KAMU GÜVENLİĞİ TEKNOLOJİLERİNDE SON GELİŞMELER VE KAMUOYUNUN YAKLAŞIMI

TREND ANALİZİ KASIM 2019

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

Taşımacılığın, iletişimin ve ticaretin modernizasyonla hızla değişimi günlük hayatımızı derinden etkiliyor. Günümüzde insanlar tek bir tuşla alışverişlerini yaparak ürünleri adreslerine teslim alabiliyor, mobil cihazlarla günlük işlerini oturduğu yerden yapabiliyor. Teknolojik gelişmelerin hayatımızın her noktasında sağladığı avantajlar kadar bu teknolojileri kötü amaçlarla kullanmak isteyenlerin imkânlarının da geliştiğini kabul etmek gerekiyor. Suçlular teknolojinin gelişimini fırsat bilerek açıkları kovalarken, kamu güvenliğinin de sürekli olarak değişimlere adapte edilerek geliştirilmesi gerekiyor[1].

Kamu Güvenliği, genel olarak toplumunun korunmasını ifade etmektedir. Birincil amaç, toplumu suçlar veya felaketler gibi güvenliği etkileyen krizlerden korumak ve tedbir sağlamaktır. Ortak alanların, kalabalık alanların ve halka açık yerlerin, insanların özgürlüklerini sınırlamadan korunması için özel bazı bilişim çözümlerine ihtiyaç duyulmaktadır[2].

Toplumun geneli kadar bireyler de kamu güvenliğine yapılan saldırılardan etkilenmektedir. Kamusal yaşamın her alanında, gelişen teknolojiler de dikkate alınarak normal yaşamın ve toplum sağlığının her zaman sürdürülebilmesi için kamu güvenliğini sağlayacak önlemlerin uygulanması önemlidir.

Her ülkenin kamu güvenliğini nasıl koruyacağına ilişkin kendi kuralları ve düzenlemeleri vardır. Bununla birlikte, bir tehlikeye maruz kalındığında toplumsal ve bireysel olarak nasıl hareket edileceği konusunda herkesin farkındalığının artırılması gerekmektedir. Bu farkındalığın artırılması için kamu çalışanlarından ve profesyonellerden destek alınabilir. Kamu güvenliği profesyonelleri, insanları doğal afetler, kitlesel saldırılar hatta hırsızlık ve benzeri diğer sosyal sorunlara karşı nasıl korunacakları konusunda bilgilendirebilir.

Ancak kamu güvenliğinin sadece kamu güvenliği profesyonelleriyle sınırlı olmadığı unutulmamalıdır. Sağlık ve salgınlarla ilgili sorunları ele alarak kamu güvenliğini koruyan sağlık çalışanları ve çevreciler de kamu güvenliğinin önemli bir parçasıdır[3].

Kamu güvenliğiyle ilgili birçok organizasyonel yapı bulunduğundan bu yapılar arasında kesintisiz ve uyumlu iletişimin sağlanması da önem kazanmaktadır. Bu noktada her organizasyonun kamu güvenliği teknolojisi için gerekli yatırımı yaparak kendini geliştirmesi ve diğer organizasyonları takip etmesi gerekmektedir[4].

Dördüncü Sanayi Devrimi ile birlikte gelişen veri paylaşımı kamu güvenliğinde de önemli rol oynamaktadır. Bilgi ve haberleşme teknolojileri kritik anlarda çok büyük fayda sağlar. Polis, itfaiye, ambulans servisleri, hatta askeri güçler analitik uygulamalarla ulusal güvenlik için tehlike oluşturabilecek verileri anında yakalayarak kritik durumlara hızla müdahale edebilir. Bu işlemlerde trafik bilgilerinden yüz tanımaya, alışveriş alışkanlıklarından yazışmalara kadar birçok veriden faydalanılır. Bilgi ve iletişim teknolojileri sadece suçların engellenmesinde değil doğal afetler veya acil yardım ihtiyacı olan durumlarda da fayda sağlar[5].

2. KAMU GÜVENLİĞİNİ GELİŞTİREN TEKNOLOJİLER

Teknoloji, güvenlik sektöründe gücü artıran önemli unsurlardan biri olarak destek sağlamaktadır. Birkaç yıl öncesine kadar güvenlik alanında yaşanabilen birçok aksaklık ve gecikme, bilgi ve hızın denkleme daha fazla dahil olmasıyla giderek ortadan kalkmıştır. Teknoloji, kamu güvenliğini sağlayanlar açısından daha hızlı, daha net ve güvenli hizmet imkânı sunar. Bu nedenle günümüzde kamu güvenliğinde öne çıkan ve ilerleyen zamanlarda öne çıkması beklenen önemli teknolojik trendlere göz atmakta fayda var.

