

Jandarma ve Sahil Güvenlik Akademisi

Güvenlik Bilimleri Enstitüsü

Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, 22-47

doi: 10.28956/gbd.1688236

Gendarmerie and Coast Guard Academy

Institute of Security Sciences

Journal of Security Sciences, Thematic Issue on Policing Practices and Security Technologies, 22-47

doi: 10.28956/gbd.1688236

Makale Türü ve Başlığı / Article Type and Title

Araştırma / Research Article

Akıllı Şehirlerde Kamu Güvenliğinin Yeniden İnşası: Kolluk Uygulamalarında Güvenlik Teknolojileri ve Etik Hususlar

Reconstruction Public Security in Smart Cities: Security Technologies and Ethical Considerations In Law Enforcement Practices

Yazar(lar) / Writer(s)

Mehmet Seyda OZAN, Dr. Öğr. Üyesi, Erciyes Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, mseydaoan@gmail.com, ORCID: 0000-0003-1821-0287

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:

-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.

-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.

This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 30.04.2025

Makale Kabul Tarihi / Accepted : 09.10.2025

Atıf Bilgisi / Citation:

OZAN M. S., (2025). Akıllı Şehirlerde Kamu Güvenliğinin Yeniden İnşası: Kolluk Uygulamalarında Güvenlik Teknolojileri ve Etik Hususlar, Güvenlik Bilimleri Dergisi *Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı*, ss 22-47. doi: 10.28956/gbd.1688236

AKILLI ŞEHİRLERDE KAMU GÜVENLİĞİNİN YENİDEN İNŞASI: KOLLUK UYGULAMALARINDA GÜVENLİK TEKNOLOJİLERİ VE ETİK HUSUSLAR

Öz

21. yüzyılda hız kazanan dijitalleşme süreci, kamu güvenliği kavramının teorik ve pratik düzeyde yeniden tanımlanmasını gerekli kılmıştır. Geleneksel kolluk yaklaşımının ötesine geçen yeni kamu güvenliği mimarisi; özellikle akıllı şehirler bağlamında veri temelli, teknolojik kapasitesi yüksek ve öngörüye dayalı müdahale mekanizmalarını ön plana çıkarmaktadır. Bu çalışmanın temel amacı; akıllı şehirlerde kullanılan ileri güvenlik teknolojilerinin yapay zekâ, büyük veri analitiği, nesnelerin interneti (IoT), yüz tanıma sistemleri ve öngörücü kolluk uygulamaları gibi bileşenler aracılığıyla kamu güvenliğine katkılarını ve bu süreçlerde gözetilmesi gereken etik ve hukuki sınırları, kamu yönetimi perspektifiyle kapsamlı bir biçimde değerlendirmektir. Çalışmada nitel araştırma yöntemi benimsenmiş olup literatür taraması, kavramsal analiz ve karşılaştırmalı vaka incelemesi tekniklerinden yararlanılmıştır. Bu kapsamda küresel örnekler olarak Amerika Birleşik Devletleri, Çin, Singapur ve Avrupa ülkelerinde uygulanan dijital güvenlik sistemleri/politikaları analiz edilmiştir. Elde edilen bulgular, söz konusu teknolojilerin kamu güvenliğine operasyonel verimlilik, hızlı müdahale kapasitesi ve karar destek mekanizmalarının güçlendirilmesi gibi açılardan önemli katkılar sunabileceğini ortaya koymaktadır. Ancak aynı zamanda bu teknolojilerin şeffaflık, hesap verebilirlik ve bireysel hakların korunması gibi yönetim ilkeleriyle uyum içinde tasarlanması gerektiği önemle vurgulanmaktadır. Bu bağlamda çalışma, teknoloji destekli güvenlik mimarisinin demokratik değerlerle bütünleşik, toplumsal meşruiyeti yüksek ve etik duyarlılığa sahip bir yapıda geliştirilmesi gerektiğini ortaya koymaktadır.

Anahtar Kelimeler: Kamu güvenliği, Kolluk Uygulamaları, Kamu yönetimi, Güvenlik Teknolojileri, Etik.

RECONSTRUCTION PUBLIC SECURITY IN SMART CITIES: SECURITY TECHNOLOGIES AND ETHICAL CONSIDERATIONS IN LAW ENFORCEMENT PRACTICES

Abstract

In the 21st century, the accelerating digitalization process has necessitated a theoretical and practical redefinition of the concept of public security. The new public security architecture, which goes beyond the traditional law enforcement approach, emphasizes data-driven, high technological capacity and predictive intervention mechanisms, especially in the context of smart cities. The main purpose of this study is to comprehensively evaluate the contributions of advanced security technologies used in smart cities to public security through components such as artificial intelligence, big data analytics, Internet of Things (IoT), facial recognition systems and predictive law enforcement practices, and the ethical and legal boundaries that should be observed in these processes from a public administration perspective. The qualitative research method was adopted in the study and literature review, conceptual analysis and comparative case study techniques were utilized. In this context, digital security systems/policies implemented in the United States, China, Singapore and European countries were analyzed as global examples. The findings reveal that these technologies can make significant contributions to public security in terms of operational efficiency, rapid response capacity and strengthening decision support mechanisms. However, it is also emphasized that these technologies should be designed in line with governance principles such as transparency, accountability and protection of individual rights. In this context, the study reveals that technology-supported security architecture should be developed in a structure that is integrated with democratic values, has high social legitimacy and ethical sensitivity.

Keywords: Public Security, Law Enforcement Practices, Public Administration, Security technologies, Ethics.

GİRİŞ

Günümüzde dijitalleşme süreci, kamu güvenliği kavramının hem teorik hem de pratik anlamda yeniden tanımlanmasını zorunlu hâle getirmiştir. Klasik kolluk anlayışının fiziksel mevcudiyet ve doğrudan müdahale ekseninden ileri teknolojiyle veri temelli karar alma süreçlerine evrilmesi, kamu güvenliğinin tesisinde köklü bir paradigma değişimini beraberinde getirmiştir (Brayne, 2018, ss. 301-303; Afzal ve Panagiotopoulos, 2024, ss. 1-7). Bu dönüşüm, akıllı şehir (smart city) kavramı etrafında şekillenen yeni bir kamu güvenliği mimarisinin temelini oluşturmaktadır. Artık kamu güvenliği yalnızca suçun önlenmesinden/bastırılmasından ziyade risklerin öngörülmesi, toplumsal hassasiyetlerin analiz edilmesi ve müdahale süreçlerinin optimize edilmesiyle ilişkilendirilmektedir.

Kamu yönetiminde bu yeni güvenlik anlayışı, teknolojik araçların temel düzeyde kullanılmasının ötesine geçerek karar alma süreçlerini yönlendiren ve sistemi şekillendiren stratejik unsurlar hâline gelmesiyle tanımlanmaktadır. Bu bağlamda yapay zekâ, büyük veri analitiği, nesnelerin interneti (IoT), coğrafi bilgi sistemleri (GIS), yüz tanıma sistemleri ve öngörücü kolluk uygulamaları; güvenlik hizmetlerinin kapsamını, etkinliğini ve toplumsal etkisini yeniden belirleyen temel bileşenler hâline gelmiştir (Dakalbab, 2022, ss. 13-22). Ancak bu teknolojik ilerleme süreci aynı zamanda bireysel hak ve özgürlükler, mahremiyet, etik sınırlar ve hukuki meşruiyet gibi çok katmanlı tartışmalı alanlarını da beraberinde getirmektedir.

Bu çalışmanın temel amacı, yeni kamu güvenliği mimarisinin merkezine yerleşen kolluk teknolojilerini kamusal işleyiş perspektifinden analiz etmek ve söz konusu uygulamaların etik-hukuki sınırlarını tartışmaktır. Literatürde kolluk teknolojileri genellikle mühendislik veya suç bilimi (criminology) perspektifinden ele alınmakta olup kamu yönetimi ve yönetim bilimi bağlamındaki değerlendirmeler sınırlı kalmaktadır. Bu araştırma; söz konusu boşluğa katkı sağlamayı hedeflemekte ve güvenlik teknolojilerini yönetsel meşruiyet, toplumsal kabul ve etik denetim ilkeleriyle birlikte ele almaktadır.

Bu bağlamda çalışmanın araştırma sorusu “Akıllı şehirlerde kamu güvenliğini tesis etmek amacıyla kullanılan güvenlik teknolojileri, kolluk uygulamalarını nasıl dönüştürmekte ve bu dönüşüm bireysel haklar ve yönetişim ilkeleri bakımından ne tür etik-hukuki hususlar doğurmaktadır?” şeklinde formüle edilmiştir.

