Yalvaç Akademi Dergisi

https://dergipark.org.tr/tr/pub/yalvac

DİJİTAL DÖNÜŞÜM EKSENİNDE KENT GÜVENLİĞİ: TÜRKİYE'DE KURUMSAL YAPILANMA, STRATEJİLER VE POLİSİYE UYGULAMALARIN ANALİZİ

Mustafa KALENDER[1*], Çiğdem AKMAN[2]

[1] Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, Türkiye
[2]Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimleri ve Kamu Yönetimi Bölümü, Isparta, Türkiye
Sorumlu Yazar: mkalender11@gmail.com

Özet: Bu çalışma, dijital dönüşüm sürecinin Türkiye'deki kent güvenliği anlayışı ve uygulamaları üzerindeki etkilerini çok boyutlu bir perspektifle analiz etmeyi amaçlamaktadır. Kent güvenliği kavramının dijital çağda nasıl bir dönüşüm geçirdiği teorik bir çerçevede ele alındıktan sonra, çalışmanın kapsamı Türkiye'nin bu alandaki kurumsal ve stratejik mimarisine odaklanmaktadır. Bu bağlamda, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Siber Güvenlik Başkanlığı gibi politika yapıcı kurumların rolü, ulusal kalkınma planları ve siber güvenlik stratejileri gibi temel politika belgeleri incelenmektedir. Çalışmada, nitel araştırma deseni benimsenmiş olup, doküman analizi ve derleme yöntemi kullanılmıştır. Bu kurumsal ve stratejik çerçevenin, Emniyet Genel Müdürlüğü'nün teknolojik kapasitesi ile suçla mücadele yöntemlerine yansımaları da analiz edilmektedir. Son olarak, teknolojik gözetim uygulamalarının bireysel özgürlükler ve hukukun üstünlüğü ile ilişkisi, Amerika Birleşik Devletleri ve Çin gibi farklı ülke pratikleri üzerinden karşılaştırmalı bir bakış açısıyla tartışılarak, konunun yalnızca teknik değil, aynı zamanda hukuki ve sosyal boyutlarına da dikkat çekilmektedir.

URBAN SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION: AN ANALYSIS OF INSTITUTIONAL STRUCTURE, STRATEGIES, AND POLICING PRACTICES IN TÜRKİYE

Abstract: This study aims to analyze the impacts of the digital transformation process on the understanding and practices of urban security in Türkiye from a multidimensional perspective. After addressing the transformation of the concept of urban security in the digital age within a theoretical framework, the scope of the study focuses on Türkiye’s institutional and strategic architecture in this field. In this context, the roles of policymaking institutions such as the Presidential Digital Transformation Office and the Cybersecurity Directorate, as well as key policy documents including national development plans and cybersecurity strategies, are examined. The study adopts a qualitative research design, employing document analysis and literature review methods. It also explores how this institutional and strategic framework is reflected in the technological capacity of the General Directorate of Security and its crime-fighting methods. Finally, the relationship between technological surveillance practices, individual freedoms, and the rule of law is discussed from a comparative perspective, drawing on examples from different countries such as the United States and China, highlighting that the issue is not only technical but also legal and social in nature.

[1] Bu çalışma Çiğdem AKMAN danışmanlığında Mustafa KALENDER tarafından hazırlanan doktora tezinden yararlanılarak hazırlanmıştır.

1. GİRİŞ

Dijitalleşmenin temelinde kolaylık, kırtasiyeciliğin azalması, zamandan tasarruf gibi olgular yer almakta ancak bu kavram bazı tehdit ve riskleri de beraberinde getirmektedir. Bunlardan en önemlisi veri güvenliği ve buna bağlı ortaya çıkan güvenlik açıklarıdır. Güvenlik ise tarih boyunca, insan var olduğu sürece tanımı ve algısı değişime uğrayan bir kavramdır. Güvenlik kavramının bir türü olan kent güvenliği, günümüzde insanların çok büyük bir kısmının kentlerde yaşıyor olması sebebiyle oldukça önemli hâle gelmiştir. Kent güvenliği kavramı tek başına bile oldukça geniş ve çok aktörlü bir kavramken, teknolojide yaşanan gelişmeler ve dijitalleşme bu kavrama daha da zenginlik katmakta; kavramın tanımını ve aktörlerini değiştirebilmektedir. Bu sebeple çalışmada ilk olarak kent güvenliği kavramı anlatılacak ve kapsamı belirlenmeye çalışılacaktır. İkinci olarak, dijitalleşme sürecinin güvenlik kavramına etkisi incelenecek ve kavramda yaşanan dönüşümler belirtilecektir.

Türkiye'de dijital güvenlik konusu ile ilgili çalışmalar 2000'li yılların başına dayansa da somut ve önemli ilk adımlar arasında sayılabilecek "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 2013 yılının ilk çeyreğinin sonlarına doğru yürürlüğe girmiştir. Eylem planının Resmî Gazete'de yayımlanmasından hemen sonra Türkiye Büyük Millet Meclisi'nde 2013 yılının ikinci çeyreğinin başlarında kabul edilerek onaylanan 10. Kalkınma Planı'nda da siber güvenlik konusuna vurgu yapılmıştır. 2018 yılında Türkiye'de yaşanan hükümet sistemi değişikliği dijital güvenlik konusuna da etki etmiş; yeni kurumlar oluşturulmuş, mevcut bakanlıklara da konu ile ilgili önemli misyonlar yüklenmiştir. Yeni oluşturulan kurumların ilki Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'dir. Ofisin haricinde Sanayi ve Teknoloji Bakanlığı'na, Ulaştırma ve Altyapı Bakanlığı'na ve bu bakanlıklara bağlı ve ilgili olan kamu kurum ve kuruluşlarına dijitalleşme ve güvenlik konusunda görevler verilmiştir. Son olarak ise 2025 yılının ilk çeyreğinde Siber Güvenlik Başkanlığı oluşturulmuştur.

Bu doğrultuda çalışmada ofise, başkanlığa, bakanlıklara ve bağlı ve ilgili kamu kurum ve kuruluşlarına verilen bu görevler incelenmiştir. Ayrıca, kent güvenliğini sağlamak için önemli aktörlerden biri olan Emniyet Genel Müdürlüğü'nün gelişen teknoloji ve dijitalleşme süreçlerine uyumu, bu uyum doğrultusunda uyguladıkları proaktif suç önleme modellerinden olan Tahmine Dayalı, İstihbarat Odaklı, Sıcak Nokta modelleri, toplum ve problem odaklı polislik, Yüz Tanıma ve Coğrafi Suç Haritalama teknolojilerinin kullanımı, bu teknolojilerin polisiye uygulamalarına yansımaları ve güncel operasyonlara etkisi irdelenmiştir. Çalışmada son olarak, teknolojinin gelişmesinde aktif rolü bulunan veya gelişen teknolojiyi aktif olarak kullanan ülkelerin güvenlik amaçlı kullandıkları teknolojilerin, bireysel özgürlükler ve hak ihlalleri ile ilgili ne gibi kaygılar ortaya çıkardığına değinilmiş; bu doğrultuda Amerika Birleşik Devletleri, Çin, İsrail, Güney Kore ve Hindistan örnekleri üzerinden bir inceleme yapılmıştır.

2. KENT GÜVENLİĞİ VE DİJİTALLEŞME

2.1. Kent Güvenliği Kavramı ve Kapsamı

Kent sınırlarının genişlemesi ve nüfus yoğunluğundaki artışla birlikte, şehirde yaşayan bireylerin güvenlik kaygıları da artmıştır. Kent yaşamında karşılaşılan problemler; ekonomik, hukuki ve yönetsel gelişmelerin yanı sıra, teknolojik ve bilimsel ilerlemeler ile kentsel dönüşüm süreçlerinin bir sonucu olarak ihtiyaçların hem çeşitlenmesine hem de çoğalmasına neden olmuştur [1].

Günümüzde, nüfusun büyük bir bölümünü barındıran kentlerde güvenlik ihtiyacı oldukça kritik bir hale gelmiştir. Tarihsel süreçte kentlerin oluşumundaki temel etkenlerden biri de güvenlik arayışı olmuştur. Ancak zamanla bu ihtiyacı karşılamak daha güç hale gelmiştir. Nüfusun artışı ve kent yoksullarının çoğalmasıyla birlikte suç, şiddet ve hatta terör olaylarında ciddi bir

yükseliş görülmüştür. Kent güvenliği yalnızca suç oranlarındaki artışla açıklanamaz; bu konu, artık temel bir kentsel hak olarak ele alınmalıdır. Bu bağlamda, şehir içinde sınırlı alanlarda güvenliği sağlamaya yönelik "güvenlikli site" uygulamaları yaygınlaşmıştır. Ancak kent güvenliği, yalnızca belirli bölgelerde sağlanan güvenlikle sınırlı kalmamalı; tüm kentsel alanlarda huzurlu ve güvenli bir yaşamı kapsamalıdır [2].

Son yıllarda kent güvenliği, yalnızca kamu düzeninin sağlanması ve suç unsurlarının ortadan kaldırılmasıyla sınırlı kalmamakta; aynı zamanda kentte yaşayan bireylerin güvenli bir çevrede yaşama hakkını da kapsayan daha geniş bir çerçevede ele alınmaktadır. Güvenli bir kentsel çevre, yalnızca düşük suç oranlarına sahip olmakla kalmaz; aynı zamanda bireylerin yaşam kalitesini artıran, huzurlu ve düzenli bir yaşam alanı sunar. Bu perspektifle güvenlik, yaşam hakkının ayrılmaz bir parçası olarak değerlendirilmekte; güvenli bir kentte yaşamak ise temel insan haklarının başlıca unsurlarından biri olarak kabul edilmektedir [3].

Türkiye'de kentsel güvenlik üzerine yürütülen tartışmalar genellikle suç oranları ve asayiş konuları çerçevesinde değerlendirilmekte; oysa gıda güvenliği, yönetişim, belediye hizmetleri, altyapı, iş güvenliği, sağlık, özel güvenlik ve çevre gibi alanlardaki güvenlik boyutlarına yeterince önem verilmemektedir [4].