2.1 Nesnelerin İnterneti

Dördüncü Sanayi Devrimi ile hayatımıza giren en önemli terimlerden birisi nesnelerin interneti (IoT) olarak biliniyor. Sensörlerin, birbirine bağlı cihazların, kameraların ve diğer iletişim aygıtlarının internet üzerinden hızlı veri transferiyle iletişim halinde olması kamu güvenliğinde görev yapanların müdahale ve önleme gerektiren durumlarda hızla hareket etmelerine imkân veriyor. Birbiriyle koordineli çalışabilen acil durum ve trafik sistemleri olası bir olayda acil müdahale ekiplerinin olay yerine ulaşması için trafik ışıklarını gerekli güzergâhta senkronize çalıştırarak trafik akışını düzenleyebiliyor. Ayrıca olay yerinde ve yakınında bulunan IoT sensörleri ve kameralar müdahale ekiplerine gerekli önlemler ve tespitler için doğru bilgileri sağlayabiliyor.

Bunlarla birlikte gaz kaçaklarını tespit eden sensörler gibi gözlem cihazlarının IoT ile desteklenmesi acil bir durumda güvenlik güçlerinin önceden haberdar edilmesiyle hayatların kurtarılmasını sağlayabiliyor[6].

Teknoloji, toplumu hızla dönüştürürken sadece fiziksel ve sanal dünyalar arasında değil organizasyonlar ve hizmet ettikleri bireyler arasındaki sınırlar da değişiyor. Kamu güvenliği organizasyonlarının ve toplumun hızla gelişen sanal bir dünyada bilgi paylaşımı ve yeni yollarla etkileşime girmesi bekleniyor.

İnsanlardan, araçlardan, sensörlerden ve mobil cihazlardan gelen veriler arttıkça kamu güvenliği organizasyonlarının yoğun verileri işleyebilecek son teknoloji altyapıları, donanımları ve hizmet tasarımlarını kullanmaları gerekiyor. Bazı şehirlerin kanalizasyon sistemlerinde kullandıkları sensörlerle, uyuşturucu miktarındaki artışın tespiti ve topluma gelebilecek zararlara karşı önceden önlem alması bile sağlanabiliyor[7].

IoT teknolojilerinin şehirlere uygulanmasıyla toplumun güvenliği de artırılabiliyor. Örneğin, akıllı sokak lambaları gerekli alanlarda aydınlatmaya destek olarak suç olasılıklarını azaltırken, trafikte araçların seyrinin daha güvenli olması sağlanıyor[8].

"AirQ" gibi şehirlerde bulunan hava kirliliğini ölçen IoT uygulamaları sağlık sorunları oluşmadan çözüm için avantaj sağlıyor. Hırvatistan'da kullanılan teknoloji gaz emisyonlarından havadaki partikül ölçümüne kadar geniş kapsamlı ölçümler yapabiliyor. Bu şekilde artan hava kirliliği bölgeleri tespit edilerek kirliliğin çevresel etkileri artmadan nedenleri araştırılabiliyor[9].

2.2 Yapay Zekâ

Kamu güvenliğinde önemli rol oynayan bir diğer teknoloji olarak yapay zekâ öne çıkıyor. Ulusal güvenlik, polis güçleri veya acil müdahale ekipleri olsun hemen her kamu güvenliği kuruluşu yapay zekâ destekli algoritmaları sistemlerinde kullanıyor. Tehlikenin tespiti, siber güvenlik, dava yönetimi, vatandaş hizmetleri, olay müdahaleleri gibi kullanım alanları olan yapay zekâ birçok alanda olduğu gibi kamu güvenliğinde de geleceği şekillendiriyor[10].

Günlük işlemlerde arka planda çalışabilen yapay zekâ uygulamaları sürekli gözetim özellikleriyle anormal durumların anlık tespitini sağlayabiliyor. Örneğin devriyeye çıkacak olan bir polis ekibine gidecekleri bölgede ortaya çıkan hırsızlık vakalarının artışını lokasyon ve zaman dilimli olarak detaylı bir şekilde sunup önceden hazırlık yapılmasını ve dikkat edilecek konumların tespitini sağlayabiliyor.

Yapay zekâ ile birçok kamera ekranının izlenmesi gibi sorunlar da ortadan kalkıyor. Yoğun miktarda veriyi çok hızlı bir şekilde inceleyebilen yapay zekâ algoritmaları sadece gerekli olduğu durumlarda görüntü akışını öne çıkarabiliyor[6].