Akıllı şehirlerde kamu güvenliği artık yalnızca kolluk gücünün fiziksel kapasitesiyle değil veriye dayalı karar mekanizmalarının şeffaflığı, hesap verebilirliği ve toplumsal meşruiyetiyle birlikte değerlendirilmesi gereken çok boyutlu bir yönetim meselesi hâline gelmiştir. Bu çerçevede çalışmada, kamu güvenliği teknolojilerinin sadece uygulamada değil politika geliştirme, uygulama ve değerlendirme aşamalarında nasıl konumlandığı da analiz edilmekte olup dijital güvenlik politikalarının bu süreçteki rolü tartışılmaktadır. Özellikle veri güvenliği, şeffaflık, yapay zekâ sistemlerinin hesap verebilirliği gibi konular, kamusal karar alma süreçlerinin etik ve hukuki sınırlarını da yeniden tanımlayan hususlar olarak ele alınmaktadır. Bu noktada çalışma, dijital kamu güvenliği politikalarının anayasal denge ilkeleriyle (özgürlük-güvenlik dengesi, özel hayatın gizliliği, orantılılık ilkesi vb.) ilişkisini vurgulayarak dijital anayasa kavramına da katkı sunmayı hedeflemektedir. Zira güvenlik teknolojileriyle şekillenen yeni kamu düzeni, klasik normatif anayasa kuramının ötesine geçerek, dijital çağın yönetsel gerçekliklerine uyarlanmış yeni bir anayasal çerçeve gerektirmektedir. Bu gereklilik hem hukuk normlarının hem de kamu yönetimi pratiklerinin yeniden yapılandırılmasını zorunlu kılmaktadır. Bu nedenle çalışmada; güvenlik teknolojilerinin yönetim ilkeleriyle ne ölçüde uyumlu olduğu değerlendirilmekte, dijital güvenlik düzenlemelerinin anayasal hak ve özgürlüklerle çatışmadan nasıl kurumsallaştırılabileceğine dair değerlendirmelere yer verilmektedir.

Çalışmada, nitel araştırma yöntemi benimsenmiştir. Bu kapsamda literatür taraması, karşılaştırmalı örnek olay (case study) analizi ve kavramsal çözümleme tekniklerinden yararlanılmıştır. Her nitel araştırmada olduğu gibi bu çalışmanın da belirli yöntemsel sınırlılıkları bulunmaktadır. Nitel yaklaşımın sağladığı kuramsal derinlik ve kavramsal çözümleme gücüne rağmen politika etkisinin nicel olarak ölçülmesine yönelik sınırlı kapasite, değerlendirmelerin genellenebilirliğini kısıtlayıcı bir etki oluşturabilmektedir. Diğer yandan dijital güvenlik sistemlerine dair kurumsal belgeler, kamu politikası metinleri ve uluslararası raporlar esas alınmış olup uygulayıcı aktörlerle derinlemesine görüşmeler yapılmamıştır. Bu durum sistemlerin pratikteki işleyişi, karşılaşılan zorluklar ve toplumsal algı düzeyine dair doğrudan kullanıcı perspektiflerinin analizine imkân tanımamaktadır. Tüm bu sınırlılıklar, çalışmadaki değerlendirmeleri bağlamsal olarak yorumlama gerekliliğini ortaya koymakta olup ilerleyen araştırmalar için çok disiplinli metodolojilerin geliştirilmesine yönelik bir ihtiyaç alanı olarak değerlendirilebilir.

Bu çalışmada örneklem kapsamına alınan Amerika Birleşik Devletleri (ABD), Çin Halk Cumhuriyeti, Singapur ve Avrupa ülkeleri; teknolojik kapasite, yönetsel yapılanma, veri koruma politikaları ve etik duyarlılık açısından belirgin biçimde ayrışan kamu güvenliği yaklaşımlarını temsil etmektedir. Bu örneklerden her biri, çalışmanın analiz etmeyi hedeflediği dijital güvenlik mimarileri, veri tabanlı kolluk stratejileri ve etik-hukuki sınır çerçevesi konularında farklı uygulama biçimlerini bünyesinde barındırmaktadır. ABD örneği, öngörücü kolluk ve yapay zekâ destekli güvenlik stratejilerinin nasıl şekillendiğini göstermesi açısından önem arz etmektedir. Çin örneği, dijital gözetim kapasitesinin maksimum düzeyde ve merkezî bir otorite altında nasıl işletildiğine dair bir bağlam sunarken Singapur modeli; kurumsal kapasite, kamu güveni ve veri temelli yönetim arasındaki ilişkiyi çözümlemeye imkân tanımaktadır. Avrupa kıtası ülkeleri ise güvenlik teknolojilerinin birey haklarına duyarlı ve hukuki normlara bağlı şekilde nasıl geliştirilebileceğine dair yapısal örnekler barındırmaktadır. Bu örneklem kompozisyonu, kolluk teknolojilerinin rejimsel sınırlar içindeki farklılaşmasını ve bu farklılaşmanın toplumsal meşruiyet üzerindeki etkilerini değerlendirme açısından çok boyutlu bir analitik çerçeve sunmaktadır. Ayrıca örnekleme yer alan ülkelerin kamu güvenliği politikalarının uluslararası kamuoyu tarafından gündeme taşınıyor olması, çalışmanın güncelliğini ve bilimsel görünürlüğünü artıran bir diğer unsurdur. Bu ülkeler üzerinden geliştirilen analiz çerçevesinde, teknolojik kapasite ile etik ve yasal çerçeve arasındaki uyum/denge hususu tartışılmıştır.

Çalışmanın birinci bölümünde kamu güvenliği ve kolluk faaliyetlerinin teknolojik dönüşümüne dair kavramsal çerçeve sunulmakta olup ikinci bölümde seçilen ülkelerdeki uygulama örnekleri değerlendirilmektedir. Üçüncü bölümde güvenlik teknolojilerine ilişkin etik ve hukuki tartışmalar analiz edilmekte; sonuç bölümünde ise bulgular genel bir değerlendirmeye tabi tutulmakta olup bazı politika önerilerine yer verilmektedir.

1. KAMU GÜVENLİĞİ VE KOLLUK FAALİYETLERİNİN TEKNOLOJİK DÖNÜŞÜMÜ

Kamu güvenliği; bireylerin yaşam hakkı, mülkiyet bütünlüğü ve toplumsal huzurunun sürekliliğini amaçlayan; devletin anayasal sorumlulukları çerçevesinde yürütülen, önleyici, koruyucu ve müdahale edici nitelikteki kurumsal ve stratejik faaliyetlerin bütünüdür. Bu kavram, yalnızca suçla mücadele kapsamında dar anlamıyla düşünülmemelidir. Kamu güvenliği;

toplumsal yaşamın devamlılığını, kriz anlarında hızlı müdahaleyi ve toplulukların refahını da içeren çok katmanlı bir yapıya sahiptir. Kavram bu yönüyle hem bireysel hakların korunmasının hem de kolektif yaşamın sürdürülebilirliğinin teminatı olarak işlev görmektedir (Friedman, 2022, ss. 725-745).

Modern kamu yönetimi literatüründe kamu güvenliğini tesis etme, salt şekilde kolluk güçlerinin fiziksel mevcudiyetinden ziyade veri odaklı karar alma süreçleri, teknolojik kapasitenin etkin kullanımı ve toplumsal katılımın sağlanmasıyla da ilişkilendirilmektedir (International Centre for Criminal Statistics, 2023). Özellikle kentleşmenin hız kazandığı ve mekânsal yoğunlaşmanın arttığı büyük şehirlerde, güvenlik olgusunun daha dinamik, çok aktörlü ve katmanlı bir yaklaşımla ele alınması zorunlu hâle gelmiştir. Bu dönüşüm, klasik kolluk paradigmasının ötesine geçerek akıllı şehir uygulamalarıyla entegre bir güvenlik mimarisinin inşasını gündeme getirmiştir.

Kamu güvenliğinin bu yeni yorumunda risk temelli öngörü mekanizmalarının, dijital gözetim altyapılarının ve gerçek zamanlı müdahale kapasitelerinin geliştirilmesi, devletin güvenlik fonksiyonunun yeniden yapılandırılmasına/yorumlanmasına neden olmaktadır. Kolluk faaliyetlerinin yalnızca reaktif bir nitelik taşımaktan çıkarılıp proaktif ve analitik kapasiteye sahip sistemlerle desteklenmesi, akıllı şehirlerin güvenlik politikalarında merkezî bir strateji olarak öne çıkabilmektedir (Garcia, 2025, ss. 1-5).

21. yüzyılın dijitalleşme süreci, kamu güvenliği anlayışını geleneksel çerçevenin ötesine taşımış; bu anlayışı, ileri seviyede teknolojik, dinamik ve etkileşimli bir güvenlik ekosistemine dönüştürmüştür. Bu dönüşümle birlikte teknolojik araçlar, kamu güvenliğinin inşasında tamamlayıcı değil kurucu ve yönlendirici bir rol üstlenmeye başlamıştır (OECD, 2024; Casey, 2025). Bu dönüşümde özellikle yapay zekâ, büyük veri analitiği, nesnelerin interneti (IoT), coğrafi bilgi sistemleri (GIS), yüz tanıma ve biyometrik doğrulama teknolojileri gibi ileri düzey dijital sistemler, kamu güvenliği politikalarının biçimlendirilmesinde belirleyici rol oynamaktadır. Kamu güvenliği kavramı; veriye dayalı tahminleme, anlık tehdit algılama ve önleyici müdahale kapasitesiyle donatılmış bir yönetim pratiğine dönüşmüştür (Xie ve Luo, 2022, ss. 1-9). Bu durum, güvenliğin geleceği öngören ve riski minimize etmeyi amaçlayan stratejik bir sürece evrilmesini beraberinde getirmiştir.