Kent güvenliği kavramı ilkel haliyle asayiş ve suç odaklı olup bu haliyle de kapsamı kolluk güçleri odaklıdır. İlkel olmayan hali ise kentte yaşayan her bir bireyin kendisini, kentin her yerinde her hal ve durumda yüzde yüz güvende hissetmesidir. Bu halinde ise kapsamı kolluk güçleri ile birlikte yerel yönetimlere, sivil toplum kuruluşlarına, eğitim kurumlarına, kamu – özel işbirliği ile çalışan kuruluşlara ve hatta kentlinin bizatihi kendisi odaklıdır. Miras olarak kentin herhangi bir yerinde bulunan müstakil binanın metruk binaya dönüşmesi kent güvenliği için bir faktördür. Bu faktörü oluşturan üç, beş kişilik mirasçıdır. Bir kentlinin hurdaya ayrılmış ancak aracın hurdalıkta değil de kentin herhangi bir yerinde lastikleri patlak camları kırık işlevsiz ve kullanışsız bir halde bulunması kent güvenliğini olumsuz etkileyebilecek bir faktördür. Trafik seyrini tehlikeye düşürecek dönüşlerin, ışıkların, yol daralmalarının bulunması kent güvenliği için bir faktördür. Bu faktörü oluşturan yerel yönetimler, ilgili kamu kurumları ve paydaşlarıdır. Bir yükseköğrenim kurumunun veya yurdunun şehrin en ıssız ve ücra yerine kurulması yine kent güvenliği için bir faktördür. Bu faktörü oluşturan ilgili karar makamlarıdır. Sayılan örneklerden de anlaşılacağı üzere kent güvenliği için faktörleri oluşturan bazen kentlinin kendisi bazen kentteki tüm kamu - sivil otorite bazen de kenti bile aşan kamu – sivil karar mercileridir.

Türkiye'de özellikle kentlerde suç ve suçlunun sıfıra indirilmesi asayişin yüzde yüz sağlanabilmesi yakın gelecek için gerçekçi bir hedef olmayacaktır. Bu doğrultuda kent güvenliği kavramına etki edebilecek olan tüm kamu – sivil – özel kuruluşların müşterek çalışmalar içinde bulunması kent ve kentli için fayda sağlayabilecektir.

2.2. Dijitalleşmenin Güvenlik Paradigması Üzerindeki Dönüştürücü Etkisi

Teknolojik gelişim ve dijitalleşme hayatın her alanına yayılması, teknoloji ve güvenlik arasındaki ilişkiyi güçlendiren bir durumu ortaya koymaktadır. Nitekim teknolojik ilerlemeler, güvenlik tehditlerine bütünüyle yeni bir form kazandırmakta ve bu tehditlerin fiziksel ortamdan sanal ortama geçişini hızlandırarak tehdidin maiyetini giderek bulanıklaştırmaktadır. 21. yüzyılda kullanımı giderek yaygınlaşan iletişim teknolojileri, bilgi teknolojileri, robotik teknolojiler, uzay teknolojileri, otonom sistemler ve yapay zekâ ülke içi ve uluslararası seviyede güvenliğin inşasına yönelik geçmişte benzerine rastlanmayan yeni güvenlik tehditlerinin ortaya çıkışına zemin hazırlamaktadır [5].

Güvenlik, insanlığın en eski dönemlerden bu yana ihtiyaç duyduğu temel gereksinimlerden biri olmuştur. Bireyler, yaşadıkları ülke, bölge ya da mahallede güvenlik sorunlarıyla karşılaşmamak adına sürekli olarak çeşitli önlemler alma çabası içinde olmuşlardır. Bu tedbirler, içinde bulunulan dönemin koşullarına bağlı olarak farklılık göstermektedir. Özellikle teknolojik ilerlemeler ve iletişim alanındaki gelişmeler, toplumları ve devletleri sürekli olarak yeni güvenlik stratejileri geliştirmeye ve önlemler almaya yöneltmiştir [6].

Dijitalleşme ile birlikte, kamu hizmetlerinin de dijitalleşmesi vatandaşlara daha hızlı ve etkin bir şekilde hizmet sunulmasını sağlamaktadır. Geleneksel kamu yönetim süreçlerinde uzun bekleme süreleri, karmaşık işlemler ve bürokratik engeller sıklıkla karşılaşılan sorunlardır. Ancak kamunun dijital dönüşümü sayesinde, vatandaşlar çeşitli hizmetlere elektronik platformlar aracılığıyla erişebilir ve işlemlerini kolaylıkla gerçekleştirebilirler [7].

Kamu hizmetlerinin dijital ortama taşınması, hizmetlerin modernleşmesi ve vatandaşlara daha verimli bir şekilde sunulması açısından önemli bir adım olarak görülmektedir. Ancak bu dijital dönüşüm süreci, çeşitli zorlukları ve engelleri de beraberinde getirmektedir. Özellikle güvenlik ve kişisel verilerin gizliliği konuları, dijitalleşmenin karşılaştığı en temel ve hassas sorunlar arasında yer almaktadır [8].

Kamu hizmetlerinin dijitalleşmesi sürecinde en ciddi endişelerden biri, veri güvenliği ve çeşitli tehdit unsurlarıdır. Kamu kurumları, vatandaşlara ait hassas bilgileri toplarken ve işlerken, bu verilerin korunması hayati öneme sahiptir. Veri sızıntıları, siber saldırılar ve kimlik avı gibi tehditler, bilgilerin yetkisiz kişilerin eline geçmesine ve kötü niyetli amaçlarla kullanılmasına neden olabilir. Özellikle sağlık, finansal ve kişisel verilerin güvenliği kritik bir konudur. Bu tür bir güvenlik ihlali, yalnızca vatandaşların devlete olan güvenini zedelemekle kalmaz, aynı zamanda kamu hizmetlerinin etkinliğini ve güvenilirliğini de ciddi biçimde olumsuz etkileyebilir [9].

Dijital dönüşüm süreciyle birlikte kamu hizmetlerine ait veri tabanlarında, büyük ölçüde kişisel bilgi yer alabilmektedir. Bu verilerin toplanması, saklanması ve analiz edilmesi süreçlerinde bireylerin mahremiyetinin korunması ve kişisel verilerin güvenliği, önemli etik sorunlardan biri olarak öne çıkmaktadır. Veri gizliliğine ilişkin politikaların yetersiz veya eksik olması, vatandaşların hem kişisel bilgilerini paylaşma konusunda çekinceler yaşamasına hem de dijital kamu hizmetlerine olan güveninin azalmasına neden olabilmektedir [10].

Güvenlik kavramı çok yakın zamana kadar bilinen, görünen duyulan gibi somut kavramlar ekseninde tanımlanırken dijitalleşme ile birlikte bu somut kavramlara soyut kavramlar da eklenmiştir. Dijital mecralarda ya da kamu – özel e-hizmet kullanımında güvenlik kavramını doğrudan etkileyen yeni ve soyut kavramlar eklenmeye başlanmıştır. Kişisel veri hırsızlığı, özel bilgi, belge ve fotoğrafların korunamaması, Türk Ceza Kanununda yer alan özel hayatın gizliliğini ihlal ve kişisel verilerin hukuka aykırı olarak ele geçirilmesi gibi suçlara sebebiyet vermektedir. Başta bu iki suç türüne ek olarak hırsızlık suçu da belki insanlık tarihi boyunca var olan suçlardır ancak bu suçların dijitalleşme sürecinden önce vuku bulabilmesi için bir kişi – kurum ile karşılıklı fiziksel bir iletişim ve temas olması gerekirken dijitalleşme ile birlikte bu gereklilik tamamen ortadan kalkmış bir kamu - özel e hizmetini kullanırken kişisel bilgileriniz zararlı bir yazılım veya farklı bir yolla hiç temas ve iletişiminizin bulunmadığı üçüncü kişilere aktarılabilmektedir. Bu durum güvenlik algısındaki dönüşümün sebeplerinden biri olabilmektedir.

3. TÜRKİYE'DE DİJİTAL GÜVENLİĞİN KURUMSAL VE STRATEJİK MİMARİSİ

3.1. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Ulusal Yapay Zeka Stratejisi

Türkiye, 2018 yılında Cumhurbaşkanlığı Hükümet Sistemine geçiş yapmış, bu geçişle birlikte yürütme organının başı Cumhurbaşkanı olmuş ve 10.07.2018 tarih ve 1'nolu Cumhurbaşkanlığı Kararnamesiyle Cumhurbaşkanlığına bağlı, özel bütçeli, kamu tüzel kişiliğini haiz, idarî ve malî özerkliğe sahip ofisler kurulmuştur.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi de bu ofislerden bir tanesidir. Görevlerinden bazıları şunlardır [11].:

• "Dijital Türkiye (e-devlet) hizmetlerinin sunumuna aracılık etmek, kurumlar arası işbirliğini artırmak ve bu alanlarda koordinasyonu sağlamak,

• Kamu dijital dönüşüm yol haritasını hazırlamak,

• Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek,

• Kamuda öncelikli proje alanlarında yapay zekâ uygulamalarına öncülük etmek ve koordinasyonu sağlamak,

• Görev alanına giren konularda politika ve strateji önerilerinde bulunmak."

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin görevleri kategorize edilerek incelendiğinde; rehberlik sunmak, koordinasyonu sağlamak, proje tasarlamak, stratejiler geliştirmek, teşviklerde bulunmak, aracılık yapmak, iş birliğini güçlendirmek ve görüş bildirmek şeklinde sıralanabilir. Kısaca, gün geçtikçe önemi artan ve gündemde daha fazla yer alan devletin dijital alanındaki gelişim ve dönüşümünü yönlendirmek, kurumlar arasında uyumu sağlamak temel sorumlulukları arasında yer almaktadır [12].

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı ile Sanayi ve Teknoloji Bakanlığı iş birliğinde ve ilgili tüm paydaşların katılımıyla hazırlanan Ulusal Yapay Zekâ Stratejisi 2021-2025, 2021 yılında yayımlanarak yürürlüğe girmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi 28 Mart 2025 tarih ve 32855 Sayılı Resmi Gazete'de yayımlanan Cumhurbaşkanlığı Kararnamesi ile kapatılmış ve görevlerinin büyük bir bölümü Siber Güvenlik Başkanlığına aktarılmıştır [13].

Ulusal Yapay Zekâ Stratejisi belgesi ülkemizde yapay zeka için oluşturulan ilk stratejik belge olma niteliğindedir. Bu strateji belgesi Cumhurbaşkanlığı İletişim Başkanlığı tarafından gerçekleştirilen faaliyetler doğrultusunda hazırlanmıştır. Dünya genelinde yaşanan gelişmeler ışığında, bazı ülkelerde yapay zeka destekli robotların seçimlerde aday olarak gösterilmesi, Yapay Zeka Bakanlıklarının kurulması ve benzeri girişimler, yapay zekanın hızla yükselen ve durdurulamayan etkisini ortaya koymaktadır. Türkiye, yapay zeka teknolojileri alanında nispeten yeni bir ülke olmasına rağmen, kurduğu kurumlar ve yapılarla bu alandaki gelişmeleri yakından takip etmeye ve sürece ayak uydurmaya çalışmaktadır [14].