Accenture'ın 25 ülkede yaptığı bir araştırmaya göre, kamu hizmeti yöneticilerininin yüzde 70'i gelecek yıllarda yapay zekâya daha fazla yatırım yapmayı planlıyor. Bu oran içinde bulunan yöneticilerin yüzde 78'i ise halkın güvenini kazanacak şeffaf karar mekanizmalı yapay zekâ sistemlerinin önemini vurguluyor. Sonuç olarak bu araştırmada yapay zekâ sistemlerinin kullanımının suçun önlenmesi ve fark edilmesinde sağladığı faydaların yanı sıra sorumlulukla, önyargısız ve herkese açık bir şekilde de uygulanması gerektiği görüşü öne çıkıyor[7].

Mart 2019'da dünyanın en büyük polis organizasyonlarından biri olan New York Polis Teşkilatı (NYPD) 2016'dan beri suçu izlemek ve olası suç kalıplarını belirlemek için yapay zekâ uygulaması kullandığını açıkladı[11]. "Patternizr" adı verilen sistem olaylardan suç kalıpları çıkararak bağlantılı suçları belirleyebiliyor. Aralık 2016'dan beri kullanılan Patternizr türünün ilk örneği olarak gösteriliyor. NYPD eski Analitik Direktörü ve Paternizr araştırmacılarından Alex Chohlis-Wood uygulamayla suç kalıplarının çok daha hızlı ortaya çıkması sonucunda tutuklamaların hızlandığını belirtiyor.

Ancak birçok özel avukat, suçla mücadelede yapay zekâ kullanımının özellikle mevcut ırkçılık ve önyargılı yaklaşımların artmasına neden olabileceği konusunda endişelerini dile getiriyor. NYPD her ne kadar yapay zekâ algoritmalarının ırk ve cinsiyeti dikkate almadan çalıştığını belirtse de geçtiğimiz yıllarda Gartner analisti ve "Yapay Zekâ Önyargısı" adlı makalenin yazarı Darin Stewart, bu konuyla ilgili endişelerini paylaştı. Stewart'a göre, yapay zekâ için ırk ve cinsiyet önyargısı öğrenilen verilerle desteklenerek engellenilmeye çalışılsa da geçmiş tarihli kayıtların makine öğrenmesine dahil edilmesi halen risk oluşturuyor.

NYPD geçmişte de büyük veri teknolojisinin suçla mücadelede kullanımı sebebiyle yoğun eleştirilere maruz kalmıştı. Bu sebeple 2016'da Brannen Center

for Justice, NYPD'nin öngörülü polislik uygulamasına karşı hukuksal mücadeleye gitme yolunu seçmişti. Geçtiğimiz Aralık ayında ise New York Eyaleti Yüksek Mahkemesi polis teşkilatına yapılan geliştirme testleri ve öngörülü polislik yazılımının kayıtlarının açıklanması emrini verdi[11].

İngiltere'de yapılan bir araştırmaya göre de, yapay zekâ kullanımına alışılması polislerin kendileri kontrol etmeden otomatik verilere güvenmelerine ve önyargılı yaklaşımları fark etmemelerine sebep olabilir. Yapılan araştırmaya göre, bir önceki örnekle benzer şekilde geçmiş tarihli kayıtların makine öğrenmesinde kullanılması bazı grupların daha sık izlenmesi veya haksız yere suçlanmasını beraberinde getirebilir[12].

Araştırmada ortaya çıkan bir diğer endişe de evsizler veya bakıma muhtaçlar gibi dezavantajlı insanların kamu hizmetlerini daha fazla kullanmak zorunda kalmaları olarak gösteriliyor. Bu sebeple haklarında daha fazla veri oluşan kişilerin yapay zekâ tarafından risk olarak algılanmaları mümkün görülüyor[12].

Yapay zekâ sistemleri ancak kendisine sağlanan veriler kadar iyi çalışabileceğinden öncelikle girilen verilerin doğruluğundan emin olunması gerekiyor. Bu verilerin doğruluğu da veri güvenliğini izleyen ve kirli verileri yakalayabilen destek programlarıyla sağlandığında yapay zekâ önyargısı probleminin bir ölçüde aşılabileceği düşünülüyor[13].

2.3 Bilgisayar Destekli Sevk (CAD) ve Otomatik Kayıt Yönetim Sistemi (RMS)

ABD'de kanun güçlerinin günlük operasyonlarında sıklıkla kullandığı, kamu güvenliğini artıran ve kaynakların efektif kullanılmasını sağlayan önemli uygulamalardan en önemlileri CAD ve RMS'dir. Bu sistemler suç analizleri, toplum polisliği ve bilgi paylaşım programları için kritik öneme sahiptir[14].