Teknolojinin bu merkezî rolü, kamu güvenliğinin sağlanmasında insan kaynaklı karar mekanizmalarının ötesine geçilerek algoritmik rasyonaliteye dayalı yeni bir karar yapısının oluşmasına da zemin hazırlamaktadır (Cheong, 2024, ss. 1-8; Elsherif, 2024). Algoritmik rasyonalite; karar alma süreçlerinde algoritmaların, özellikle de makine öğrenimi, yapay zekâ ve büyük veri analitiği temelli sistemlerin, insan aklının sınırlılıklarını aşma vaadiyle konumlandırıldığı yeni bir rasyonalite formunu ifade etmektedir. Bu rasyonalite teknolojisinde karar süreçleri öngörülebilirlik, hesaplanabilirlik ve veriye dayalı optimizasyon ilkeleri üzerine inşa edilmektedir (Halpern ve Pass, 2015; Lowrie, 2017). Ancak bu teknolojik yeniden tanımlama süreci; aynı zamanda bireysel mahremiyetin korunması, dijital hakların gözetilmesi ve etik denetim mekanizmalarının işlerliği gibi önemli kamusal sorunsalları da beraberinde getirebilmektedir.

Akıllı şehir kavramının merkezinde yer alan teknolojik altyapılar, kolluk faaliyetlerinin biçimini, kapsamını ve etki düzeyini köklü biçimde dönüştürmektedir. Nesnelerin interneti (IoT), büyük veri ve yapay zekâ gibi dijital teknolojiler, kamu güvenliği hizmetlerinde hem verimlilik artışı sağlamakta hem de müdahale biçimlerini daha öngörülebilir, hızlı ve hedef odaklı hâle getirmektedir (Johnson, 2025). Bu teknolojiler; kolluk kuvvetlerinin klasik denetim ve müdahale yöntemlerinden ayrışarak veri temelli stratejik güvenlik yönetimi anlayışına yönelmesini zorunlu kılmaktadır.

Nesnelerin interneti, fiziksel nesnelerin kendi aralarında ve merkezî dijital sistemlerle sürekli veri alışverişi yapabilen bir iletişim ağı içinde işlev görmesini ifade eden kavramsal ve teknik bir yapıdır. Bu teknolojiler, kentsel güvenlik için gerekli olan çevresel verilerin anlık olarak toplanmasını ve merkezî sistemlerle entegre edilmesini mümkün kılarken trafik kameraları, sensörler, giyilebilir teknolojiler ve akıllı aydınlatma sistemleri gibi bileşenlerle suç önleme kapasitesini geliştirmektedir. Büyük veri analitiği ise bu devasa veri kümelerinin anlamlı hâle getirilmesini, suç desenlerinin çözülmesini ve risk haritalarının oluşturulmasını sağlamaktadır (Malcolm, 2024; Global Trade, 2024). Bu süreçte kolluk kuvvetleri, geçmiş vakalardan türetilen istatistiksel modeller aracılığıyla daha proaktif güvenlik politikaları geliştirebilmektedir. Yapay zekâ ise kolluk faaliyetlerinde hem karar desteği sağlayan sistemler hem de otomatik tehlike algılama ve yanıt sistemleri aracılığıyla işlev görebilmektedir. Özellikle yüz tanıma, kalabalık analiz sistemleri ve anomalileri tespit eden algoritmalar, insan hatasını en aza indirerek güvenlik

operasyonlarının hassasiyetini artırabilmektedir (Rapid Innovation, 2024; U.S. Department of Justice, 2024). Bu sistemler müdahaleyi ve kaynak tahsisini daha rasyonel ve veri odaklı kılabilir.

Kolluk kuvvetlerinin dijital dönüşümü, teknolojik donanımların temin edilmesini aşarak güvenlik kurumlarının kurumsal işleyişinin, operasyonel kapasitesinin ve müdahale yaklaşımlarının çarpıcı biçimde yeniden şekillendirilmesiyle ilişkilidir (Murugan, 2024; Johnson, 2025). Bu dönüşümde en belirgin yeniliklerden biri, gerçek zamanlı veri aktarımı ve analizine olanak tanıyan mobil sistemlerdir. Kolluk kuvvetleri artık olay yerine gitmeden önce mekânsal veriler, geçmiş vaka bilgileri ve şüpheli profilleri gibi kritik bilgilere mobil cihazlar üzerinden erişebilmekte bu da hem hazırlık süresini azaltmakta hem de müdahale etkinliğini artırmaktadır (BlueForce, 2025). Bu kapsamda kullanılan yeni nesil uygulamalar (örneğin suç haritalama yazılımları, dijital kimlik doğrulama sistemleri, mobil tutanak uygulamaları), olay yönetimini daha sistematik ve şeffaf hâle getirmektedir.

Ayrıca insansız hava araçları (İHA), otomatik plaka tanıma sistemleri, entegre güvenlik kameraları ve giyilebilir kameralar gibi teknolojiler, dijital denetimin sahadaki uzantılarını oluşturmaktadır. Bu teknolojik araçlar; özellikle kalabalık yönetimi, sınır güvenliği, trafik kontrolü ve asayiş denetimleri gibi alanlarda kolluk kuvvetlerine yüksek düzeyde görünürlük ve müdahale avantajı sunmaktadır (Cyr, 2024; Elistair, 2025; Utility, 2025). Diğer yandan klasik sezgisel yaklaşımlar yerini algoritmik destekli karar süreçlerine bırakabilmektedir. Öngörücü polislik (predictive policing), yapay zekâ destekli devriye rotalama, risk skorlaması ve toplumsal hassasiyet analizi gibi uygulamalar, kolluk faaliyetlerinin yönünü proaktif bir önleyiciliğe çevirmiştir (Olaoye ve Egon, 2024, ss. 2-10).

Bununla birlikte teknoloji destekli karar sistemlerinin yükselişi, insan faktörünün tamamen devre dışı bırakıldığı bir yönetim modeline evrilmemelidir. Aksine dijital sistemlerle insan karar vericiler arasında kurulan karşılıklı bağımlılığa ve dengeye dayalı simbiyotik ilişki, kararların hem teknik geçerliliğini hem de toplumsal kabulünü artırabilmektedir. Bu noktada teknoloji, karar sürecinde “nihai bir otorite” değil karar vericiye yön gösteren bir danışman işlevi üstlenmelidir. Ancak bu süreç yalnızca teknik bir kapasite meselesi değildir. Teknoloji destekli karar verme uygulamalarının hukuki meşruiyeti, etik sınırları ve toplumsal güven boyutları da kamu yönetiminde

giderek daha fazla önem kazanmaktadır. Kararların algoritmalar tarafından nasıl üretildiği, hangi verilerle beslendiği ve bu kararların toplum üzerindeki etkileri, kamu yönetimi açısından yeni bir etik gündemi oluşturmaktadır.

2. KAMU GÜVENLİĞİNİN DİJİTALLEŞMESİ: AKILLI ŞEHİRLERDE GÜVENLİK TEKNOLOJİLERİ VE ULUSLARARASI DENEYİMLER

Bu çalışmada karşılaştırmalı analiz için uygun bir çeşitlilik sunma adına örneklem olarak Amerika Birleşik Devletleri, Çin Halk Cumhuriyeti, Singapur ve Avrupa kıtasından bazı örnek ülkeler seçilmiştir. ABD öngörücü polislik gibi veri odaklı sistemlerin öncüsü olarak teknik yenilikçiliği temsil ederken Çin yüksek teknolojiyi yaygın gözetimle bütünleştiren otoriter bir model sunmaktadır. Singapur, yüksek kamu güveni ve kurumsal kapasiteyle teknolojiyi bütüncül yönetimle birleştiren yapısıyla dikkat çekerken Avrupa ülkeleri bireysel hakları korumayı önceleyen etik-yasal düzenlemeleriyle ayrılmaktadır. Bu seçki; çalışmanın kamu güvenliği teknolojilerinin farklı rejimlerdeki kurumsal, etik ve hukuki yansımalarını analiz edilmesini mümkün kılmaktadır.

Amerika Birleşik Devletleri (ABD): Öngörücü Polislik (Predictive Policing) ve Yapay Zekâ Destekli Suç Önleme Sistemleri

ABD suç tahmini ve kamu güvenliği uygulamalarında önde gelen ülkelerden biridir (Gül, 2009: 151). Bu kapsamda ABD’de en dikkat çeken örneklerinden biri, öngörücü polislik (predictive policing) adı verilen uygulamalardır. Öngörücü polislik, geçmiş suç verilerini analiz ederek gelecekte işlenme ihtimali yüksek suçları ve bunların gerçekleşebileceği yerleri önceden tahmin etmeyi amaçlayan algoritmik bir yaklaşımdır. Bu sistem, yalnızca olayın meydana geldiği alanları değil suçun oluşmasını tetikleyebilecek sosyal ve mekânsal risk faktörlerini de analiz ederek kolluk güçlerine müdahale öncesinde stratejik bir yönlendirme sunabilmektedir (Brunette, 2025; Thomson Reuters, 2025; Johnson, 2025).