Ulusal Yapay Zekâ Stratejisi belgesinde vizyonun, müreffeh bir Türkiye için çevik ve sürdürülebilir yapay zeka ekosistemiyle küresel ölçekte değer üretmek olarak belirlenmiştir. Bu vizyon çerçevesinde ise altı stratejik öncelik oluşturulmuştur. Bunlardan ilki, yapay zeka uzmanlarını yetiştirmek ve alanda istihdamı artırmak, ikincisi, araştırma, girişimcilik ve yenilikçiliği desteklemek, üçüncüsü, kaliteli veriye ve teknik altyapıya erişim imkânlarını genişletmek, dördüncüsü sosyoekonomik uyumu hızlandıracak düzenlemeleri yapmak, beşincisi uluslararası düzeyde iş birliklerini güçlendirmek, altıncısı ise yapısal ve iş gücü dönüşümünü hızlandırmaktır [15].

Ulusal Yapay Zeka Stratejisi belgesinin yapay zeka alanındaki küresel gelişmeler, uluslararası kuruluşların politikaları ve çeşitli ülkelerin strateji belgeleri incelenerek ve yerel ölçekte de ilgili paydaşların görüş ve katkıları alınarak katılımcı bir yaklaşımla hazırlandığı vurgulanmış,

merkezi yönetim ve bağlı kuruluşları dışında özel sektör, sivil toplum kuruluşları, üniversiteler, farklı disiplinlerdeki alan uzmanları ile görüşüldüğü, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Sanayi ve Teknoloji Bakanlığı koordinesinde iki farklı çalıştay düzenlenerek geniş katılımla güçlü ve zayıf yönleri ile fırsat ve tehditlerin belirlendiği, ayrıca ülke genelinde yapay zeka konusu ile ilgili yapılan on farklı çalıştaya da katılım sağlandığı, yapay zeka strateji belgesi hazırlamış olan dört farklı ülkenin uzmanları ile bilgi alışverişi yapıldığı, anket çalışması ve örnek uygulamaların incelenmesi neticesinde ortaya çıkarıldığı belirtilmiştir.

2021 yılında yayımlanan ve beş yıllık bir program için hazırlanan Ulusal Yapay Zekâ Stratejisi belgesinin, paydaş tüm kamu kurum ve kuruluşları başta olmak üzere, sivil toplum kuruluşları, akademisyen ve uzmanların davet edilmesi, çalıştaylar düzenlenmesi ve düzenlenen çalıştaylara katılımcı gönderilmesi, diğer ülke uzmanları ile görüşülmesi, somut ve sayısal verilere dayalı hedefler belirlenmesi, genel amaç ve hedeflerinde alt başlık ve bölümlerle açıklanması gibi pek çok sebeplerden yoğun bir hazırlık sürecinin sonunda ortaya çıktığını göstermektedir. 2025 yılı sonu itibariyle belirlenen hedef ve amaçlara ulaşılması ve temenni edilmektedir.

3.2. Siber Güvenlik Başkanlığı ve USOM: Tehditlerle Merkezi Mücadele

Siber Güvenlik Başkanlığı 08.01.2025 tarih ve 32776 sayılı Resmi Gazetede yayımlanan Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığına bağlı, kamu tüzel kişiliğine haiz ve özel bütçeli bir başkanlık olarak kurulmuştur.

Siber Güvenlik Başkanlığının Cumhurbaşkanlığı Kararnamesine göre başlıca görevleri şunlardır [16].:

• "Siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planları hazırlamak, mevzuat çalışmalarını yürütmek, ilgili faaliyetlerin koordinasyonunu sağlamak, bunların etkin şekilde uygulanmasını takip etmek.

• Siber güvenliğe ilişkin ihtiyaç duyulan alanlarda Ar-Ge ve teknoloji transferi yapmak.

• Siber güvenlik zafiyetlerinin tespit edilmesi amacıyla çalışmalar yürütmek.

• Siber güvenlik acil durum ve kriz yönetim planları oluşturmak, bu planlar çerçevesinde ortak operasyon merkezleri kurmak.

• Siber güvenlik alanında kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılmasına yönelik çalışmalar yapmak.

Siber Güvenlik Başkanlığına, Dijital Dönüşüm Ofisinin kapatılmış olduğu genelge ile yukarıda sayılan görevlere ek olarak "Kamunun dijital dönüşümüne ve kamuda yapay zekâ uygulamalarına öncülük etmek, Dijital Türkiye (e-devlet) hizmetlerinin sunumuna aracılık etmek, bu alanlarda kurumlar arası işbirliğini artırmak ve koordinasyonu sağlamak." Görevi de 28 Mart 2025 tarih ve 32855 Sayılı Resmi Gazete'de yayımlanan Cumhurbaşkanlığı Kararnamesi ile tevdi edilmiştir.

Siber Güvenlik Başkanlığına Cumhurbaşkanlığı Kararnamesi haricinde 12.03.2025 tarih ve 7545 Sayılı Siber Güvenlik Kanunu ile de bazı görevler verilmiştir. Bu görevlerden başlıcaları şunlardır [17].:

• "Kritik altyapılar ve bilişim sistemlerinin siber dayanıklılığının artırılmasına, siber saldırılara karşı korunmasına, gerçekleştirilen siber saldırıların tespitine, muhtemel saldırıların önlenmesine ve etkilerinin azaltılmasına veya ortadan kaldırılmasına yönelik faaliyet yürütmek, bu kapsamda zafiyet ve sızma testleri ile varlıklara yönelik risk analizleri yapmak veya

yaptırmak, siber tehditlerle mücadele etmek, siber tehdit istihbaratı elde etmek, oluşturmak ve paylaşmak, zararlı yazılım inceleme faaliyetleri yürütmek.

• Siber Olaylara Müdahale Ekibi (SOME) kurmak, kurdurmak ve denetlemek, SOME'lerin olgunluk seviyelerinin belirlenmesi ve artırılması için çalışmalar yapmak, siber güvenlik tatbikatları gerçekleştirerek SOME'lerin siber olay müdahale kabiliyetlerini ölçmek, diğer ülkelerin siber olaylara müdahale ekipleriyle koordinasyon kurmak, her türlü siber müdahale aracının ve milli çözümlerin üretilmesi ve geliştirilmesi amacıyla çalışmalar yapmak, yaptırmak ve bunları teşvik etmek.

• Siber güvenlik alanında faaliyet gösterenlerin uyması gereken usul ve esasları düzenlemek.

• Siber güvenlik alanına ilişkin yazılım, donanım, ürün, sistem ve hizmetlere yönelik test ve sertifikasyon işlemlerini yürütmek, buna yönelik test altyapıları kurmak, kurdurmak ve işletmek ile siber güvenlik uzmanları ve şirketlerine yönelik sertifikasyon, yetkilendirme ve belgelendirme işlemlerini ilgili kurumlarla koordineli olarak yürütmek.

• Siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak.

• Kamu kurum ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün ve hizmetleri ile bunları sağlayacak işletmelerin taşıması gereken niteliklere yönelik teknik kriterler belirlemek ve mevzuat düzenlemeleri yapmak, bunların denetimini yapmak ya da yaptırmak, denetimleri yapacak kuruluşların taşımaları gereken nitelikleri belirlemek, bu kuruluşları görevlendirmek, gerektiğinde görevlendirmeyi geçici olarak durdurmak ya da iptal etmek."

Siber Güvenlik Başkanlığı 2025 yılı Ocak ayında bir Cumhurbaşkanlığı Kararnamesi ile kurulmuş ve başkanlığa dair temel kuruluş hükümleri belirlenmiş olsa da yine aynı yılın Mart ayında kanunla çok daha detaylandırılmış ve şekillendirilmiştir. Kurumun bir kararname ile kurulup kanunla da temellendirilmesi kuruma oldukça önem atfedildiğinin göstergesidir. Nitekim 7545 Sayılı Siber Güvenlik Kanunu incelendiğinde siber güvenliğin milli güvenliğin bir parçası olduğu, siber güvenlik çalışmalarının kurumsallık, sürdürülebilirlik ve süreklilik gerektiği hükümleri yer almaktadır.

3.3. Sanayi ve Teknoloji Bakanlığı ve TÜBİTAK'ın Ar-Ge Rolü

10.07.2018 tarihli ve 30474 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren 1 numaralı Cumhurbaşkanlığı Kararnamesi başta olmak üzere diğer mevzuat hükümleri doğrultusunda Sanayi ve Teknoloji Bakanlığı'nın dijitalleşme ve güvenlik ile ilgili görev ve yetkilerinden bazıları özetle şunlardır [18].:

Yüksek katma değerli ve kritik teknolojik ürünlerin milli ve özgün imkânlarla geliştirilmesi ve yerli üretimin artırılmasıyla, ulusal düzeyde teknolojik atılımı hedefleyen Milli Teknoloji Hamlesi'nin temel hedeflerini, odak alanlarını ve yol haritalarını belirlemek; bu hedeflerin hayata geçirilmesi için gerekli tedbirleri almak.

• Bilimsel ve teknolojik ilerleme, ekonomik kalkınma, toplumsal refah ve milli güvenlik doğrultusunda, ilgili kurum ve kuruluşlarla iş birliği yaparak bilim, teknoloji ve yenilik politikalarını oluşturmak ve uygulanmasını sağlamak; sanayi ve teknoloji alanındaki Ar-Ge, geliştirme ve yenilikçilik programlarını, işbirliği ve kümelenme faaliyetlerini desteklemek, teşvik etmek, düzenlemek ve denetlemek.

• Ekonomiye yüksek katkı sağlayan ve birçok sektörde büyümeyi hızlandırma potansiyeline sahip ileri teknolojiler ile büyük veri, yapay zekâ ve siber güvenlik gibi kritik alanlarda,

bireylerin ve işletmelerin Ar-Ge ve üretim kapasitesini artırmak amacıyla politika ve stratejiler geliştirmek; bu stratejilerin uygulanmasını sağlamak; ilgili alanlardaki Ar-Ge, yatırımları ve girişimleri desteklemek, düzenleme ve denetlemeler yapmak.

• Bireylerin ve işletmelerin dijital dönüşümünü desteklemek ve ulusal dijital ekonomiyi geliştirmek için politika ve stratejiler hazırlamak; bu stratejilerin uygulanması için kamu, özel sektör, üniversiteler ve sivil toplum gibi paydaşlar arasında işbirliği ve koordinasyon sağlamak; dijital ekonomi ve dönüşüm ekosistemini güçlendirmek amacıyla programlar ve projeler yürütmek.