CAD ve RMS sistemlerinin geçmişte kullanılan versiyonları çok karmaşık olmakla beraber kullanımları ve bakımları zaman kaybına sebep olmaktaydı. Yeni bir sistemin kurulması ise uzun yıllar ve milyonlarca dolar gerektiriyordu. Günümüzde inovatif kamu güvenliği yazılım firmaları artık web tabanlı bir yaklaşım olan "Yazılım Hizmeti (SaaS)" ile kuruluşlara ilgilendikleri servislere abone olmaları ve bakım sorumluluklarını hizmet sunanlara bırakmaları konusunda fayda sağlıyor.

Web tabanlı uygulamalarla görev için kritik öneme sahip fotoğraf, video veya bina planları gibi bilgiler bulut depolama alanlarında saklanarak saha personelinin kolayca erişimine imkân veriyor. Web tabanlı CAD ve RMS sistemleri aynı zamanda akıllı telefon ve tabletlerde kolayca kullanılarak kritik bilgilere kesintisiz ulaşım imkânı sunuyor[6].

2.4 5G Teknolojisi

5G teknolojisi özellikle IoT sensörleriyle kamu güvenliği uygulamalarının bağlantılarında daha hızlı ve gelişmiş

iletişim imkânı sunarak kamu güvenliğini iletişim alanında güçlendiriyor. FirstNet™ gibi acil müdahale ekiplerini destekleyen sistemlerin gelişmiş iletişimlerinde de kullanılan 5G, geleceğin iletişim teknojisi olarak öne çıkıyor. 5G teknolojisinin sağladığı ultra hızlı bağlantı imkânı kamu güvenliği uygulamalarının ihtiyaç duyduğu zengin veri trafiğini destekliyor. Düşük gecikme süreleri acil müdahale veya bomba imha gibi zamanın kritik olduğu operasyonlarda görüntünün kesintisiz sunulmasını sağlıyor. Ayrıca yüksek yoğunluk kapasitesiyle binlerce IoT cihazın sorunsuz bağlantısına imkân veriyor[15].

5G teknolojisi tasarımsal olarak da acil bir durumda iletişim önceliğinin kamu güvenlik güçlerinde olmasını sağlıyor. Bu sayede müdahale veya operasyonlarda güvenlik güçlerinin ihtiyaç duydukları verileri öncelikli ve kesintisiz alması mümkün oluyor.

2.5 Giyilebilir Cihazlar (Akıllı Saatler ve Sensörler)

Bu cihazlar sadece spor yaparken veya mesaj okurken değil aynı zamanda kamu güvenliği organizasyonlarında da önem kazanıyor. Saha kaynaklarının kullanımında yöneticilerin akıllı saatlere gönderdikleri bilgiler ve yaptıkları takiplerle ekipleri organize etmesi kolaylaşırken, kullananların çevreye fark edilmeden uyarılması mümkün kılınıyor. Yüksek çözünürlüklü ekranlardan haritalarla GPS uygulamaları kullanılarak keskin yönlendirmeler dahi yapılabiliyor. CAD sistemlerle bağlanabilen akıllı saatler operasyonlarda kritik anlarda uyarılarda bulunabiliyor[6].

Akıllı saatlerde CAD sistemlerin kullanılması birçok durumda fayda sağlıyor[16]:

- Kazalar, çalıntı araçlar, kaçırma olayları, yaralanmalar gibi kritik konularda uyarılar akıllı saatlerle alınabiliyor,
- Destek gerektiğinde tek bir tuşla en yakın ekiplere bilgi verilebiliyor,
- Gerçek zamanlı GPS ile yakın konumda artan olaylarla ilgili uyarılar verilebiliyor,
- Kullananların kalp ritminin izlenmesiyle yaralanma veya ölüm durumunun izlenmesine imkân veriliyor,
- Olaylarla ilgili bilgi güncellemeleri sağlanabiliyor.

2.6 Yüz Tanıma Teknolojisi

Kamu güvenliğini güçlendiren önemli teknolojilerden biri de yüz tanımadır. İnsan yüzü, insanın kimliğini açığa vurduğu için sosyal ilişkilerde önemli bir rol oynar. İnsan yüzünü güvenliğin en önemli unsuru olarak kullanan biyometrik yüz tanıma teknolojisi, hem emniyet güçlerine hem de farklı sektörlere yönelik çok çeşitli uygulamaları sayesinde son birkaç yıldır dikkatleri üzerine çekmeyi başarmıştır. Yüz tanıma sistemi, parmak izi/avuç içi izi ve irisin kullanıldığı diğer biyometrik sistemlere kıyasla temassız işlem özelliği sayesinde belirgin avantajlara sahiptir. Yüz görüntüleri, kimliği tespit edilen kişiye dokunmadan, belirli bir mesafeden yakalanabilir ve tanımlama işlemi için sözkonusu kişiyle etkileşime girilmesine gerek yoktur. Ayrıca, kaydedilen ve arşivlenen yüz görüntüleri daha sonra bir kişinin kimliğini tespit etmede kullanılabildiği için yüz tanıma sistemi, suçlular üzerinde caydırıcı bir etkiye sahiptir[17].