Bu doğrultuda Kaliforniya eyaletindeki bazı akıllı şehirlerde kullanılmış/kullanılan PredPol (Predictive Policing) yazılımı, suç istatistiklerine dayanarak “nerede”, “ne zaman” ve “ne tür” suçların meydana geleceğini tahmin edebilmekte; kolluk güçlerinin devriye dağılımını ve kaynak yönetimini veri temelli bir düzlemde yeniden yapılandırabilmektedir. Bununla birlikte hem PredPol hem de öngörücü polislik sistemleri ABD’de ciddi etik ve hukuki

tartışmalara yol açmaktadır. Genel anlamda eleştiriler, algoritmaların geçmişteki ayrımcı kolluk uygulamalarını yeniden ortaya çıkarabileceği ve sosyal adalet ilkesinin zedelenebileceği üzerinedir (Los Angeles Times, 2020; TechPolicy, 2024). Bu bağlamda PredPol'e yönelik en yoğun eleştirilerden biri, algoritmik önyargı olgusuna ilişkindir. PredPol gibi tahmine dayalı kolluk yazılımları, tarihsel suç verilerini temel alarak çalıştığı için geçmişteki sistemik önyargıları ve yapısal eşitsizlikleri algoritmik düzlemde yeniden üretebilme riskini barındırmaktadır. Özellikle etnik, sosyoekonomik ya da mekânsal temelli ayrımcılık içeren veri kümeleriyle eğitilen algoritmalar, tarafsız gibi görünen teknolojik müdahalelerin dahi ayrımcı sonuçlar doğurabileceğini göstermektedir (Ziosi ve Pruss, 2024).

Çin Halk Cumhuriyeti: Yüz Tanıma ve Toplumsal Gözetim Sistemleri

Çin Halk Cumhuriyeti, kamu güvenliği iddiasıyla ileri düzey dijital gözetim teknolojilerini en kapsamlı kullanan ülkelerden biri olarak öne çıkmaktadır. Ülkede yüz tanıma teknolojileri (facial recognition technology), hem suçla mücadele amacıyla hem de toplumsal düzenin denetimi, bireylerin günlük yaşamlarının izlenmesi ve kamu davranışlarının düzenlenmesi gibi çok katmanlı amaçlarla yaygınlaştırılmıştır. Bu sistemler, kent kameralarıyla entegre biçimde çalışmakta ve vatandaşların kimliklerini saniyeler içinde doğrulabilmektedir (The Sun, 2025; Reuters, 2025).

Bu teknolojik altyapıların en çarpıcı uygulamalarından biri “Sosyal Kredi Sistemi” ile ilişkilendirilen gözetim mimarisidir. Vatandaşların finansal geçmişleri, sosyal medya davranışları ve kamusal alandaki tutumları gibi çok sayıda veri kümesi; kentlerdeki merkezî algoritmalar aracılığıyla analiz edilerek bireylere sosyal puanlar atanmaktadır. Bu puanlar; bireylerin ulaşım, eğitim, istihdam ve kamu hizmetlerinden yararlanma düzeyini doğrudan etkilemektedir (Liang vd., 2018, ss. 415-416; Zhao ve Liu, 2025, ss. 50-55). Bu uygulama, kamu düzenini sağlama gerekçesiyle meşrulaştırılsa da uluslararası alanda insan hakları, özel yaşamın gizliliği ve devletin aşırı müdahalesi konularında ciddi eleştirilere yol açmıştır. Çin'deki bu uygulamaların şeffaflıktan uzak yürütülmesi ve hukuki temellerinin zayıf olması, Çin'in gözetim devletine (surveillance state) doğru evrildiğine dair küresel endişeleri pekiştirmiştir. Çin; ileri teknolojiye gözetim sistemlerinin suç önleme ve sosyal düzenin sağlanması açısından teknik başarılar sağladığını iddia etse de uluslararası kamuoyunda bu uygulamalar, özellikle Uygur bölgelerindeki kitlesel izleme faaliyetleri

nedeniyle “teknoloji yoluyla otoriterleşme” olarak yorumlanmaktadır (The New York Times, 2018; Naushad, 2024; AFCEA, 2025).

Singapur: Smart Nation Güvenlik Programları ve Sensör Tabanlı İzleme

Singapur, dijital dönüşümü ulusal kalkınma stratejisinin merkezine yerleştiren ve güvenlik alanında bu vizyonu sistematik biçimde uygulayan öncü ülkelerden biridir. 2014 yılında başlatılan Smart Nation girişimi, kamu hizmetlerinin dijitalleştirilmesini ve kamu güvenliğinin veri temelli sürekli izlenmesini hedeflemiştir. Bu çerçevede Singapur, sensör tabanlı izleme sistemlerini kent ölçeğinde yapılandırarak suçla mücadelede ve kamu düzeninin sağlanmasında dijital gözetimi temel bir stratejik araç hâline getirmiştir (Smart Nation Singapore, 2014; IEREK, 2025). Özellikle “Lamppost-as-a-Platform” (LaaP) adı verilen program, şehir genelindeki aydınlatma direklerine yerleştirilen çok işlevli sensörler aracılığıyla çevresel verilerin insan yoğunluklarının ve potansiyel güvenlik tehditlerinin sürekli olarak izlenmesini mümkün kılmaktadır. Bu sistemde yer alan kameralar ve IoT cihazları; yüz tanıma ve anomali tespiti gibi özelliklerle donatılmış olup kolluk güçlerine anlık veri akışı sağlamaktadır (Reuters, 2018; NUS, 2020; Smart Nation Singapore, 2024). Ek olarak VIP (Video Intelligence Platform) gibi projeler, kamusal alanlarda gerçekleşen davranışsal sapmaları tespit edebilen yapay zekâ algoritmaları sayesinde olağan dışı durumlara otomatik uyarı sistemleriyle yanıt verilmesini mümkün kılmaktadır. Örneğin kalabalık içinde ani bir koşu hareketi ya da şüpheli davranış tespit edildiğinde sistem güvenlik birimlerine bildirim gönderebilmekte, bu kapsamda müdahale daha erken ve hedefli hâle getirilebilmektedir (Pensees Singapore, 2025; GovTech Singapore, 2025a). Öte yandan Akıllı Ulus vizyonunun vatandaş odaklı dijital hizmet ayağında yer alan ulusal dijital kimlik sistemi SingPass da yaygın biçimde benimsenmiştir. 2025 itibarıyla SingPass her ay 5 milyon kullanıcıya ulaşmakta ve 800’ü aşkın kamu kurumu ile özel kuruluşun sunduğu 2.700’ün üzerinde dijital hizmete güvenli erişim imkânı tanıyarak aylık 41 milyon işlemi mümkün kılmaktadır (GovTech Singapore, 2025b).

Avrupa Kıtası: Genel Veri Koruma Tüzüğü’ne (GDPR) Uyumlu Veri Güvenlik Protokolleri ve Akıllı Kolluk Sistemleri

Avrupa kıtasında akıllı şehir uygulamaları çerçevesinde geliştirilen güvenlik teknolojileri hem teknik yeterlilik ve operasyonel etkinlik hem de birey haklarının korunması veri gizliliği ve hukuki meşruiyet ilkeleri doğrultusunda

şekillendirilmektedir. Bu noktada Genel Veri Koruma Tüzüğü (GDPR - General Data Protection Regulation), Avrupa Birliği (AB) genelinde dijital güvenlik ve gözetim uygulamalarına yön veren temel yasal çerçeveyi oluşturmaktadır. Kolluk birimlerinin dijital teknolojileri kullanarak veri işlemesi, bu tüzük kapsamında özel düzenlemelere tabidir ve “gereklilik”, “ölçülülük” ve “şeffaflık” ilkeleri temelinde sınırlandırılmıştır (GDPR EU, 2025). Bu bağlamda Avrupa’daki birçok ülkede akıllı güvenlik sistemleri hem algoritmik gözetimi hem de veri koruma mekanizmalarını entegre biçimde içeren “ethics-by-design (tasarımla etik)” anlayışına dayanmaktadır (EU, 2024; Sherpa, 2025). Örneğin AB üye devletlerince geliştirilen bazı projelerde, yapay zekâ ile desteklenen suç analiz sistemleri, veri anonimleştirme teknikleri ile güçlendirilerek kullanıma sunulmakta ve vatandaşların bireysel kimliklerinin korunması öncelikli hâle getirilmektedir (Eerstekamer NL, 2024). Avrupa’da öne çıkan bir diğer uygulama ise PRECINCT (Predictive Resilience and Effective Coordination for Critical Infrastructures) projesidir. Bu proje kapsamında kritik altyapılara yönelik tehditlerin yapay zekâ ve büyük veri analitiği ile öngörülmesi hedeflenmekte aynı zamanda elde edilen tüm verilerin GDPR standartlarına uygun şekilde işlenmesi için ileri düzey şifreleme ve güvenlik protokolleri uygulanmaktadır (European Commission, 2021).

