, 9(1), e12721. <https://doi.org/10.1016/j.heliyon.2023.e12721>
- Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications.
- Shaw, M. (2001). *The role of local government in community safety*. Montreal: ICPC.

- Singh, S., Razaque, A., & Bashir, A. K. (2021). *Edge-based video analytic for smart cities*. International Journal of Advanced Computer Science and Applications, 12(7), 1–8. https://thesai.org/Downloads/Volume12No7/Paper_1-Edge_based_Video_Analytic_for_Smart_Cities.pdf
- Smith, G. J. (2007). Exploring relations between watchers and watched in control (led) systems: Strategies and tactics. *Surveillance & Society*, 4(4).
- Su, P., Chen, Y., & Lu, M. (2022). Smart city information processing under internet of things and cloud computing. *The Journal of Supercomputing*, 78(3), 3676–3695. <https://doi.org/10.1007/s11227-021-03971-0>
- Şahin, Y., & Korkmaz, M. (2021). Dijital dönüşüm sürecinde ulusal güvenlik politikaları. İstanbul: Stratejik Araştırmalar Vakfı.
- Şeker, N., Başpınarlı, B. A., Çankara, Ç., Üngör, İ., & Müftüoğulları, M. (2025). Dijital dönüşümün devlet yapısına etkisi. *Socrates Journal of Interdisciplinary Social Researches*, 11(50). <https://doi.org/10.5281/zenodo.1487063569>
- T.C. Çevre ve Şehircilik Bakanlığı. (2019). *2020–2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*. T.C. Çevre ve Şehircilik Bakanlığı Yayınları.
- T.C. İçişleri Bakanlığı. (2015). Muhtar Bilgi Sistemi. <https://www.icisleri.gov.tr/bilgiteknolojileri/muhtar-bilgi-sistemi-projesi>
- Tanrıverdi, A. (2021). Yapay zekânın kamu hizmetinin sunumuna etkileri. *Adalet Dergisi*, (66), 293–314.
- Teichert, R. (2019). Digital transformation maturity: A systematic review of literature. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 67(6), 1673–1687. <https://doi.org/10.11118/actaun201967061673>
- Tozkoparan, İ. B. (2019). Değişen güvenlik anlayışında geleceğin akıllı kentleri. *ASSAM Uluslararası Hakemli Dergi*, 13, 417–427.
- Uğurlu, Ö. (2010). Kentlerin tarihsel gelişimi. In *Türkiye Perspektifinden Kent Sosyolojisi Çalışmaları* (ss. 33–50).
- Ulubaş, Y. (2023). Akıllı kentlerde güvenlik teknolojileri. In M. H. Cengiz & M. Y. Yıldız (Eds.), *Güvenli kentler ve teknoloji* (pp. 67–90). Beta Yayınları.
- UN-Habitat. (2007). *Enhancing urban safety and security: Global report on human settlements 2007*. Nairobi.