Devletin ve kanun güçlerinin yüz tanıma teknolojisini kamu yararına kullanmasının sağladığı avantajlar kadar

yarattığı endişeler de birçok platformda tartışılıyor. Yakın zamanda yapılan bir araştırma, ABD kanun güçlerinin Motorlu Taşıtlar Dairesi kayıtlarını insanların onayı olmadan kullanarak tanımlama işlemleri yaptığını gösteriyor. Çin gibi bazı ülkeler ise yüz tanıma teknolojisini polis güçlerinin vazgeçilmez bir donanımı haline getirerek kamu güvenliğinde davranış ve aktivitelerin izlenmesine imkân veriyor[18].

Yüz tanıma teknolojisi, girişleri yapılmış kayıtlar üzerinden inceleme yaparak suçlu davranışlarını izlediğinden ırkçılık veya önyargı gibi yaklaşımlara sebep olmuyor. Sadece davranışlarla verileri eşleştirerek sonuçları çok hızlı bir şekilde kullanıcıya aktarıyor. 2017'de Washington Eyalet Şerif Ofisi Bilgi Sistemleri Analisti olan Chris Adzima, aranan bir suçlunun Amazon'un Rekognition sistemiyle nasıl yakalandığını bir blog yazısında açıklıyor. Yazıya göre, eyalet kayıtlarındaki 300 bin vesikalık resmin sisteme yüklenmesiyle üç hafta gibi bir sürede yerel mağazalardan 5.000 dolarlık hırsızlık yapan bir suçlu teşhis edilerek tutuklanıyor.

Yapılan başka bir araştırma ise polislerin sokakta daha uzun süre bulunmasının suçların engellenmesinde önemli bir rol oynadığını gösteriyor. Ceza yazmak, kimlik onaylamak ve bilgilerin sorgulanması ciddi bir zaman kaybı yarattığından bu işlemlerin yüz tanıma teknolojisiyle çok hızlı yapılması polis güçlerinin sokaklarda devriye amaçlı daha fazla zaman geçirmesine imkân verebiliyor[19].

Havaalanları da yüz tanıma teknolojisinin yoğun bir şekilde kullanıldığı kamu alanlarından biri olarak öne çıkıyor. Güvenlik noktalarında kullanılan teknolojiyle suçluların ülkelere girişi engellenebiliyor. Ayrıca insanların izlendiklerini bildikleri takdirde suç işleme olasılıklarının da azalacağı düşünülüyor[20].

Bir diğer yandan yüz tanıma teknolojisi, avantajlarının yanında bazı riskleri de barındırıyor. Kalabalık bir alanda işlenen bir suça karşı kanun güçlerinin suçlunun fotoğrafını sisteme yüklediği bir örnekte binlerce kişi içinden suçlu olan hızla bulunarak tutuklanabiliyor. Ancak sistemin hata yaptığı ve aslında suçluya çok benzer birini hedef gösterdiği bir durum yaşanabilmesi de olası görülüyor.

ABD'de yakın zamanda bir teknoloji firması yüz tanıma teknolojisini kanun güçlerine asla satmayacağını duyurdu. Bir diğer firma ise kongrenin bu taleplerin engellenmesi için müdahil olmasını istediğini bildirdi. Bu gelişmeler yüz tanıma teknolojisinin olası hatalı veya kötü niyetli kullanımına yönelik endişelerden kaynaklanıyor[21].

ABD'nin San Fransisco, Cambridge, Massachusetts gibi birçok şehrinin yönetimi yüz tanıma teknolojisinin risklerinin faydalarından daha fazla olduğunu düşünüyor. Bu sebeple bu teknolojinin kanun güçleri tarafından kullanımının yasaklanması gündemlerinde bulunuyor.

Yüz tanıma teknolojisinin risk yarattığı bir diğer alan da hassas bilgilerin veri bankalarında depolanması olarak düşünülüyor. Siber suçlularca bu verilerin ihlal edilerek kötü niyetle kullanılması toplumda endişe uyandırıyor[20].

Ancak bütün olumsuzluklara rağmen ABD'de yaşayan yetişkin vatandaşların yüzde 50'sinden fazlası kanun güçlerinin yüz tanıma teknolojisini sorumlulukla kullanacağını düşünüyor. Yüzde 59'luk bir kesim de kamu alanlarında suçun önlenmesi için yüz tanıma teknolojisinin kullanımını uygun buluyor. Yapılan araştırma yüz tanıma teknolojisinin kanun güçleri tarafından kullanımını, özellikle ileri yaşlıların gençlere oranla daha uygun bulduğunu da gösteriyor[18].