3.KAMU GÜVENLİĞİ BAĞLAMINDA KOLLUK TEKNOLOJİLERİNİN ETİK VE HUKUKİ BOYUTU: NORMATİF ÇERÇEVE, UYGULAMA SORUNLARI VE POLİTİKA ÖNERİLERİ

Akıllı şehir güvenlik sistemlerinin merkezine yapay zekâ ile büyük veri ve sürekli gözetim teknolojilerinin yerleştirilmesi, bireylerin özel hayatlarının gizliliği, kişisel verilerin işlenme biçimi ve kamusal alandaki görünürlüklerinin denetlenmesi gibi temel hak ve özgürlükler açısından ciddi etik ve hukuki sorunları da beraberinde getirebilmektedir (Mantelero, 2018, ss. 755-759; Mark ve Anya, 2019, ss. 1-11). Özellikle yüz tanıma ve davranış analizine dayalı algoritmik gözetim sistemleri, bireylerin rızası dışında ve sürekli izleme gibi uygulamalarla mahremiyet hakkının sınırlarını zorlamaktadır. Dünya genelinde özellikle kamusal alanlarda yapılan yüz tanıma uygulamalarında bu sistemlerin hangi ölçütlere göre çalıştığı, kimleri hedeflediği ve yanlış tanılama durumunda bireylerin hak arama yollarının nasıl işletildiği ciddi bir belirsizlik alanı oluşturabilmektedir.

Avrupa Birliği ülkelerinde Genel Veri Koruma Tüzüğü (GDPR) ve bu koruma tüzüğüyle bağlantılı olarak geliştirilen AI Act gibi düzenlemeler, özellikle biyometrik veriler gibi “özel nitelikli kişisel veriler”in toplanmasına ve işlenmesine sıkı kısıtlamalar getirmiştir. Bu düzenlemeler çerçevesinde vatandaşlara; verilerine ilişkin erişim, düzeltme, silme ve itiraz hakları tanınmakta; algoritmik kararların bireyler üzerinde ciddi etkiler doğurması hâlinde, insan temelli yeniden değerlendirme zorunluluğu getirilmektedir (Epic, 2024; Your Europe, 2025). Ayrıca şeffaflık ve hesap verebilirlik ilkeleri doğrultusunda, gözetim sistemlerinin bağımsız denetim organları tarafından düzenli olarak denetlenmesi ve kamuoyuna açık raporlarla hesap verilmesi gerektiği hem Avrupa Konseyi hem de Birleşmiş Milletler İnsan Hakları Komiserliği tarafından önerilen küresel ilkeler arasındadır (Council of Europe, 2015; UN, 2023).

Akıllı şehir güvenliği uygulamalarının merkezine yerleştirilen teknolojik gözetim araçları, kamu güvenliğini artırma amacını taşımakla birlikte aynı zamanda toplumsal yaşamı sürekli denetim altında tutan bir yapının altyapısını da inşa etmektedir. Bu durum, modern kamu yönetiminde “güvenlik-özgürlük ikilemi” çerçevesinde ele alınmakta bireyin görünürlüğüne arttığı, anonimliğin azaldığı ve davranışlarının sürekli izlendiği bir kamusal alan inşasının liberal-demokratik değerlerle ne ölçüde bağdaşabileceği sorusunu gündeme taşımaktadır (Schuilenburg ve Peeters, 2018, ss. 5-9; Greitens, 2020; Park, 2023). Gözetim toplumuna evrilme riski, teknolojik araçların fiziksel mekânlarda görünür olmasından çok bu araçların işlediği verilerin nasıl, kim tarafından ve hangi amaçla kullanıldığıyla ilgilidir. Bu bağlamda Çin’deki uygulamalar, bu riskin pratikte nasıl somutlaştığına dair dikkat çekici bir örnek sunmaktadır. Çin’de kamu güvenliğini sağlama iddiasıyla yaygın biçimde kurulan yüz tanıma sistemleri ve sosyal puanlama uygulamaları, bireylerin dijital kimlikleri üzerinden sürekli izlenmesini ve davranışlarının merkezî algoritmalarla puanlanmasını içeren kapsamlı bir gözetim mimarisini oluşturmuştur. Bu yapı; suçla mücadele gerekçesiyle kamusal denetimi artırmakta, mahremiyet hakkı ve kişisel özerklik gibi temel haklar üzerinde ciddi bir baskı oluşturmakta ve bireylerin kamusal alandaki davranışlarını içselleştirilmiş bir gözetim bilinciyle biçimlendirmelerine yol açmaktadır.

Tablo. Çin ve Avrupa Birliği Ülkelerinde Güvenlik Teknolojileri Uygulamalarının Yapısal Karşılaştırması

Karşılaştırma Boyutu	Çin Halk Cumhuriyeti	Avrupa Birliği Ülkeleri
<i>Kullanılan Teknolojiler</i>	Yüz tanıma, sosyal kredi sistemi, kitlesel gözetim kameraları, yapay zekâ, davranış analitiği	Yüz tanıma (sınırlı), IoT tabanlı gözetim, büyük veri analitiği, yapay zekâ destekli suç tahmin sistemleri
<i>Hukuki Düzenlemeler ve Normatif Çerçeve</i>	Devlet merkezli idari düzenlemeler, şeffaf olmayan normlar	GDPR ve AI Act gibi kapsamlı ve birey haklarını önceleyen düzenlemeler
<i>Bireysel Hakların Korunması</i>	Mahremiyet ve veri kontrolü zayıf, rıza ilkesi gözetilmiyor.	Mahremiyet ve bireylerin açık rızası aranmaktadır.
<i>Şeffaflık ve Hesap Verebilirlik</i>	Düşük düzeyde; algoritmalar kamuya açık değil denetim mekanizmaları sınırlı	Algoritmik sistemler denetime tabidir, bağımsız veri koruma otoriteleri gözetimi sağlamaktadır.
<i>Etik Hususlar</i>	Devlet merkezli çıkar yaklaşımı; “gözetimle kontrol” anlayışı	“Ethics-by-design” gibi ilkelerle etik yönetim tasarımı; kamusal meşruiyet vurgusu
<i>Sosyopolitik Sistemle İlişki</i>	Otoriter yönetim modeli; gözetim araçları sosyal kontrol aracı olarak işlev görmektedir.	Güvenlik teknolojileri toplumsal denge ve insan hakları çerçevesinde sınırlandırılmaktadır ve demokratik değerlerle uyumludur.

Kaynak: The New York Times, 2018; European Commission, 2021; Big Data China 2022; Naushad, 2024; EU, 2024; AFCEA, 2025, Sherpa, 2025, GDPR EU, 2025. (Bu şekil yazar tarafından oluşturulmuştur.)

Çin Halk Cumhuriyeti, kamu güvenliği iddiası altında ileri düzey dijital gözetim sistemlerini otoriter bir yönetim anlayışıyla bütünleştirmiştir. Bu bağlamda, yüz tanıma sistemleri ve sosyal kredi mekanizmaları, toplumsal davranışları şekillendirmek ve merkezî kontrolü kurumsallaştırmak amacıyla da kullanılmaktadır. Özellikle bireylerin dijital davranışlarının sistematik biçimde izlenmesi ve puanlanması, “normatif vatandaşlık” anlayışını dijital disiplin

mekanizmalarıyla sağlamaktadır. Ancak bu yapı, şeffaflık, hesap verebilirlik ve hukuki güvenceler açısından ciddi eksiklikler barındırmakta ve gözetimin otoriter versiyonu olarak değerlendirilmektedir.

Avrupa Birliği ülkelerinde ise güvenlik teknolojilerinin kullanımı, birey haklarını önceleyen normatif bir çerçeveye oturtulmuştur. GDPR ve AI Act gibi düzenlemeler, yapay zekâ ve veri işleme sistemlerinin hem teknik yeterlilik hem de etik uyumluluk içinde tasarlanmasını şart koşmaktadır. “Ethics by design” ilkesi, sistemlerin henüz inşa aşamasındayken insan haklarına duyarlı olacak biçimde yapılandırılmasını sağlamaktadır. Ayrıca bireylerin kişisel verileri üzerindeki kontrolü yalnızca teorik bir hak değil pratikte de işleyen bir mekanizma hâline gelmiştir (EU, 2024; Sherpa, 2025).