• Bilişim ve ileri teknoloji ürünlerinin siber ve bilgi güvenliği seviyesini artırmak; yerli ve milli siber güvenlik ürünlerinin geliştirilmesi ve yaygınlaştırılması; veri merkezi ve veri işleme altyapısını güçlendirmek; siber güvenlik ekosistemini geliştirmek için destek ve teşvik programları uygulamak.

Bakanlığın resmi sitesinde yer alan performans programları ve faaliyet raporları incelendiğinde 2020 - 2024 dönemi için belirlenen amaç ve hedeflerden yine dijitalleşme ve güvenlik konusu ile ilgili olan bölümlerinde dijitalleşme ile gelen yeni dönemin gerekliliklerine uygun yetkinliklerin belirlenmesi, eğitim modellerinin dönüştürülmesi ve sürdürülebilir ilerleme için toplum genelinde yetkinlik gelişimi sağlanacaktır denilmekte, Bilişim, Yazılım, Siber Güvenlik ve Açık Kaynak Yazılım Ekosistemi Geliştirileceği belirtilmekte ve sanayinin dijital dönüşümü sürecinde sürdürülebilirliğin sağlanması ve dijital dönüşümün hızlandırılması yoluyla imalat sanayinin rekabet gücü artırılacaktır denilmektedir [19, 20].

24 Temmuz 1963 tarihinde kurulan Türkiye Bilimsel ve Teknolojik Araştırma Kurumunun (TÜBİTAK), hükümet değişikliği sistemiyle 15.07.2018 tarihli Cumhurbaşkanlığı Kararnamesine göre kuruluş amacı ve yapısı ile ilgili "Türkiye'nin rekabet gücünü ve refahını artırmak ve sürekli kılmak için toplumun her kesimi ve ilgili kurumlarla işbirliği içinde, ulusal öncelikler doğrultusunda bilim ve teknoloji politikaları hakkında çalışmak, bunları gerçekleştirecek altyapının ve araçların oluşturulmasına katkı sağlamak, araştırma ve geliştirme faaliyetlerini özendirmek, desteklemek, koordine etmek, yürütmek, bilim ve teknoloji kültürünün geliştirilmesinde öncülük yapmak amacıyla tüzel kişiliğe, idarî ve malî özerkliğe sahip, Sanayi ve Teknoloji Bakanlığıyla ilgili ve özel bütçeli Türkiye Bilimsel ve Teknolojik Araştırma Kurumu kurulmuştur" ifadelere yer verilmiştir [18].

TÜBİTAK resmi internet sitesinde ise "Toplumumuzun yaşam kalitesinin yükselmesine ve ülkemizin sürdürülebilir kalkınmasına katkı sağlamayı amaçlayan TÜBİTAK, bilim ve teknoloji alanlarında yenilikçi, yol gösterici, katılımcı ve paylaşımcı bir kurum olma vizyonunu benimsemiştir. TÜBİTAK, akademik ve endüstriyel Ar-Ge faaliyetlerini desteklemenin yanı sıra, ulusal önceliklere uygun Araştırma-Teknoloji-Geliştirme çalışmaları yürüten Ar-Ge enstitülerini işletmektedir. Ayrıca, ülkemizin bilim ve teknoloji politikalarını belirleyerek, toplumda bu konularda farkındalık yaratmak amacıyla kitap ve dergi yayınları gerçekleştirmektedir. Bilim insanlarının yurtiçi ve yurtdışındaki akademik çalışmaları burs ve ödüllerle teşvik edilmekte; üniversiteler, kamu kurumları ve sanayi tarafından yürütülen projeler fonlanarak ülkemizin rekabet gücünün artırılması hedeflenmektedir" ifadeleri yer almaktadır [21].

TÜBİTAK 1963 yılında çok dar bir amaç ve kapsam doğrultusunda bir kanunla kurulmuş, teknolojide yaşanan gelişmeler kurumu çok daha etkin ve aktif çalışmalar yapmaya zorlamıştır. Nitekim Cumhurbaşkanlığı Hükümet Sistemine geçişten sonra çıkarılan Cumhurbaşkanlığı Kararnamesi ile görev alanı ve sorumlulukları daha da genişletilmiştir. Ülkemizde dijitalleşme ve güvenlik konusunda en önemli kurumlardan biri olan TÜBİTAK, bünyesinde faaliyet

gösteren araştırma – geliştirme merkezleri ve enstitülerin yapmış oldukları ve yapacakları çalışmalarla dijital çağı yakalama, çağa uyum sağlayabilme ve dijital atılım gerçekleştirme adına çalışmalar yaptığını söylemek mümkündür.

3.4. Ulaştırma ve Altyapı Bakanlığı: BTK ve USOM

10.07.2018 tarihli ve 30474 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren 1 numaralı Cumhurbaşkanlığı Kararnamesi başta olmak üzere diğer mevzuat hükümleri ve bakanlığın resmi sitesinde yer alan performans programları ve faaliyet raporları incelendiğinde bakanlığa dijitalleşme ve güvenlik konusu ile ilgili belli misyonlar yüklendiği görülmektedir.

Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirleme, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirleme, eylem planlarını hazırlama, ilgili faaliyetlerin koordinasyonunu sağlama, kritik altyapılar ile ait oldukları kurumları ve konumları belirleme, gerekli müdahale merkezlerini kurma, kurdurma ve denetleme, her türlü siber müdahale aracının ve milli çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapma yaptırma ve bunları teşvik etme ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmalarını yürütme, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlama bakanlığa yüklenen misyonlar arasındadır [13].

Bakanlığın hedefleri arasında "Bilgi ve iletişim teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemleri siber risk ve tehditlerden koruyarak ülkemizin güvenli işleyen bir siber ortama sahip olması sağlanacaktır" yer almaktadır. Ayrıca yine bakanlığın stratejileri arasında, "ulusal siber olaylara hazırlık seviyesi ve müdahale kabiliyetleri arttırılması, gelişen teknolojiler ve ortaya çıkan tehditler göz önünde bulundurularak oluşturulacak strateji belgesi ve eylem planı ile ulusal siber güvenlik seviyesinin artırılması, ülkemizin siber güvenlik alanındaki ulusal kapasitesi geliştirilecek ve uluslararası alanda Türkiye'nin üst sıralara taşınması" yer almaktadır [22].

Türkiye'de bilgi ve iletişimin verimli ve kaliteli sunumunu, telekomünikasyon alanın işleyiş ve gelişimini tertip eden veya revize eden kurum vazifesi gören Bilgi Teknolojileri ve İletişim Kurumu (BTK), Türkiye çapında oluşturulmuş olan ilk sektörel nitelikteki düzenleyici kurumdur. 2813 sayılı, 5 Nisan 1983 tarihli Telsiz Kanunu'nda değişiklik yapan 27 Ocak 2000 tarihli, 4502 sayılı kanun ile "Telekomünikasyon Kurumu" kurulmuştur. 10 Kasım 2008 tarihli ve 5809 sayılı, Elektronik Haberleşme Kanunuyla "Telekomünikasyon Kurumu" ismi Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir [23].

2813 Sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun hükümlerine göre Kurum görevlerini yerine getirirken bağımsızdır. Hiçbir organ, makam, merci veya kişi Kuruma emir ve talimat veremez. Kurumun ilişkili olduğu bakanlık Ulaştırma ve Altyapı Bakanlığıdır [24].

Yeni teknolojilerin ve yerli üretimin teşvik edilmesi ve haberleşme sistem ve altyapılarının güvenliği ve ulusal siber güvenliğin sağlanması kurumun stratejik amaçları arasında yer almaktadır. Günümüzde hızla ilerleyen bilgi ve iletişim teknolojileri, haberleşme sistemlerinin ve altyapılarının toplumsal işleyiş, ekonomi ve güvenlik üzerinde temel bir etki alanı oluşturduğunu açıkça göstermektedir. Ancak bu dijitalleşme ve bağlantılılık artışı, aynı ölçüde siber tehditlerin de artmasına neden olmuştur. Bu siber tehditler, devletlerin ve bireylerin güvenliğini ciddi şekillerde tehlikeye sokabilen, hassas verilerin sızdırılması ve altyapıların çökertilmesi gibi sonuçlar doğurabilen riskleri beraberinde getirir. Bu bağlamda, ülkemizde Bilgi Teknolojileri ve İletişim Kurumu haberleşme sistemlerinin güvenliği ve ulusal siber

güvenliğin sağlanması stratejik bir öncelik olarak belirlemiş ve Ulusal siber güvenliğin sağlanmasını öncelikli hedefler arasındadır [23].

20.10.2012 tarih ve 28447 sayılı Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince 20.06.2013 tarih ve 28683 sayılı Resmi Gazetede yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ile "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında, ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27.05.2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) oluşturulmuştur [25].

2023 yılı faaliyet raporu önsözünde kurum başkanının da belirttiği üzere Siber güvenlik, sosyal ve ekonomik hayatın seyri ile ilişkili riskler nedeniyle ulusal güvenliğimizin bir parçası haline gelmiştir. Siber saldırılar gün geçtikçe artarak daha karmaşık, odaklanmış, yaygın ve tespiti zor bir hale gelmektedir. Siber güvenlik artık milli güvenliğin önemli bir parçasıdır bu kapsamda kurum bünyesindeki Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile ülkemize yönelik siber tehditlerin bertaraf edilmesi ve olabilecek saldırılara karşı kurum, şirket ve vatandaşlarımızın önceden uyarılması için çalışmalara kesintisiz devam edilmelidir [23].

USOM, Türkiye'deki bütün kamu kurumları, özel sektör kuruluşları, internet servis sağlayıcıları ve diğer internet aktörleri ile çalışma yapma; Sektörel ve Kurumsal SOME'lere, üniversitelere ve siber güvenlik topluluklarına yönelik siber güvenlik eğitimi faaliyetinde bulunma; ulusal ve uluslararası sivil, askeri siber güvenlik tatbikatlarına, NATO tatbikatlarına ve konferanslar ve çalıştaylara katılma yetkilerine de sahiptir. USOM'un siber güvenliğe yönelik uluslararası tatbikat ve organizasyonlarda bulunabilmesi, bu yapının, Türkiye'nin siber güvenlik stratejisi için ne denli kritik bir rol üstlendiğini göstermektedir. USOM'un NATO'nun siber güvenlik tatbikatlarında bulunabilmesi, kıymetli kabiliyete sahip bir yapı olduğunun göstergesidir [26].