İzleme teknolojilerinin güçlendirilmesi elbette şehirlerin daha güvenli olmalarında önemli bir rol oynayabilir. Trafik akışı daha iyi düzenlenebilir, havaalanı ve stadyumların giriş sıralarındaki yoğunluk daha hızlı çözülebilir, kamu güvenliği çalışanlarının daha üretken ve hızlı çalışmaları da sağlanabilir. Pew Research'ün yaptığı ankete göre büyük resme bakıldığında insanlar belirli durumlarda güvenlik sözkonusu olunca izlenmeyi kabul edebiliyor. Yüz tanıma teknolojisi gibi gelişmeler güvenlik güçlerinin kullanımı sözkonusu olunca büyük ölçüde toplumda kabul görebilir ancak reklam veya diğer teknoloji firmalarının bu teknolojiyi kullanmaları kamu tarafında hoş karşılanmayabilir.

NYPD komiserlerinden James O'Neill, 2018 yılında yüz tanıma teknolojisi kullanılarak yapılan eşleştirmelerle 1000'e yakın tutuklama yapıldığını belirtiyor[22].

3. KİŞİSEL KAMU GÜVENLİĞİ UYGULAMALARI

Kamu güvenliğini sağlayan organizasyonların yanında bireylerin yapacakları katkılar doğru uygulanabilirse şehirlerin güvenliği daha da iyileştirilebilir.

Amazon'un Ev Güvenlik firmasının sunduğu bir uygulama herkesin kendi mahallesinde güvenliği sağlamasını amaçlıyor. "Neighbors" adı verilen hizmet bir sosyal medya suç bildirim uygulaması olarak çalışıyor. Eğer evinizde Ring güvenlik kameralarından kullanıyorsanız görüntünün anında Neighbors'ta paylaşılması mümkün kılınıyor. Amazon'un küçük suçların engellenmesi için düşündüğü bu uygulama hizmete girdiğinden bu yana yüzlerce bildirim yapılmış durumda. Yapılan bildirimler çoğunlukla şüphe kaynaklı ve beyaz olmayan insanları kapsıyor. Bu sebeple uygulamanın kullanımında ırkçı ve önyargılı yaklaşım riskleri öne çıkıyor[23].

Genç kadınlar için oluşturulmuş "Free to Be" uygulaması ise şehrin herhangi bir yerinde kadınların güvende hissetmedikleri alanların belirlenmesi ve şehir konseyi ile kanun güçlerinin önlem alması için düşünülmüş bir diğer kişisel kamu güvenliği teknolojisi olarak karşımıza çıkıyor. Uygulama, "Plan International Australia" tarafından yapılan bir araştırmada şehirde yaşayan kadınların bazı alanlarda Pakistan'da yaşayan kadınlar kadar güvensiz hissetiklerini belirtmeleri fikriyle ortaya çıkmıştır.

Hindistan, Endonezya, Filipinler, Kolombiya ve Kenya'da kullanılan "Safetipin" adı verilen uygulama ise şehirde güvensiz olarak işaretlenmiş bir alana girdiğinizde veya yaklaştığınızda kullanıcısına uyarı gönderebiliyor. Uygulama güvensiz alanları, bildirimlerin yanında yetersiz aydınlatma ve görüş alanı gibi farklı kriterlerle oluşturuyor[24].

3.1 Akıllı Şehirlerde Kamu Güvenliği

Akıllı şehirlerde kullanılan birçok teknolojinin öncelikle kamu yararına işlemlerin hızlanması, ekonomik hale gelmesi ve güvenliğin artırılması için uygulandığı biliniyor. Bu sebeple bütün teknojilerin bir sinerjiyle hareket etmesi akıllı şehirlerin kamu güvenliğinde daha başarılı olmalarını sağlayabiliyor. İletişim sistemlerinin kesintisiz sağlanması, acil müdahale ve kanun güçlerinin koordineli çalışması, bireylerin zamanında bilgilendirilmesi ve şehrin her noktada izlenerek güvenliğinin artırılması mümkün görülüyor[6].

Singapur akıllı şehir uygulamalarının hayata geçtiği yerlerden biri. Yapılan araştırmalarda Singapurlu vatandaşların kamu hizmetlerinden beklentileri şu şekilde bildiriliyor[25]:

- Vatandaşların yüzde 73'ü güvenliğin kamu hizmetlerinin içinde olmasını bekliyor.
- Vatandaşlar normal suçlara göre siber suçlardan yüzde 54 oranla daha fazla endişe duyuyor.
- Vatandaşların yüzde 67'si dijital alışveriş ve bağışlarda daha güvende hissetmek istiyor.
- Vatandaşların yüzde 60'ı güvenlik güçlerinin kamu güvenliği uygulamalarını destekliyor.