Akıllı şehir güvenliği kapsamında kullanılan teknolojiler, kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerini doğrudan etkilediği için hukuki düzenlemeler bu alanda belirleyici bir zemine sahiptir. Bu bağlamda hem ulusal düzeyde hem de uluslararası alanda geliştirilen veri koruma rejimleri, güvenlik teknolojilerinin kullanımında sınır çizici ve yön gösterici bir işlev üstlenmektedir. AB bünyesinde uygulanan Genel Veri Koruma Tüzüğü (GDPR) ise özellikle hassas verilerin işlenmesi, bireylerin verileri üzerinde sahip olduğu kontrol hakları ve algoritmik karar alma süreçlerine yönelik şeffaflık yükümlülükleri bakımından normatif bir yapıya sahiptir. GDPR, yapay zekâ ve büyük veri teknolojilerinin toplumsal etkilerini gözeterek kamu güvenliği uygulamalarında dahi birey haklarını önceleyen bir yaklaşımı esas almaktadır (Daoudagh vd., 2021, ss. 1-18). Bu düzenlemeler, güvenlik ile temel haklar arasındaki dengeyi kurumsal düzeyde tesis etme çabasının bir ürünüdür. Teknolojinin gelişmişliği kadar bu teknolojinin hangi sınırlar içinde ve hangi güvencelerle uygulandığı da kamu güvenliğinin demokratik temeller üzerinde sürdürülebilirliği açısından belirleyici rol oynamaktadır. Özellikle kamusal güvenlik ile bireysel mahremiyet arasında sağlanacak hassas denge, hukuki sistemin yalnızca norm koyan değil, aynı zamanda teknolojik uygulamaları denetleyen bir yapıya sahip olmasını gerekli kılmaktadır.

Modern kamu yönetimi pratiklerinde dijitalleşmenin yükselişi, kamu güvenliği ile bireysel özgürlükler arasındaki sınır çizgisini her zamankinden daha önemli hâle getirmiştir. Özellikle akıllı şehirlerde kullanılan güvenlik teknolojileri, bireyin görünürlüğünü artırırken onun kamusal ve özel yaşam alanları arasındaki farkı yeniden tanımlar hâle gelmiştir. Bu noktada karşılaşılan temel etik ikilem, güvenli bir toplum düzeni ile bireyin mahremiyetine ve

özgürlüğüne duyulması gereken saygı arasındaki hassas dengedir. Bu nedenle bu ikilemin çözümü, iki değeri de asgari zarar ve azami fayda ilkesine göre birlikte değerlendiren dengeleyici bir yönetim yaklaşımıdır.

Bu çerçevede ve güvenlik teknolojilerinin gelişimiyle birlikte gündeme gelen bir diğer önemli konu ise yapay zekâ sistemlerinin nasıl yapılandırıldığı ve bu yapılandırmaların hangi toplumsal etkileri doğurabileceğine ilişkin değerlendirme ihtiyacıdır. Özellikle algoritmaların eğitildiği veri kümelerinde yer alabilecek sistematik ön yargılar, bazı toplumsal gruplar açısından sakıncalı risk değerlendirmelerine yol açabilmektedir. Kullanılan dijital sistemlerin belirli denetim ilkeleri çerçevesinde izlenebilir ve gerektiğinde gözden geçirilebilir olması hem kamu kurumları hem de vatandaşlar açısından güven artırıcı bir husustur. Bu kapsamda şeffaflık, hesap verebilirlik ve denetlenebilirlik gibi yönetim ilkeleriyle uyumlu bir dijital güvenlik mimarisinin inşa edilmesi, teknolojinin kamu yararına katkı sunma potansiyelini pekiştirecektir. Ayrıca algoritmaların karar alma süreçlerinde hangi verilere dayandığı, bu kararların nasıl üretildiği ve bireylerin bu süreçlere nasıl itiraz edebileceği gibi hususlara yönelik açık iletişim kanallarının oluşturulması kamusal güvenliğe yönelik uygulamaların toplumsal meşruiyetini de güçlendirecektir. Bu yönde geliştirilecek her türlü etik çerçeve ve hukuki mekanizma, kolluk faaliyetlerinin hem teknolojik kapasitesini hem de toplumsal kabul düzeyini destekleyici nitelikte olacaktır.

SONUÇ VE DEĞERLENDİRME

Kamusal güvenlik, tarih boyunca devletlerin meşruiyetini güçlendiren temel işlevlerden biri olarak öne çıkmıştır. Bireylerin can ve mal emniyetinin sağlanması, kamu düzeninin korunması ve toplumsal istikrarın tesisi gibi asli görevler, uzun süre boyunca fiziksel denetim ve merkezî otoriteye dayalı klasik kolluk pratikleri üzerinden yürütülmüştür. Bu geleneksel modelde güvenlik hizmetlerinin belirleyici unsuru, kolluk gücünün sahadaki görünürlüğü ve müdahale kapasitesi iken karar alma süreçleri ise büyük ölçüde sezgilere, kişisel deneyime ve kurumsal reflekslere dayanmaktaydı. Ancak nüfusun artması, toplumsal yapının değişmesi, kentleşme süreçlerinin hızlanması ve dijital teknolojilerin yaşamın her alanına nüfuz etmesiyle birlikte kamusal güvenlik hizmetlerinin yürütülme biçimi de radikal bir dönüşüme uğramıştır. Bu dönüşümde geleneksel kolluk anlayışının sınırlılıkları belirginleşmiş; ani gelişen krizlere zamanında müdahale edememe, risk öngörüsünde yetersizlik ve kaynakların verimli kullanılamaması gibi sorunlar daha görünür hâle gelmiştir.

Günümüzde güvenliğin yalnızca fiziksel müdahale kapasitesiyle sınırlanmaması gerektiği bunun yanında stratejik öngörü, veriye-teknolojiye dayalı karar desteği ve toplumsal etkileşim boyutlarının da dikkate alınması gerektiği kabul görmektedir. Bu yeni güvenlik mimarisi içerisinde teknoloji destekli kolluk yaklaşımı giderek önem kazanmaktadır. Yapay zekâ algoritmaları, büyük veri analitiği, sensör sistemleri ve mobil uygulamalar gibi dijital araçlar, sadece bilgiye erişim ve müdahale hızını artırmakla kalmayıp aynı zamanda güvenlik yönetimini daha bütüncül, öngörülebilir ve hesap verebilir bir yapıya dönüştürebilmektedir. Artık kamusal güvenlik, yalnızca tehditlere tepki veren bir yapıdan çıkmakta; riskleri öngören, erken uyarı mekanizmaları geliştiren ve stratejik müdahale kapasitesini sürekli olarak güncelleyen bir sistem mantığıyla yeniden tasarlanmaktadır. Bu bağlamda teknoloji destekli kolluk hem operasyonel kapasitenin hem de yönetsel süreçlerin yeniden tanımlandığı bir dönüşüm sürecini temsil etmektedir.

Diğer yandan güvenlik hizmetlerinin insan hakları, etik değerler ve toplumsal kabul düzeyleriyle uyumlu olarak kurgulanması, bu dönüşümün sürdürülebilirliği ve demokratik meşruiyeti açısından kritik önem taşımaktadır. Dolayısıyla kamusal güvenliğin dijitalleşme süreci, salt bir teknik evrim değil aynı zamanda normatif, kurumsal ve kültürel boyutlarıyla bütüncül bir yeniden inşa süreci olarak değerlendirilmelidir. Bu kapsamda güvenlik teknolojilerinin karar süreçlerine entegrasyonunun hem teknik bir optimizasyon süreci olarak hem de yönetim ilkeleriyle ilişkili bir yapı olarak ele alınması önemlidir. İlgili süreçte şeffaflık, hesap verebilirlik, hukuki meşruiyet ve toplumsal güven unsurları, teknolojik uygulamaların başarısı üzerinde belirleyici bir rol oynamaktadır. Bu kapsamda çalışmada incelenen uluslararası örnekler, güvenlik teknolojilerinin etik ve hukuki sınırlarının nasıl tanımlandığının kamu güvenliğinin niteliği üzerinde belirleyici olduğunu ortaya koymaktadır. Özellikle Çin’de görülen uygulamalar, yüksek teknolojiye gözetim araçlarının kamu güvenliği iddiasıyla aşırılık içeren denetim araçlarına dönüşme riskini gözler önüne sermektedir. Bu sistemlerin toplumsal kontrolü önceleyen yapısı, birey hakları ve mahremiyet gibi değerler bakımından ciddi tartışmaları beraberinde getirmektedir. Buna karşılık AB ülkelerinde geliştirilen güvenlik teknolojilerinin bireysel özgürlükler ile kamu güvenliği arasında hassas bir denge kurmayı amaçladığını söylemek mümkündür. GDPR gibi düzenlemelerin sunduğu çerçeve, teknolojinin demokratik gözetim mekanizmaları içinde kamu yararına hizmet etmesini mümkün kılabilen şekilde güvenlik sistemlerine duyulan toplumsal güveni pekiştirebilmektedir. Bu iki örnek arasındaki fark,