3.5. Yasama Organının Rolü: TBMM Dijital Mecralar Komisyonu

Dijital Mecralar Komisyonu 23/7/2020 tarihli ve 7252 sayılı Kanun ile kurulmuştur. Komisyon; kanunlara, bireylerin kişilik haklarına, özel hayatın gizliliğine ve diğer temel hak ve özgürlüklere aykırı yahut çocukların fiziksel ve psikolojik gelişimlerine zarar verici şekilde internet kullanımının önlenmesi amacıyla alınan tedbirler ile yapılan iş ve işlemler hakkında inceleme, görüşme, raporlama, tavsiye ve görüş bildirme işlemlerini yürütmek üzere kurulmuştur [27].

7252 Sayılı Kanun ile Dijital Mecralar Komisyonunun başlıca görev ve yetkileri özetle şunlardır [28].:

• Komisyon Başkanlığının talebi üzerine veya ihtisas komisyonlarının istemi doğrultusunda; Türkiye Büyük Millet Meclisi Başkanlığına sunulan kanun teklifleri ile olağanüstü hal döneminde çıkarılan Cumhurbaşkanlığı kararnamelerini görev alanı açısından inceleyip görüş bildirmek,

• İnternet kullanımının kanunlara, bireylerin kişilik haklarına, özel hayatın gizliliğine ve diğer temel hak ve özgürlüklere aykırı şekilde ya da çocukların fiziksel ve psikolojik gelişimini olumsuz etkileyen biçimde gerçekleşmesini önlemeye yönelik görüş ve öneriler sunmak,

• İnternet aracılığıyla işlenen suçlarla etkili bir şekilde mücadele edilmesine yönelik görüşler ve öneriler sunmak,

• Görevleriyle ilgili olarak, kamu kurum ve kuruluşlarından; 4/5/2007 tarihli ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi" Kanunu kapsamındaki içerik sağlayıcılar, erişim sağlayıcılar, yer sağlayıcılar ile yerli veya yabancı diğer gerçek ve tüzel kişilerden bilgi ve belge talep etmek ve ilgili kişilerden bilgi almak,

• Görev alanına giren faaliyetleri yürüten kamu kurumları, üniversiteler, sivil toplum örgütleri ve kamu niteliğindeki meslek kuruluşlarının çalışmalarından faydalanmak,

• Gerek gördüğü durumlarda, uygun bulduğu uzmanları görüş almak amacıyla davet etmek şeklinde belirtilmiştir.."

Dijital Mecralar Komisyonunun ilki 01.12.2020 sonuncusu ise 20.07.2025 tarihinde olmak üzere farklı yasama dönemlerinde 30 kez toplandığı, toplantılarda yürütme erki başta olmak üzere ilgili kamu kurum ve kuruluşlarının temsilcilerinin dijitalleşme ile ilgili sunumları, dijital gündemde yaşanan son gelişmeler, kanun teklifleri, küresel sosyal medya uygulamaları temsilcilerinin sunumları ve küresel ölçekteki dijital içerik üretilen platform ve arama motor temsilcilerinin komisyonu bilgilendirici sunumlar yaptığı komisyon tutanaklarından anlaşılmaktadır.

3.6. Ulusal Strateji Belgeleri: Kalkınma Planları ve Siber Güvenlik Eylem Planları

Ülkemizde ilk olarak 1963 yılında yayımlanmaya başlayan kalkınma planları beşer yıllık süreler için tasarlanmıştır. Bu beşer yıllık sürelerin tek istisnası dokuzuncu kalkınma planı olup dokuzuncu kalkınma planı yedi yıllık süre için hazırlanmıştır.

Türkiye'de dijital güvenlik konusu ile ilgili çalışmaların 2003 yılında kabul edilen Başbakanlık Genelgesi ile başlamış, 2009 yılında Milli Güvenlik ve Siyaset Belgesinde dijital güvenlik konusunun yer almış, 2012 yılında ise dijital güvenlik ve siber güvenlik konusu ile ilgili politikalar üretilmeye ve eylem planı hazırlıkları yapılmıştır. Nitekim 2013 yılında Ulusal Siber Güvenlik Stratejileri ve Eylem Planının ilki yayımlanmıştır.

Dijitalleşme, dijitalleşme ve güvenlik, siber güvenlik konuları dokuzuncu kalkınma planı dahil olmak üzere ilk dokuz kalkınma planında yer almamıştır. 2014 – 2018 yıllarını kapsayan 10. Kalkınma Planında ise dijitalleşme, dijitalleşme ve güvenlik konularına değinilmemiş olup siber güvenlik konusuna "Bilişim dünyasındaki ilerleme ve gelişmelere bağlı olarak artan siber suçlarla etkin bir şekilde mücadele amacıyla 2011 yılında Emniyet Genel Müdürlüğü bünyesinde özel bir birim kurulduğu, ulusal ve uluslararası güvenlik stratejilerine paralel olarak, birey, kurum ve devleti tehdit eden siber suçlarla etkin bir şekilde mücadele edileceği, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bünyesinde Siber Güvenlik Kurulu oluşturulduğu ve siber güvenlik alanındaki çalışmaların hız kazandığı, kişisel verilerin korunması, ulusal bilgi güvenliği ve elektronik ticaret alanındaki düzenlemelerin tamamlanması ihtiyacının önemini koruduğu" [29] şeklinde değinilmiştir.

On Birinci Kalkınma Planının birinci bölümünde "Küresel Eğilimler ve Türkiye Etkileşimi" başlığı altında "Siber Güvenlik ve Mahremiyet" alt başlığı ile siber güvenlik konusunda iki tespite yer verilmiştir. Bunlar [30].:

• "Dijital teknolojilerin yaygınlaşması ve sınır aşan doğası nedeniyle siber tehdit ve suçların çeşitlenerek genişlemesine bağlı olarak, ulusal savunmanın asli unsurlarından biri haline gelen siber güvenlik konusunda ülkeler gerekli teknik altyapıyı, kurumsal kapasiteyi ve beşeri sermayeyi oluşturmak üzere yoğun çaba sarf etmektedir."

• "Büyük teknoloji firmalarına sahip ülkeler dijital verilerin sınır aşan transferlerinin kolaylaştırılmasını isterken, diğer ülkeler bu transferlere izin vermemekte veya belirli hukuki ve teknik tedbirlerin alınmasını şart koşmaktadır. Mahremiyet koruması ve sınır aşan veri transferleri konusunda daha sıkı düzenlemelerin gündeme gelmesi beklenmektedir."

11. Kalkınma Planında dijitalleşme ve güvenlik konusu ile ilgili belirlenen amaç, politika ve tedbirler ile ilgili, dijitalleşmenin artırılması kamu ve tüm sektörlerde etkin bir şekilde kullanımının yaygınlaştırılması vurgusu yapılmıştır. Yapay zeka kullanımının üretim ve kullanımının artırılması, siber güvenlik alanında hem kamu hem de toplumun tüm kesimi için bilinçlendirici ve geliştirici politikalar üretileceği belirtilmiştir. Güvenlik alanında ise teknolojinin çok daha etkin kullanılması yönünde politikalar geliştirileceği belirtilmektedir.

12. Kalkınma planında dijitalleşme ve güvenlik konusu ile ilgili belirlenen amaç, politika ve tedbirler ile ilgili, 11. Kalkınma Planında da olduğu gibi dijitalleşmenin artırılması kamu ve tüm sektörlerde etkin bir şekilde kullanımının yaygınlaştırılması vurgusu yapılmıştır. Bununla birlikte 11. Kalkınma Planında farklı olarak "dijital devlet" alt başlığı altında temel bir amaç ve 34 politika ve tedbir belirlenmiştir. Dijitalleşme yönüyle 12. Kalkınma Planının 11. Kalkınma Planına göre daha kapsayıcı ve daha çok vurgulanan konu olarak kendisine yer bulduğunu söylemek mümkündür. Yapay zeka kullanımının üretim ve kullanımının artırılması, siber güvenlik alanında hem kamu hem de toplumun tüm kesimi için bilinçlendirici ve geliştirici politikalar üretileceği yine bir önceki planda olduğu gibi 12. Kalkınma Planında da belirtilmiştir. Güvenlik alanında da yine teknolojinin çok daha etkin kullanılması yönünde politikalar geliştirileceği belirtilmektedir.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20.06.2013 tarih, 28683 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Özünde, siber güvenlik alanında bilinç oluşturmak ve bu konuda kurum ve kuruluşların sorumluluklarını yerine getirmelerini sağlamak temel amaçtır. Tüm kamu kurum ve kuruluşlarında bilgi teknolojileriyle gerçekleştirilen işlemlerin güvenliğinin temin edilmesi, kritik altyapıların korunması, siber suç veya olaylar ortaya çıktığında kurumların takip etmesi gereken prosedürlerin belirlenmesi ve bu yol haritasına uygun hareket edilmesini sağlamak genel hedefler arasında yer almaktadır [6].

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı doğrultusunda 29 adet eylem maddesi, 86 adet ise alt eylem maddesi belirlenmiş, sorumlu ve ilgili olduğu kurum ve kuruluşlar listelenerek eylemlerin bir kısmı için bitirilme hedef süreleri paylaşılmıştır.

İlk eylem plan doğrultusunda Siber Olaylara Müdahale Ekipleri (SOME) oluşturulmuş, eğitim ve farkındalık faaliyetleri gerçekleştirilmiş, insan kaynaklarının güçlendirilmesine yönelik altyapılar kurulmuş ve yerli teknolojiler desteklenmiştir. Ancak, genel olarak hedeflerin büyük bir kısmına ulaşıldığını söylemek zor olmaktadır [31].

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2013-2014 yıllarında hazırlanan önceki eylem planlarının süresi dolduktan sonra, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından, teknolojideki gelişmeler ve siber güvenliğin giderek zorunlu hale gelmesi dikkate alınarak oluşturulmuştur. İkinci eylem planının hazırlanması sırasında diğer kurumlarla işbirliği ve koordinasyon faaliyetleri yürütülmüştür. Ayrıca, plan hazırlanırken diğer ülkelerin siber güvenlik alanındaki deneyimlerinden faydalanmak amacıyla, ilgili stratejiler ile araştırma ve geliştirme çalışmaları detaylıca incelenmiş ve değerlendirilmiştir [6].

İkinci eylem planındaki her bir faaliyet için sorumlu ve ilgili kurum ve kuruluşlar belirlenmiştir. Bu çerçevede, ilgili kurumlar eylemlerin tamamlanmasına destek verirken, yetkili kurumlar doğrudan eylemin gerçekleşmesinden sorumludur. Sorumlu kurumların koordinasyon görevini

üstlenirken sürecin yönetiminde aktif rol almaları hedeflenmiştir. Ayrıca, hazırlanan eylemler için bitiş tarihleri belirlenmiş ve bazı eylemlerin sürekli olarak tekrarlanması planlanmıştır [31].