Akıllı şehirler, iletişim sistemleri, görüntüleme ve izleme uygulamaları, yapay zekâ algoritmalarıyla desteklendiğinde aslında güvenli şehirlere dönüşüyor. Şehirde devriye gezen drone'lar gaz kaçakları veya kimyasal sızıntıları tespit edebilen cihazlarla donatılabiliyor. Akıllı aydınlatmalar olay yerini daha fazla aydınlatarak müdahale ekiplerine destek olabiliyor. Akıllı veya güvenli şehir planlaması doğru uygulanırsa suçun engellenmesinde sağladığı faydanın yanında kimseye fark ettirmeden çalışarak herkesin daha güvende hissetmesine imkân veriyor[26].

4. SONUÇ

Kamu güvenliği, herhangi bir ülkenin veya devletin kritik altyapısının önemli bir parçasıdır ve etkili olmasını sağlamak için mümkün olduğunca sağlam, esnek ve güvenilir ağlar ve teknolojiler gerektirir.

Son yıllarda gerçekleşen veri analitiği, otomasyon ve yapay zekâ gibi alanlardaki yenilikler, kamu otoritelerinin, kamu güvenliği hizmetlerini geliştirmek ve iyileştirmek için en son teknolojileri benimsemeye başlamasını sağlamıştır.

Kamu güvenliği teknolojilerinin avantajları ve dezavantajları farklı topluluklarda tartışılırken günümüzde suçun ve terörün yüzde 100 engellenebildiği bir izleme teknolojisi bulunmasa da gelecekte ortaya çıkabilecek yenilikler bu alanda büyük ilerlemeler sağlayabilir[22].

Dijitalleşme ve yeni teknolojilerin yarattığı değişim kamu güvenliği organizasyonlarını yeni riskleri değerlendirmeye zorlarken inovatif çözümleri de beraberinde getirmektedir. Kamu güvenliğinin en iyi şekilde sağlanması verilerle desteklenen önleyici bir yaklaşımla mümkün olabilir. Günümüzde üretilen muazzam miktarda verinin doğru zamanda doğru şekilde kullanımı suç faaliyetlerinin önceden tespit edilmesi ve önlenmesinin yolunu açabilir.

Dijitalleşen çağımızda teknolojilerin kamu güvenliğine ve hizmetlerine dahil olması iş akışlarında tasarruf ve hız sağlarken, aynı zamanda tüm vatandaşların güvenliği daha iyi sağlanabilir[27].

KAYNAKÇA

[1] *Laurier*, (2019), "The Importance of Public Safety in Modern Society", (25 Haziran 2019), https://online.wlu.ca/news/2019/06/25/importance-public-safety-modern-society. (Erişim Tarihi: 28 Ekim 2019)

[2] Mia Teknoloji, "Kamu Güvenliği", http://www.miateknoloji.com.tr/icerik/69/kamu-guvenligi------. (Erişim Tarihi: 28 Ekim 2019)

[3] Cornell, Chris; (2010), "The Importance of Public Safety", *Ezine Articles*, (31 Ekim 2010), https://ezinearticles.com/?The-Importance-of-Public-Safety&id=5298940. (Erişim Tarihi: 28 Ekim 2019)

[4] *Kova Corp*, (2016), "Importance Of Public Safety Technology For Public Spaces And Large Organizations", (1 Eylül 2016), https://www.kovacorp.com/importance-public-safety-technology-public-spaces-large-organizations/. (Erişim Tarihi: 28 Ekim 2019)

[5] *T Systems*, "Security agencies rely on digital technology", https://www.t-systems.com/de/en/industries/public/topics/national-security/public-safety-245930. (Erişim Tarihi: 28 Ekim 2019)

[6] Stockton, Dale; (2018), "5 Major Public Safety Technology Trends for 2019", *Samsung Insights*, (21 Aralık 2018), https://insights.samsung.com/2018/12/21/5-major-public-safety-technology-trends-for-2019/. (Erişim Tarihi: 28 Ekim 2019)

[7] Slessor, James; (2018), "Five technology trends for public safety: More collaborative, connected and intelligent than ever", *Accenture*, (4 Temmuz 2018), https://voicesfrompublicservice.accenture.com/unitedkingdom/five-technology-trends-for-public-safety?lang=en_GB. (Erişim Tarihi: 28 Ekim 2019)

[8] *GSMA*, "Smart Cities Safety", https://www.gsma.com/iot/smart-cities-resources/smart-cities-safety/. (Erişim Tarihi: 28 Ekim 2019)

[9] *GSMA*, (2018), "AirQ Internet of Things Case Study", (Ocak 2018), https://www.gsma.com/iot/wp-content/uploads/2018/02/iot_dt_airq_01_18.pdf. (Erişim Tarihi: 28 Ekim 2019)