teknolojinin sadece nasıl geliştirildiği değil hangi değerler doğrultusunda ve ne tür toplumsal amaçlarla kullanıldığı sorusunun da önemini açıkça ortaya koymaktadır. Bu bağlamda, kamu güvenliği ile bireysel özgürlükler arasında kurulması gereken hassas dengenin teknik bir uzmanlık ve güçlü bir yönetim kültürüyle desteklenmesi kaçınılmazdır. Geleceğin güvenlik politikaları, teknolojik yeniliklerin kurumsal rasyonaliteyle bütünleştiği, aynı zamanda temel hak ve özgürlüklerin korunduğu dengeli bir yönetim yaklaşımıyla sürdürülebilir hâle gelecektir. Diğer yandan güvenlik teknolojilerinin yaygınlaştığı bir yönetim ortamında, etik ve hukuki farkındalığın güçlendirilmesi, kamu güvenliğinin toplumsal meşruiyetini sağlamada stratejik önemini koruyacaktır. Bu kapsamda etik ilkelere dayalı eğitim programları, sürekli mesleki gelişim uygulamaları ve karar süreçlerinde şeffaflığı artıran mekanizmalar yoluyla güvenlik hizmetlerinde sorumluluk bilinci ve hukuk devleti ilkesiyle uyumlu bir kurumsal kültür inşa edilmesi son derece önemlidir. Bu çerçevede geliştirilecek yönetim modelleri, teknolojinin kamu yararı ve güvenliği doğrultusunda kullanıldığı denetlenebilir ve hesap verebilir bir güvenlik mimarisi oluşturulmasına katkı sağlayacaktır.

Akıllı şehirlerde dijital güvenlik teknolojilerinin kamu güvenliğine entegrasyonu sürecinde etik, hukuki ve yönetsel boyutları birlikte gözetken politika önerilerini aşağıdaki gibi özetlemek mümkündür:

- Kolluk birimlerinin kullandığı güvenlik teknolojilerine ilişkin veri işleme süreçlerini, algoritma tasarımı, şeffaflığı ve tüm bu sürecin insan haklarına etkilerini denetlenecek bağımsız, çok paydaşlı ve uzman temelli denetim kurulları yapılandırılmalıdır. Bu kurullar, yıllık denetim raporlarını kamuoyuyla paylaşarak hesap verebilirlik düzeyini artırmalıdır.
- Yeni bir güvenlik teknolojisi uygulamaya alınmadan önce bu teknolojinin birey hakları, toplumsal eşitsizlikler ve dijital ayrımcılık üzerindeki potansiyel etkilerini değerlendiren etik etki analizleri yasal zorunluluk hâline getirilmelidir.
- “Ethics-by-Design” ilkesi yasal düzenlemelere entegre edilmelidir. Teknolojiler daha tasarım aşamasındayken etik ilkelere uygun biçimde şekillendirilmeli, sistemler bireyin mahremiyetini koruyan ön tanımlı ayarlarla yapılandırılmalıdır.
- Veri erişimi ve itiraz hakkı tanıyan katılımcı mekanizmalar geliştirilmelidir. Bireylerin, kendileri hakkında toplanan verilere erişim, bu verileri düzeltme/silme ve algoritmik kararlara itiraz etme haklarını kullanabilecekleri kolay erişilebilir dijital platformlar hayata geçirilmelidir.

- Yapay zekâ sistemleri için şeffaflık yükümlülüğü getirilmelidir. Kolluk uygulamalarında kullanılan yapay zekâ sistemlerinin hangi verilerle beslendiği, nasıl çalıştığı ve kararları nasıl ürettiği kamuoyuyla paylaşılmalı; “açıklanabilir yapay zekâ” prensibi doğrultusunda tasarım standartları belirlenmelidir.
- Kolluk görevlilerine yönelik etik farkındalık ve dijital haklar eğitimi zorunlu hâle getirilmelidir. Kolluk personeline teknolojik araçların kullanımıyla birlikte dijital mahremiyet, ayrımcılık riskleri, şeffaflık ve hesap verebilirlik konularını içeren etik odaklı sürekli eğitim programları uygulanmalıdır (Gül, 2008: 91).
- Güvenlik teknolojilerinin kullanımıyla ilgili temel çerçeve, yerel yönetimler ve vatandaşlar arasında açık istişareye dayalı “toplumsal mutabakat” belgeleriyle belirlenmeli; kamuoyunun süreçlere aktif katılımı sağlanmalıdır. Akıllı güvenlik teknolojilerinin teknik kapasitesi ne ölçüde gelişmiş olursa olsun bu yapıların bireylerin temel hak ve özgürlüklerini gözetten bir normatif çerçeve içinde tasarlanması, toplumsal kabulü kolaylaştıracaktır. Bu doğrultuda geliştirilecek kamu politikalarında bireyin sadece izlenen/tanımlanan bir nesne olarak değil hak sahibi bir özne olarak görülmesi son derece kıymetli ve önemlidir. Mevcut gelişmeler, bu sürecin teknik kabiliyet kadar etik duyarlılıkla da yürütülmesinin önemine işaret etmektedir.

KAYNAKÇA

- AFCEA (2025). The PRC Continues Its Authoritarian Repression Abroad. Eriřim Tarihi: 11 Nisan 2025, <https://www.afcea.org/signal-media/intelligence/prc-continues-its-authoritarian-repression-abroad>
- Afzal, M., & Panagiotopoulos, P. (2024). Data in Policing: An Integrative Review. *International Journal of Public Administration*, 48(7), 411–430.
- Big Data China (2022). The AI-Surveillance Symbiosis in China, Eriřim Tarihi: 1 Ağustos 2025, <https://bigdatachina.csis.org/the-ai-surveillance-symbiosis-in-china>
- BlueForce (2025). Why Mobile Data is Revolutionizing Criminal Investigations. Eriřim Tarihi: 03 Nisan 2025, <https://www.blueforcelearning.com/blog/why-mobile-data-is-revolutionizing-criminal-investigations>
- Brayne, S. (2018). The Criminal Law and Law Enforcement Implications of Big Data. *Annual Review of Law and Social Science*, 14(1), 293-308.
- Brunette, A. (2025). Policing in the AI Era: Balancing Security, Privacy & The Public Trust. Eriřim Tarihi: 07 Nisan 2025, <https://www.thomsonreuters.com/en-us/posts/government/policing-ai-security/>
- Casey (2025). Closing the Digital Gap: The Importance of Secure Development Practices in Government IT Modernization, Eriřim Tarihi: 13 Nisan 2025, <https://federalnewsnetwork.com/commentary/2025/01/closing-the-digital-gap-the-importance-of-secure-development-practices-in-government-it-modernization/>
- Cheong BC (2024) Transparency and Accountability in AI systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making. *Front. Hum. Dyn.* 6:1421273. doi: 10.3389/fhumd.2024.1421273
- Council of Europe (2015). Democratic and Effective Oversight of National Security Services. Eriřim Tarihi: 1 Nisan 2025, <https://rm.coe.int/16806daadb>
- Cyr, D. (2024). Everything You Need to Know About Automated License Plate Readers in Modern Policing. Eriřim Tarihi: 23 Mart 2025, <https://sirixmonitoring.com/blog/automated-license-plate-readers/>

- Dakalbab, F., Talib, M. A., Waraga, O. A., Nassif, A. B., Abbas, S., & Nasir, Q. (2022). Artificial Intelligence & Crime Prediction: A Systematic Literature Review. *Social Sciences & Humanities Open*, 6(1), 100342.
- Daoudagh, S., Marchetti, E., Savarino, V., Bernabe, J. B., García-Rodríguez, J., Moreno, R. T., ... & Skarmeta, A. F. (2021). Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. *Sensors*, 21(21), 7154.
- Eerstekamer NL (2024). AI and Policing The Benefits and Challenges of Artificial Intelligence for Law Enforcement. Erişim Tarihi: 11 Mart 2025, https://www.eerstekamer.nl/bijlage/20241106/ai_and_policing_the_benefits_and/document3/f%3D/vmi4ngeiyxl6.pdf
- Elistair (2025). Police Drones: Applications and Advantages in the Field. Erişim Tarihi: 14 Mart 2025, <https://elistair.com/police-drones/>
- Elsherif, S. (2024). Public Policy Toward Algorithmic Decision-Making. Erişim Tarihi: 19 Mart 2025, <https://resoinsights.com/insight/public-policy-toward-algorithmic-decision-making/>
- Epic (2024). What U.S. Regulators can Learn from the EU AI Act. Erişim Tarihi: 02 Nisan 2025, <https://epic.org/what-u-s-regulators-can-learn-from-the-eu-ai-act/>
- EU (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations. Erişim Tarihi: 19 Mart 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- European Commission (2021). Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats and Effects with Focus on District or Regional Protection. Erişim Tarihi: 05 Nisan 2025, <https://cordis.europa.eu/project/id/101021668>
- Friedman, B. (2022). What is Public Safety? *Boston University Law Review*, 102(2), 725–768.
- Garcia, E. (2025). AI-Enhanced Public Safety Systems in Smart Cities. Erişim Tarihi: 11 Nisan 2025, <https://philpapers.org/rec/GARAPS-5>
- GDPR EU (2025). General Data Protection RegulationGDPR. Erişim Tarihi: 13 Nisan 2025, <https://gdpr-info.eu/>