2020-2023 dönemini kapsayan üçüncü Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, önceki planlarda belirtilen hususlara ek olarak, ülke ekonomisinin gelişimi ve korunmasında ulusal güvenlik ve dolayısıyla siber güvenliğin önemine vurgu yapmıştır. Siber güvenlik ve kritik altyapıların korunması konusunda ulusal düzeyde tüm kurum ve kuruluşların koordineli işbirliği içinde hareket etmesi gerektiği belirtilmiştir. Ulusal siber güvenliğin sağlanmasında kritik sektörler tanımlanmış, siber güvenlik kapasitesinin artırılması, siber saldırılara karşı ortak mücadele için güvenli ağların oluşturulması, yerli ve milli teknolojilerin geliştirilip desteklenmesi ve özellikle uluslararası tehditler ve risklere karşı uluslararası işbirliğinin güçlendirilmesi konularına önem verilmiştir [6].

Dördüncü eylem planı olan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) 06.09.2024 tarihinde 32655 sayılı resmi gazetede yayımlanmıştır. Eylem planında öncelikle ilk üç eylem planı ile ilgili değerlendirilmelere yer verilmiş ve gerçekleştirilen çalışmalar sunulmuştur. Bu eylem planında diğer eylem planlarında belirtilen hususlara ek olarak, insan odaklı siber güvenlik yaklaşımı, siber alanda yapılan çalışmaların uluslararası alanda örnek teşkil etmesi amaçları yer almıştır.

4. EMNİYET GENEL MÜDÜRLÜĞÜ ÖZELİNDE TEKNOLOJİK KAPASİTENİN GELİŞİMİ VE POLİSİYE UYGULAMALAR

4.1. Savunma Sanayii Teknolojilerinin Kent Güvenliğine Entegrasyonu

21. yüzyıl itibariyle ülkemizde savunma sanayii alanında önceden gelen birikim ve tecrübe çok daha ilerilere taşınmış, yerli ve milli savunma sanayii ürünleri üretimi teşvik sayesinde üretilmiş, kullanılmaya başlanmış ve geliştirilmeye devam etmektedir. Özellikle son yıllarda "milli teknoloji hamlesi" tabiri oldukça yaygın olarak kullanılmaya başlanmış bu alanda teşvik ve devlet destekleri artırılmıştır. Son kalkınma planları başta olmak üzere stratejik tüm eylem ve planlarda yerli ve milli teknoloji üretimi ve kullanımı vurgulanmaktadır.

Savunma sanayiinde yaşanan bu gelişmelerin Emniyet Genel Müdürlüğüne (EGM) yansımaları ve bu yansımalarında kent güvenliğine bakılacak olursa müdürlüğün resmi sitesinde yer alan 2025 yılı performans programında paylaşılan verilere göre yerli ve milli teknoloji kapsamında bünyesinde 3 adet Atak Helikopteri, 13 adet İnsansız Hava Aracı (İHA), 6 adet Silahlı İnsansız Hava Aracı (SİHA) ve 2 adet Midi İnsansız Hava Aracı (MdİHA) bulunmaktadır [32].

EGM'nin resmi sitesinde yer alan faaliyet raporları incelendiğinde yukarıda sayısal verileri verilen hava araçları ile trafik denetimi yapıldığı ayrıca bombalama, soygun, sabotaj, saldırı, terör eylemleri, cezaevi firarları, kapkaç, gasp gibi olaylara karışan şahısların tespit, takip ve yakalanmaları hava araçları marifetiyle daha kısa sürede mümkün olduğu belirtilmektedir.

4.2. Veri ve Teknoloji Odaklı Modern Polislik Stratejileri

Modern polisiye tedbirlerin temel amacı kısaca kamu düzeni ve istirahatinin temini, şahıs can ve mal emniyetinin sağlanması, suçun önlenmesi ve suçlunun yakalanıp adalete teslim edilmesidir. Modern polisiye tedbirleri klasik polisiye tedbirlerden ayıran en önemli unsur çoğunlukla bir veri veya analize dayalı olmasıdır.

Veri ve teknoloji odaklı modern polisliğin daha anlaşılabilir olabilmesi için düzensiz göçmen ve göçmen kaçakçılığı konusundan bir örnek vermek gerekirse, göçmen kaçakçılığı organizatörü olduğu değerlendirilen kişilere veya konu olarak göçmen kaçakçılığı organizasyonlarına yönelik modern tedbirlerden birinin ya da birden çoğunun aynı anda

uygulanmak suretiyle gerçekleştirilmesidir. Klasik polisiye tedbir ile ise kentlerin işlek meydanlarından gelip geçen yabancı uyruklu şahısların rastgele sorgulanması ve bu sorgulama neticesinde hasbelkader düzensiz göçmen tespitinin yapılmasıdır. Özetle modern yöntemde, hedef şahıs/lar ya da konu, ön bilgi, alan araştırması, istihbari çalışmalar, teknolojik imkanlardan faydalanma varken klasik yöntemde ise sadece bir konu doğrultusunda, ön bilgi, alan araştırması ve istihbari bilgi ve diğer modern yöntemler bulunmaksızın genel sorgulama gerçekleştirilmesidir.

4.2.1. Proaktif Suç Önleme Modelleri (Tahmine Dayalı, İstihbarat Odaklı, Sıcak Nokta)

Öngörücü polislik veya Prediktif polislik olarak da bilinen/anılan tahmine dayalı polisliğin temelinde teknolojik verilere dayalı bir tahmin bulunmaktadır. Teknolojik veri temelli tahminlerle suç kalıpları, suç bölgeleri ve bölgede yaşayan toplumun analiz edilerek suç gerçeklemeden önce önlenmesi amacıyla uygulanan bir modern polisiye tedbirdir.

Polis Akademisi yayınlarında yer alan tanım " Tahmine Dayalı Polislik: Suç kalıplarını analiz ederek suçların nerede meydana gelme olasılığının daha yüksek olduğunu tahmin etmek için verileri ve teknolojiyi kullanmaya dayanmaktadır" şeklindedir [33].

Türk Polis Teşkilatında tahmine dayalı polislik, kullanımı ve etkinliğine dair istatistiki bir veri bulunmasa da İçişleri Bakanlığı resmi sitesinde paylaşılan haber ve duyurulardan "Analiz Sistemleri Narkotik Ağı ASENA programı, milyonlarca veriyi yapay zeka ile birleştirerek bir arabanın uyuşturucu kaçırıp kaçırmayacağını tespit ediyor. Bu arabanın burada ne işi var, bu arabanın sahibi kim, bu araba niye bu rotaya gidiyor veya bir kişi, bu insanlarla niye bir ilişki içerisinde? Hemen alarm çalıyor, oraya gidiliyor. ASENA programının başladığı 1,5 yılda 6 bin 636 yakalama oldu. Programın verdiği her 100 alarmın yarıya yakını doğru. Bu, bazen istihbari olarak takip edemediğimiz bazen ihbarla gelmeyen birçok yakalamanın gerçekleşmesini sağlıyor" [34] tahmine dayalı polislik yöntemlerinin kullanıldığı sonucunu çıkartmak mümkündür.

İstihbarat odaklı polislik kavramı oldukça geniş ve tanımlaması zor olan kavramlardan bir tanesidir. İstihbari bilgilerin polisiye tedbirlere işlenmesi ya da suç sonrası şüpheli tespiti ve yakalanmasına yönelik olarak kullanılması olarak tanımlamak yanlış olmayacaktır.

Polis Akademisi yayınlarında yer alan tanım "İstihbarat Odaklı Polislik: Polislik stratejilerini güçlendirmek ve polisin kaynaklarını yüksek riskli alanlara hedeflemek için verileri ve istihbaratı kullanan suç önleyici tedbirdir" [33] şeklindedir.

Türk Polis Teşkilatında istihbarat odaklı polisliğin 1937 yılında Önemli İşler Şube Müdürlüğünün EGM bünyesinde kurulmasıyla başlamış olabileceğini söylemek mümkün ise de Osmanlı Devletinin son dönemlerinde Erken Cumhuriyet Döneminde de polis teşkilatı içerisinde farklı isimler altında istihbarat faaliyetlerinin kesintili de olsa sürdürüldüğü görüşü de bulunmaktadır [35].

Sıcak nokta polisliği, suçun önceki tarihlerde yoğun olarak işlendiği bölge /mahalle /semt /cadde /sokaklarda yeniden işlenmemesi adına nokta bazlı alınan tedbirlere denilmektedir. Polis Akademisi yayınlarına göre ise Sıcak Nokta Polisliği: Polis kaynaklarının suç oranlarının yüksek olduğu bölgelerde yoğunlaştırılmasına dayanan modern suç önleyici tekniktir. Dünyanın çeşitli ülkelerinde yaygın kullanımıyla dikkat çekmektedir [33].

Sıcak nokta polisliği veriye dayalı bir önleyici polislik tedbiri olması nedeniyle modern polisiye tedbirler arasında sıralanırken suçların yoğun olarak işlendiği alanlarda tekrar suç işlenmemesi adına çoğunlukla klasik polisiye tedbirler uygulanmaktadır.

4.2.2. Toplum ve Sorun Merkezli Yaklaşımlar (Toplum Odaklı, Problem Odaklı)

Toplum odaklı ya da destekli polislik suç ve suçlularla etkin mücadele edilebilmesi amacıyla toplumun da bu mücadeleye dahil edilmesi zemininde oluşturulmuş bir tedbir modelidir. Toplumla daha fazla irtibat ve işbirliğinin suç önleme ve suçlu tespitine katkı sağlayacağı modelin temel argümanıdır.

EGM'nin tanımı "Etkin bir güvenlik hizmeti yürütülmesinde kabul gören anlayış; suçla mücadeleye ve güvenlik politikalarının uygulanmasına toplumun katılım ve desteğinin sağlanmasına dayanmakta; öncelikle toplumsal beklentilerin ve taleplerin karşılanması bu anlayışın odak noktasını oluşturmaktadır. Buna kısaca "Toplum Destekli Polislik" denilmektedir" şeklindedir [36].

Polis Akademisi yayınlarında yer alan tanım ise "Toplum Odaklı Polislik: Polis ve toplum üyeleri arasında suç ve güvenlik endişelerini ele almak için ortaklıklar kurma, toplumu veri toplama ve kullanılacak teknolojiye karar verme sürecini bilgilendirme gibi adımları içeren modern suç önleyici tedbirdir" şeklindedir [33].