- United Nations Office on Drugs and Crime (UNODC). (2010). *Handbook on the crime prevention guidelines: Making them work*. New York.
- Uslu, H. (2023). Dijital dönüşüm ve kamu hizmetleri yönetiminde yenilikçi yaklaşımlar ve zorluklar. *Uluslararası Politik Araştırmalar Dergisi*, 9(3), 15-31.
- Uysal, Y. (2020). Klasik kamu yönetiminden yeni kamu işletmeciliği ve Post-YKİ'ye kamu hizmetlerinin dönüşümü üzerine bir değerlendirme. *International Journal of Management and Administration*, 4(7), 112–155.
- Ün, A. (2022). Siber güvenlik ve bireysel verilerin korunması. In İ. Akgül & S. A. Erçetin (Eds.), *Siber güvenlik ve toplum* (pp. 413–437). Pegem Akademi.
- Vega-Huerta, H., Vilca Velasquez, J., Anicama Espinoza, N., Maquen-Niño, G. L. E., Guerra-Grados, L., Pantoja-Collantes, J., ... & Lázaro-Guillermo, J. C. (2025). Mobile application based on KDD to predict high-crime areas and promote sustainability in citizen security in a district of Lima-Perú. *Frontiers in Computer Science*, 7, 1585632. <https://doi.org/10.3389/fcomp.2025.1585632>
- Yıldırım, U., & Öner, Ş. (2004). Bilgi toplumu sürecinde yerel yönetimlerde eğitim-bilişim teknolojilerinden yararlanma: Türkiye'de e-belediye uygulamaları. *The Turkish Online Journal of Educational Technology*, 3(1), 49–60.
- Yıldız, H. (2020). *Dijitalleşme kuramları ve uygulama modelleri*. Ege Üniversitesi Yayınları.
- Yıldız, R. (2022). Dijital altyapı yatırımları ve kamu yönetimi: Akıllı şehir perspektifinden bir değerlendirme. *Kamu Politikaları ve Yerel Yönetimler Dergisi*, 11(2), 103–118.
- Yoshimori, S., Mitsukura, Y., Fukumi, M., & Akamatsu, N. (2003). License plate detection using hereditary threshold determine method. In *Lecture Notes in Artificial Intelligence*, 2773 (pp. 585–593).
- Yüceyılmaz, A. A. (2007). Konya örneğinde kentsel suçlar ve kent esenliği (Yayımlanmamış yüksek lisans tezi). Selçuk Üniversitesi, Konya.
- Zhou, W., Li, H., Lu, Y., & Tian, Q. (2012). Principal visual word discovery for automatic license plate detection. *IEEE Transactions on Image Processing*, 21(9), 4269–4279.

- Zhuang, J., Hou, S., Wang, Z., & Zha, Z. J. (2018). Towards human-level license plate recognition. In V. Ferrari et al. (Eds.), *Computer Vision – ECCV 2018, Lecture Notes in Computer Science, 11207* (pp. 306–321). https://doi.org/10.1007/978-3-030-01219-9_19
- Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In *New labor forum* (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: Sage Publications.



EKLER

MAXQDA GÖRÜŞME FORMU

Katılımcı Bilgileri

- Katılımcı Kodu :
- Görüşme Tarihi :
- Görüşme Süresi :
- Görüşmeci :
- Yaş :
- Eğitim Durumu :
- Meslek :
- Yaşanılan Şehir : Kütahya
- Cinsiyet :
- Görüşme Türü : Yüz yüze

A. KATILIMCIYA İLİŞKİN BİLGİLER

1. KGYS sistemine dair bilginiz var mı?
2. Daha önce KGYS sistemiyle ilgili bir deneyiminiz oldu mu?

B. DİJİTAL DÖNÜŞÜM VE KENT GÜVENLİĞİ

3. Dijitalleşmenin kent güvenliği üzerindeki etkisi hakkında ne düşünüyorsunuz?
4. KGYS'yi dijital dönüşüm bağlamında nasıl değerlendiriyorsunuz?
5. Dijital güvenlik sistemlerinin şehir yaşamındaki rolü sizce nedir?

C. KGYS'NİN İŞLEYİŞİ VE ETKİNLİĞİ

6. KGYS kentteki güvenliği sağlamada ne kadar etkilidir?
7. KGYS bileşenlerinden hangileri daha etkili?
8. Veriler yeterince değerlendiriliyor mu?

D. MAHREMİYET VE VERİ GÜVENLİĞİ

9. Kamera sistemleri bireysel mahremiyeti nasıl etkiliyor?
10. KGYS kapsamında toplanan verilerle ilgili endişeniz var mı?
11. Güvenlik ile mahremiyet arasında nasıl bir denge kurulmalı?

E. TOPLUMUN TUTUMU VE KATILIMI

12. Vatandaşlar sizce KGYS uygulamalarını biliyor mu?

13. Toplumsal güven için neler yapılmalı?

14. Vatandaşlar bu tür sistemlere katkı sunmalı mı?

F. GELECEK ÖNGÖRÜLERİ VE DİJİTALLEŞME

15. KGYS sisteminde gelecekte ne gibi değişiklikler bekliyorsunuz?

16. Yeni teknolojilerin (yapay zekâ, büyük veri vb.) entegrasyonu hakkında ne düşünüyorsunuz?

17. Dijital güvenlik sistemleri ile geleneksel yöntemler nasıl ilişkilendirilmeli?

Ekleme İstedığınız Başka Bir Görüş veya Öneriniz Var mı?

.....
.....