- Global Trade (2024). Public Safety Solution for Smart City Market: Revolutionizing Urban Security with Advanced Technologies. Eriřim Tarihi: 04 Mart 2025, <https://www.globaltrademag.com/public-safety-solution-for-smart-city-market-revolutionizing-urban-security-with-advanced-technologies>
- GovTech Singapore (2025a). Smart Nation Sensor Platform. Eriřim Tarihi: 11 Nisan 2025, <https://www.tech.gov.sg/our-capabilities/smart-city-technology/>
- GovTech Singapore (2025b). SingPass – Singapore’s Digital Identity. Eriřim Tarihi: 02 Ağustos 2025, <https://www.tech.gov.sg/products-and-services/for-citizens/digital-services/singpass>
- Greitens, S. C. (2020). Surveillance, Security, and Liberal Democracy in the Post-COVID World. *International Organization*, 74(S1), E169–E190. doi:10.1017/S0020818320000417
- Gül, S. K. (2008). Kamu Yönetiminde ve Güvenlik Hizmetlerinde Hesap Verebilirlik. *Polis Bilimleri Dergisi*, 10(4), 71-94.
- Gül, S. K., & Polat, A. (2009). Kamu Güvenlik Politikalarının Oluřturulmasında Yeni Bir Yaklařım: Suç Tahmini. *Türk İdare Dergisi*, 463(81), 131-156.
- Halpern, J. Y., & Pass, R. (2015). Algorithmic Rationality: Game Theory with Costly Computation. *Journal of Economic Theory*, 156, 246-268.
- IEREK (2025). Singapore Smart-City Transformation From Old to Bold. Eriřim Tarihi: 03 Mart 2025, <https://www.ierek.com/news/singapore-smart-city-transformation-from-old-to-bold/>
- International Centre for Criminal Statistics (2023). Data-Driven Decision Making in Government. Eriřim Tarihi: 11 Nisan 2025, <https://iccs-isac.org/assets/uploads/research-repository/JC-Research-Report-Data-Driven-Decision-Making-in-Government-May-2023-FINAL.pdf>
- Johnson, K. (2025). The Future of Law Enforcement: Smart Technology, Accountability, and Strategy. Eriřim Tarihi: 17 Mart 2025, <https://www.soundthinking.com/blog/the-future-of-law-enforcement-smart-technology-accountability-and-strategy/>

- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing A Data-Driven Society: China's Social Credit System As A State Surveillance Infrastructure. *Policy & Internet*, 10(4), 415-453.
- Los Angeles Times (2020). LAPD will end Controversial Program that Aimed to Predict Where Crimes would Occur. Erişim Tarihi: 14 Nisan 2025, <https://www.latimes.com/california/story/2020-04-21/lapd-ends-predictive-policing-program>
- Lowrie, I. (2017). Algorithmic Rationality: Epistemology and Efficiency in the Data Sciences. *Big Data & Society*, 4(1). <https://doi.org/10.1177/2053951717700925>
- Malcolm (2024). What Is "The Internet Of Things" And What Can It Do?. Erişim Tarihi: 03 Mart 2025, <https://www.govpilot.com/blog/what-the-internet-of-things-can-do-govpilot>
- Mantelero, A. (2018). AI and Big Data: A Blueprint for A Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, 34(4), 754-772.
- Mark, R., & Anya, G. (2019). Ethics of Using Smart City AI and Big Data: The Case of Four Large European Cities. *The ORBIT Journal*, 2(2), 1-36.
- Murugan (2024). Digital Transformation: For Policing and Criminal Justice. Erişim Tarihi: 02 Mart 2025, <https://publicsectornetwork.com/insight/digital-transformation-for-policing-and-criminal-justice>
- Naushad, S. (2024). The Global Influence of Mass Surveillance: China's Uyghur Genocide and the Limits of the Wassenaar Arrangement. Erişim Tarihi: 13 Nisan 2025, <https://djilp.org/the-global-influence-of-mass-surveillance-chinas-uyghur-genocide-and-the-limits-of-the-wassenaar-arrangement/>
- NUS (2020). 60 Years of Facial Recognition: The Hidden Perils Behind Singapore's 'Facial Recognition Era'. Erişim Tarihi: 19 Mart 2025, <https://www.comp.nus.edu.sg/news-media/2020-facialreg/>
- OECD (2024). Digital Public Infrastructure for Digital Governments. Erişim Tarihi: 01 Nisan 2025, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/digital-public-infrastructure-for-digital-governments_11fe17d9/ff525dc8-en.pdf

- Olaoye, F. & Egon, A. (2024). Predictive Policing and Crime Prevention. Eriřim Tarihi: 05 Nisan 2025, <https://easychair.org/publications/preprint/lQ2r>
- Park, S. (2023). Smart Cities: Striking a Balance Between Urban Resilience and Civil Liberties. arXiv preprint arXiv:2303.14597. Eriřim Tarihi: 03 Mart 2025, <https://arxiv.org/abs/2303.14597v1>
- Pensees Singapore (2025). Intelligent Video Analytics: The Vision of Tomorrow. Eriřim Tarihi: 21 Mart 2025, <https://www.pensees.sg/white-paper-on-video-analytics>
- Rapid Innovation (2024). Role of AI in Surveillance Systems. Eriřim Tarihi: 06 Mart 2025, <https://www.rapidinnovation.io/post/role-of-ai-in-surveillance-systems>
- Reuters (2018). Singapore to test facial recognition on lampposts, stoking privacy fears. Eriřim Tarihi: 11 Mart 2025, <https://www.reuters.com/article/technology/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0S6/>
- Reuters (2025). China Says Facial Recognition should not be Forced on Individuals, Eriřim Tarihi: 11 Nisan 2025, <https://www.reuters.com/technology/china-says-facial-recognition-should-not-be-forced-individuals-2025-03-21>
- Schuilenburg, M., & Peeters, R. (2018). Smart Cities and the Architecture of Security: Pastoral Power and the Scripted Design of Public Space. *City, Territory and Architecture*, 5(13), 1-9.
- Sherpa (2025). Recommendation: Promote Ethics by Design for Researchers in EC-Funded Projects. Eriřim Tarihi: 17 Nisan 2025, <https://www.project-sherpa.eu/ethics-by-design/>
- Smart Nation Singapore (2014). Smart Nation 1.0: Spurring Singapore's Digital Transformation. Eriřim Tarihi: 11 Nisan 2025, <https://www.smartnation.gov.sg/sn1/>
- Smart Nation Singapore (2024). Update on Lamppost as a Platform Project (PQ Reply by Minister Josephine Teo. Eriřim Tarihi: 07 Nisan 2025, <https://www.smartnation.gov.sg/media-hub/parliament/07112023a/>

- TechPolicy (2024). Politicians Move to Limit Predictive Policing After Years of Controversial Failures. Erişim Tarihi: 05 Nisan 2025, <https://www.techpolicy.press/politicians-move-to-limit-predictive-policing-after-years-of-controversial-failures/>
- The New York Times (2018). Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras, Erişim Tarihi: 21 Nisan 2025, <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>
- The Sun (2025). Surveillance State Inside Dystopian Chinese Megacity Of 32million Where Workers 'Don't See Sunlight' & Big Brother is Always Watching. Erişim Tarihi: 17 Mart 2025, <https://www.thesun.co.uk/news/34737593/inside-dystopian-chinese-megacity-sunlight-big-brother>
- Thomson Reuters (2025). Predictive Policing: Navigating the Challenges. Erişim Tarihi: 17 Nisan 2025, <https://legal.thomsonreuters.com/blog/predictive-policing-navigating-the-challenges/>
- U.S. Department of Justice (2024). Artificial Intelligence and Criminal Justice Final Report. Erişim Tarihi: 11 Nisan 2025, <https://www.justice.gov/olp/media/1381796/dl>
- UN (2023). Resolution Adopted by the Human Rights Council on 12 October 2023. Erişim Tarihi: 09 Mart 2025, <https://documents.un.org/doc/undoc/gen/g23/215/42/pdf/g2321542.pdf>
- Utility (2025). Advanced Police Body Camera Technology. Erişim Tarihi: 17 Nisan 2025, <https://www.utility.com/eos>
- Xie, X., & Luo, X. (2022, October). Application of Big Data in Public Security Governance: Dilemma Risk and Optimization Path. In Proceedings of the International Conference on Information Economy, Data Modeling and Cloud Computing (ICIDC 2022).
- Your Europe (2025). Data Protection under GDPR. Erişim Tarihi: 17 Mart 2025, https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

- Zhao, H., & Liu, T. (2025). China's Social Credit System and the Family: Punishment and Collective Resistance. *Economy and Society*, 54(1), 49-69.
- Ziosi, M., & Pruss, D. (2024, June). Evidence of What, for Whom? The Socially Contested Role of Algorithmic Bias in A Predictive Policing Tool. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1596-1608).