EGM resmi internet sitesine göre bilgilendirme çalışmaları, bireysel irtibat çalışmaları, okul aile birliği toplantılarına katılım, sosyal etkinlikler, sosyal yardım faaliyetleri, suç mağduru ve diğer destek ziyaretleri [36] toplum odaklı polisliğin temel taşlarını oluşturmaktadır. Türk Polis Teşkilatında 2006 yılından itibaren pilot iller şeklinde uygulamaya konulan toplum odaklı polislik modelinin 2009 yılı itibariyle tüm illerde şube müdürlüğü olarak kuruluşu gerçekleşmiş olup çalışmalarını sürdürmektedir.

Problem odaklı polislik suç işlenmesini tetikleyen, sebep olan unsurların belirlenmesi ve bu unsurlara karşı topyekûn müşterek bir mücadeleyi öncelik edinmiş bir model olduğunu söylemek mümkündür. Polis Akademisi yayınlarına göre ise Problem Odaklı Polislik: Yoksulluk, uyuşturucu bağımlılığı ve evsizlik gibi suça katkıda bulunan temel konulara odaklanmak ve bu konuları çok disiplinli ortaklıklar yoluyla ele almaya dayanan, çok boyutlu sorunları çözmeye odaklanan bir önleyici tedbirdir [33].

Türk Polis Teşkilatında problem odaklı polislik uygulaması olarak doğrudan yapılan bir çalışma bulunamamıştır. Bunun yerine toplum destekli polislik modeli ile örneğin uyuşturucu ile mücadele konusunda başta aileler olmak üzere toplumun belli kesimlerini de mücadeleye dahil etme çalışmalarına rastlanmışsa da sistematik ve tek düze bir uygulama olduğu söylenemeyecektir.

4.2.3. Teknolojik Gözetim ve Analiz Araçları (Yüz Tanıma, Coğrafi Suç Haritalama)

Yüz tanıma uygulaması, teknolojik alt yapı sayesinde bir olaya karışan ve suçlu olarak nitelendirilen kişilerle bir olaya karışacağı değerlendirilen kişilerin açık kimlik bilgilerinin tespit edilebilmesi amacıyla kullanılan bir modeldir.

Türkiye'de yaygın kullanım alanına sahip modern suç önleyici tedbirlerden birisi de yüz tanıma uygulamasıdır. Yüz tanıma, yüzlerin benzersiz özelliklerini analiz ederek, bir kişiyi tanımlamak için kullanılan bir teknolojidir. Bir eşleşme bulmak için elde edilen bir görüntünün yüz özellikleri, bilinen yüzlerden oluşan bir veri tabanıyla, algoritmalar vasıtasıyla karşılaştırmalar yapılmaktadır. Bu yöntem, genellikle güvenlik amacıyla kullanılır (örneğin, telefonların kilidini açmak), öte yandan, gizlilikle ilgili endişeleri de beraberinde getirmektedir. Yüz tanıma teknolojisi bazen polis kuvvetleri tarafından adli soruşturmalar ve şüphelileri belirlemek için kullanılmaktadır [33].

Yüz tanıma uygulamasının Türk Polis Teşkilatında kullanıldığı, yasal dayanak olarak 2559 Sayılı Polis Vazife ve Salahiyet Kanunu (PVSK) 5, ek 6 ve ek 7. maddeleri olduğunu haricen uygulamanın kullanımına engel bir mevzuat hükmü bulunmadığını söylemek mümkündür. Coğrafi suç haritalama sistemi, suç türlerinin nerede ve ne zaman işlendiğini esas alarak teknolojik verilerle haritada görsel olarak sunulması modelidir. Bu modelin temel amacı suç türlerinin zaman ve mekan bakımından tespitinin yapılması akabinde diğer klasik ve modern polisiye tedbirlerin doğru yer ve zamanda uygulanmasıdır. Coğrafi Suç Haritalama Sistemi, polis kuvvetlerinin suç verilerini coğrafi konumlara göre görselleştirmesine ve analiz etmesine olanak tanıyan bir araçtır. Suç olaylarını haritalamak; kalıpları, eğilimleri ve sıcak noktaları görüntülemek için Coğrafi Bilgi Sistemleri Teknolojisini kullanılmaktadır. Sistem, polis kuvvetlerinin suçun mekânsal ve zamansal yönlerini daha iyi anlamalarına ve kaynakları nereye tahsis edecekleri konusunda daha bilinçli kararlar vermelerine yardımcı olmaktadır [33]. Coğrafi suç haritalama sistemi sayesinde mekan – suç ilişkilerinin analizinin yapılabilmesine, suçun yoğun olarak gerçekleştiği bölge insanının gerçekleşen suç türlerine karşı kişisel tedbir noktasında bilgilendirilmesine ve işbirliği yapılabilmesine, alınacak tedbirlerin doğru olarak belirlenebilmesine ve tedbirlerin etkinliğinin tespit edilebilmesine imkan sağlamaktadır.

4.3. Polisiye Stratejilerin Sahadaki Yansımaları: Güncel Operasyonların Tematik Analizi

Emniyet Genel Müdürlüğü (EGM) kurulduğu tarihten itibaren suç ve suçlularla etkin mücadele, kamu düzeni ve asayişin sağlanması, can ve mal güvenliğinin temini gibi konularda çalışmalar yapmaya devam etmektedir. Özellikle teknolojik gelişmeler, küreselleşme, salgın hastalıklar ve savaşlar son yıllarda suç ve suçlularla çok daha etkin bir mücadeleyi zorunlu hale getirmiştir. Yaşanan bu gelişmeler yeni suç ve suç alanları ortaya çıkarmakla birlikte yeni mücadele yöntemleri geliştirmeyi de gerektirmektedir. Bu doğrultuda EGM'nin yeni tedbirler kapsamında da yapmış olduğu çalışmalar bulunmaktadır. Bu çalışmalarda EGM'nin ve diğer silahlı kolluk kuvvetlerinin yapmış olduğu operasyonlara operasyon içeriğine göre isimler verilmiş ve elde edilen neticeler bakanlığın resmi sitesinden 2023 yılı son çeyreğinden itibaren paylaşılmaya başlanmıştır. İçişleri Bakanlığı ve bağlı kuruluşları yıllardır her türlü suç ve suçlularla mücadele etmeye devam etmektedir ancak yapılan bu mücadelelerin paylaşımı ki özellikle sayısal veri paylaşımı EGM ve diğer silahlı kolluk kuvvetleri için 2023 yılının son çeyreğinden itibaren yapılmaya başlanmıştır.

2023 yılı son çeyreğinden itibaren yapılan operasyon isimlendirmeleri ve bu kapsamda yapılan operasyonlar hem EGM hem Jandarma Komutanlığı hem de Sahil Güvenlik tarafından yapılmaktadır. Ancak yapılan arşiv tetkikinde operasyonların büyük çoğunluğunun EGM tarafından gerçekleştirildiği dikkati çekmektedir. Yapılan bu operasyon isimlendirmeleri ve içeriği aşağıda tabloda sunulmuştur.

Tablo 1. Güncel Polisiye Tedbirler Kapsamında Yapılan Çalışmalar

Operasyon İsmi	Operasyon İçeriği
Bozdoğan (Kahramanlar)	Bölücü Terör Örgütleri
Çember	Aranan Şahıslar
Kalkan	Göçmen Kaçaklığı
Kıskaç	Fethullahçı Terör Örgütü / Paralel Devlet Yapılanması
Kuyu (Mahzen / Kafes)	Organize Suç Örgütleri
Mercek	Ruhsatsız Silah Üretim, Ticareti ve Taşınması
Narkoçelik (Narkogüç)	Uyuşturucu Kullanımı, Üretimi ve Ticareti
Sibergöz	Çevrimiçi Suçlar

Kaynak: Yukarıdaki tablo 04.06.2023 – 03.06.2024 tarihleri arasında İçişleri Bakanlığı tarafından bakanlığın son bir yılında yapılan operasyon ve çalışmalara yönelik 13.06.2024 tarihinde gerçekleştirilen basın toplantısında paylaşılan bilgi ve sunumlar doğrultusunda yazar tarafından oluşturulmuştur.

Tabloda operasyon isimleri sütununda parantez içerisinde yer alan isimler daha önce operasyon içeriğine göre o isimlerin kullanıldığı tespit edildiğinden paylaşılmıştır. Örneğin organize suç örgütlerine yönelik yapılan operasyonlar ilk olarak Kafes olarak adlandırılmış daha sonra bu kapsamda yapılan operasyonlar Mahzen olarak nitelendirilmiş son olarak da Kuyu ismiyle paylaşılmaktadır. Operasyon isimlerindeki bu değişiklikler ile ilgili dikkat çeken konu bir isimle 50 farklı operasyon yapılmışsa o kapsamda yapılan operasyonda isim değişikliğine gidildiği gözlemlenmiştir. Norkogüç adıyla 50 farklı operasyon yapıldıktan sonra Uyuşturucu kullanım, üretim ve ticaretine yönelik yapılan operasyonlara Narkoçelik isminin verildiği görülmektedir.

Tablo 2. Güncel Polisiye Tedbirler Kapsamında Yapılan Operasyon Verileri

Operasyon İsmi	Gerçekleştirilen Operasyon Sayısı	İşlem Yapılan Kişi Sayısı (GÖZALTI)	Tutuklanan Kişi Sayısı	Gözaltı / Tutuklu Oranı (%)
Bozdoğan (Kahramanlar)	34.215	14.085	2.856	20
Çember	18	198.918	-	-
Kalkan	7.599	12.386	4.493	36
Kıskaç	5.543	8.892	1.595	18
Kuyu (Mahzen / Kafes)	1.451	10.285	3.891	38
Mercek	20	121.027	-	-
Narkoçelik (Narkogüç) (TCK 188 Verileri)	44.937	74.703	31.792	43
Sibergöz	3.201	13.502	3.597	27
TOPLAM	96.984	453.798	48.224	30

Kaynak: Yukarıdaki tablo 04.06.2023 – 03.06.2024 tarihleri arasında İçişleri Bakanlığı tarafından bakanlığın son bir yılında yapılan operasyon ve çalışmalara yönelik 13.06.2024 tarihinde gerçekleştirilen basın toplantısında paylaşılan bilgi ve sunumlar doğrultusunda yazar tarafından oluşturulmuştur.