[10] Sengupta, Nilanjan; (2019), "AI for public safety: Nilanjan Sengupta weighs in", *Accenture*, (15 Nisan 2019), https://www.accenture.com/us-en/insights/us-federal-government/ai-for-public-safety. (Erişim Tarihi: 28 Ekim 2019)

[11] Charles, J. Brian; (2019), "NYPD's Big Artificial-Intelligence Reveal", *Governing*, (26 Mart 2019), https://bit.ly/2NmDWhR. (Erişim Tarihi: 28 Ekim 2019)

[12] *BBC*, (2019), "Police officers raise concerns about 'biased' AI data", (16 Eylül 2019), https://www.bbc.com/news/technology-49717378. (Erişim Tarihi: 28 Ekim 2019)

[13] Hao, Karen; (2019), "Police across the US are training crime-predicting AIs on falsified data", *MIT Technology Review*, (13 Şubat 2019), https://www.technologyreview.com/s/612957/predictive-policing-algorithms-ai-crime-dirty-data/. (Erişim Tarihi: 28 Ekim 2019)

[14] *International Association of Chiefs of Police*, "CAD/RMS", http://dnn9ciwm8.azurewebsites.net/About-IACP/Governance/-CAD-RMS. (Erişim Tarihi: 28 Ekim 2019)

[15] Burridge, Mike; (2019), "The Facts About 5G for Public Safety", *Sierra Wireless*, (8 Ağustos 2019), https://www.sierrawireless.com/iot-blog/iot-blog/2019/08/5g-public-safety/. (Erişim Tarihi: 28 Ekim 2019)

[16] Kennedy, TJ; (2019), "CAD on Smartwatches Is a Game Changer for Police Communications", (29 Mayıs 2019), https://insights.samsung.com/2019/05/29/cad-on-smartwatches-is-a-game-changer-for-police-communications/. (Erişim Tarihi: 28 Ekim 2019)

[17] NEC, "Bir Yüze Sadece Bir İsimden Daha Fazlasını Yerleştirebilir", https://tr.nec.com/tr_TR/global/solutions/safety/face_recognition/index.html. (Erişim Tarihi: 28 Ekim 2019)

[18] Smith, Aaron; (2019), "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly", Pew Research Center, (5 Eylül 2019), https://www.pewinternet.org/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/. (Erişim Tarihi: 28 Ekim 2019)

[19] Quintas, Peter; (2018), "The Truth and Benefit of Using Facial Recognition in Law Enforcement", *Medium*, (23 Haziran 2018), https://medium.com/10-eight/the-truth-and-benefit-of-using-facial-recognition-in-law-enforcement-55c029080c23. (Erişim Tarihi: 28 Ekim 2019)

[20] Marr, Bernard; (2019), "Facial Recognition Technology: Here Are The Important Pros And Cons", *Forbes*, (19 Ağustos 2019), https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#1074b80514d1. (Erişim Tarihi: 28 Ekim 2019)

[21] Schuppe, Jon; (2018), "Facial recognition gives police a powerful new tracking tool. It's also raising alarms.", *NBC*, (30 Temmuz 2016), https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936. (Erişim Tarihi: 28 Ekim 2019)

[22] Waddell, Kaveh; (2019), "The case for surveillance", *Axios*, (7 Eylül 2019), https://www.axios.com/surveillance-benefits-b06e404e-cc9c-495f-b498-2aab8be37307.html. (Erişim Tarihi: 28 Ekim 2019)

[23] Haskins, Caroline; (2019), "Amazon's Home Security Company Is Turning Everyone Into Cops", *Vice*, (7 Şubat 2019), https://bit.ly/366oeA1. (Erişim Tarihi: 28 Ekim 2019)

[24] *Inspired Adventures*, (2017), "6 Personal safety apps that are revolutionising safety in our cities", (28 Ağustos 2017), https://inspiredadventures.com.au/blog/6-personal-safety-apps-that-are-revolutionising-safety-in-our-cities/. (Erişim Tarihi: 28 Ekim 2019)

[25] Accenture, "Smart Nation Singapore", https://www.accenture.com/sg-en/ps-industry-index. (Erişim Tarihi: 28 Ekim 2019)

[26] *Black & Veatch*; (2018), "Smarter, Safer Cities: Improving Public Safety", (25 Şubat 2018), https://www.bv.com/insights/expert-perspectives/smarter-safer-cities-improving-public-safety. (Erişim Tarihi: 28 Ekim 2019)

[27] Accenture, "Public Safety", https://www.accenture.com/us-en/services/public-service/public-safety. (Erişim Tarihi: 28 Ekim 2019)

thinktech

STM Teknolojik Düşünce Merkezi

http://thinktech.stm.com.tr