04.06.2023 -03.06.2024 tarihleri arasında silahlı kolluk güçlerince yukarıda verilen 8 farklı operasyon alanı için toplam 96.984 operasyon yapılmış, yapılan bu operasyonlarda 453.798 şahıs gözaltına alınmıştır. Aranan şahıslara yönelik çember ismiyle ve Ruhsatsız Silah Üretim, Ticareti ve Taşınmasına yönelik mercek adıyla yapılan operasyonlarda tutuklu sayısı paylaşılmadığı için gözaltına alınan şahıslardan tutuklananların oranı hesaplanamamıştır. Ancak özellikle aranan şahısların tamamı ya da çok büyük bir kısmının tutuklanmış olma ihtimali çok yüksektir çünkü haklarında kesinleşmiş hapis cezalarıyla aranmakta olduğu paylaşılan veriler arasındadır. Yukarıdaki tabloya göre tutuklama oranının en yüksek olduğu alan uyuşturucu ticareti suçudur. İkinci sırada organize suç örgütlerine yapılan operasyonlar üçüncü sırada ise göçmen kaçakçılığına yönelik yapılan operasyonlar yer almaktadır.

5. TEKNOLOJİK GÖZETİM, BİREYSEL ÖZGÜRLÜKLER VE HUKUKUN ÜSTÜNLÜĞÜ: KARŞILAŞTIRMALI BİR DEĞERLENDİRME

5.1. Amerika Birleşik Devletleri: Gözetim ve Mahremiyet Tartışmaları

Amerika Birleşik Devletleri, modern demokrasi olgusunun ortaya çıkmış olduğu ilk ülke olarak bilinmektedir. Bununla birlikte ülke, zenginlik, gelişmişlik seviyesi ve teknoloji noktasında dünya sıralamalarında daima zirve ve zirveye en yakın noktada yer almış ve bulunduğu konumu korumuştur [37].

11 Eylül 2001 terör saldırı sonrası ülkede ve hatta tüm dünyada güvenlik algısı değişmiş ve bu değişim ulusal güvenlik için anti – demokratik uygulamaların kullanılabilmesine de sebebiyet

vermiştir. Ancak ulusal güvenlik (terör, organize suç vb.) yönüyle kullanılan anti – demokratik uygulamalar devletin tüm bireylerini doğrudan etkilememiştir. Ancak Covid – 19 virüsünün ortaya çıkması ve pandemi süreci devletin neredeyse tüm bireylerini doğrudan etkilemiş ve mücadele kapsamında yürütülen tedbirlerin ulusal güvenlik uygulamalarının bir benzeri olması tartışmaları beraberinde getirmiştir.

Amerika'da pandemi tedbirleri kapsamında bilindik temas izleme uygulamaları dışında bazı sosyal medya şirketlerinden elde edilen verilerin kullanılmasının ortaya çıkması iki farklı hukuksuzluğu ve anti demokratik durumu gözler önüne sermiştir. Bunlardan ilki uygulama şirketi ya da uygulama şirketinin dışındaki bir şirketin, kullanıcının rızası olmadan verileri farklı bir amaç doğrultusunda işlemesi ve bundan gelir elde etmesi, ikincisi ise devletin bir şirketten kullanıcı verilerini alması ve kendi amaçları doğrultusunda kullanmasıdır [38].

Sosyal medya uygulamalarını kullanmak için sosyal medya şirketiyle paylaşılan kişisel verilerin ve uygulama kullanımı esnasında kullanılan konum bilgilerinin sosyal medya şirketleri tarafından işlenmesi, bu verilerin kamu kurumlarıyla paylaşılması ve dahası başka şirketlere de satılması çok yönlü eleştirileri ortaya çıkarmaktadır. Devletin kişisel verileri koruma adına politikalar yürütmesi gerekirken kişisel verileri şirketlerden (satın) alan, satılmasına / paylaşılmasına göz yuman konumunda bulunması ve bu verileri pandemi mücadelesi kapsamında kullanması anti demokratik bir süreç olarak nitelendirilmiştir.

5.2. Çin: Sosyal Kredi Sistemi ve Kitlesel Gözetim Uygulamaları

Çin Halk Cumhuriyeti, 2000'li yıllardan önce ekonomi, teknoloji, politika ve uluslararası ilişkiler alanlarında yaptığı atılımlarla, teknoloji ya da milenyum çağı olarak adlandırılan 21. yüzyıla hazır bir şekilde girmiştir. Ekonomi ve teknolojiye yatırım yapan firmaların girişimleri ve üretimleri ile ucuz iş gücünün sağladığı avantajlar, Çin'de önemli bir üretim merkezi oluşmasını sağlamıştır. Ekonomik açıdan uygun koşullarda yapılan üretimin fazla arz yarattığı baskı ve dünya genelindeki yüksek talep, Çin'in küresel pazarlarda etkin bir oyuncu haline gelmesinin başlıca nedenlerindendir [39].

Dünyanın en gelişmiş teknolojisine sahip ilk üç ülkesinden biri olarak kabul edilen Çin, geliştirmiş olduğu bu teknolojiyi güvenlik politikalarına entegrasyonu hakkında Covid – 19 virüsü ve pandemi sürecine kadar bilgi sahibi olunamıyordu. Virüsün ortaya çıktığı ülke olan Çin'in pandemi mücadelesindeki teknoloji temelli tedbirlerden bazılarının anti demokratik olduğu iddia edilmektedir.

Anti demokratik olduğu iddia edilen tedbirlerden birincisi, hükümet salgın döneminde, iki büyük mobil ödeme sistemi sağlayıcısı Alipay ve WeChat, kullanıcıların sağlık, konum ve finansal verilerini birleştirerek kişisel enfeksiyon riskini değerlendiren uygulamaları hızla devreye almıştır. Çin hükümeti, vatandaşların salgın sürecinde karantinaya alınıp alınmayacağına veya kamusal alanlara giriş izinlerinin verilip verilmeyeceğine karar vermek amacıyla, bu uygulamaların akıllı telefonlarda kullanılmasını zorunlu kılmıştır. Vatandaşlara, uygulama üzerinden sağlık durumlarını yetkililere gösterebilmeleri için yeşil, sarı ve kırmızı renklerde QR kodlar verilmeye başlanmış ve bu sistem hızla ülke genelindeki tüm şehirlere yaygınlaştırılmıştır [40].

Anti demokratik olduğu iddia edilen tedbirlerden ikincisi ise Çin'de, salgınla birlikte hükümetin köy ve sokaklarda sayısını artırdığı kapalı devre televizyon kameralarının (CCTV), apartman girişlerine de yerleştirilmeye başlandığı, vatandaşların bu kameralara kendisini tanıtmasının zorunlu hale geldiği ve kayıt altına alınmanın meşrulaştırıldığı görülmektedir [41].

5.3. İsrail, Güney Kore ve Hindistan: Ulusal Güvenlik Odaklı Teknoloji Kullanımı ve Hukuki Sınırlar

İsrail 1990 ve sonraki yıllarda uygulamış olduğu yenilik ve teknoloji politikaları sayesinde iyi bir ekonomik seviyeye ulaşmış, gelir ve refahlarını artırmış ve gelişmiş batı ülkeleriyle olan gelişmişlik farkını kapatmışlardır. Bu ekonomik iyileşme ve gelişmişlik düzeyi teknoloji politikalarına ve yatırımlarına da etki etmiş, yazılım, veri tabanı yönetimi, eğitim yazılımları, internet yazılımları, anti-virüs ve bilgisayar destek-koruma-güvenlik sistemleri alanında gelişmeler göstermiş, fiber-optik, elektro-optik kontrol sistemlerinde ise dünya liderliğine yaklaştığını söylemek mümkündür [42].

Dünya Sağlık Örgütü tarafından pandemi ilan edilmesinden hemen sonra İsrail Başbakanı ülkenin iç güvenlik ve istihbarat ajansına (Şin-Bet) yetki verdiğini, virüsün yayılımını izlemek ve karantina süreçlerini kontrol altında tutmak için tüm yurttaşların konum geçmişlerine ulaşacak ve telefon izleme yazılımını kullanılacağını duyurmuştur [41].

İsrail başbakanı tarafından verilen bu yetki ile vatandaşlarının seyahat geçmişine, sağlık bilgilerine, salgın bölgelerinde ne kadar zaman geçirdiklerine, potansiyel olarak virüs taşıyanlarla temasa geçip geçmedikleri başta olmak üzere kişisel veri ve mahremiyet kapsamında olduğu nitelendirilecek birçok bilgiye erişilebildiği ortaya çıkmıştır.

İsrail'de Pandemi süreci ile birlikte salgın hastalıkların yayılımını önlemek amacıyla kullanılan ve devlet otoritesinin veriler ve teknolojik takip sistemleri sayesinde erişebildiği bilgilerin ortaya çıkmasıyla gizlilik ve kişisel veri alanlarında kaygıları artırmış, dijital gözetim teknolojisinin gelişimi ve ulaştığı nokta hakkında da fikir vermiştir.

Güney Kore, dünyanın en büyük on ekonomisinden biri olma yolunda ilerlerken bu gelişmişlik seviyesini teknoloji ve teknolojik gelişmeler için yaptığı yatırımlara borçludur. 1960'lı yıllardan günümüze teknoloji parkları, sanayi ve teknolojiyi bir araya getiren bölgeler ve araştırma merkezleri kurmuşlar ve bu alanda yatırım yapmaktan hiç vazgeçmemişlerdir [43].

Ülkenin teknoloji zemininde büyümesi ve gelişmesi en üst seviyede teknolojik imkanlara sahip olduğunu ortaya koymakla birlikte ülke güvenliği için yine teknoloji temelli tedbirlerin anti demokratik olup olmadığı bilinememekteydi. Covid – 19 virüsü ve pandemi sürecini oldukça zor atlatan ülkelerden biri olan Güney Kore'de bu kapsamda uygulanan tedbirlerden bazılarının anti demokratik olduğu iddia edilmektedir.

Anti demokratik olduğu iddia edilen tedbir, virüsle enfekte her birey hakkında, ülke genelindeki hareketleri de dâhil olmak üzere son derece ayrıntılı bilgileri halka açık şekilde sunan bir COVID-19 vaka veri tabanı oluşturulmuştu. "Corona 100m" adlı takip uygulaması hızla yaygınlaştırılmış; kredi kartı işlemleri, cep telefonu konum verileri ve CCTV görüntüleri gibi konum bilgileri bir araya getirilerek veri tabanı sürekli güncellenmiştir. Hükümet tarafından denetlenen bu veri tabanı, enfekte kişileri haritalandırmakta; yaş, cinsiyet ve uyruk gibi bilgiler sağlamaktadır. Ayrıca, enfekte kişiye atanan koda bağlı olarak, o kişinin belirli süreçlerine ilişkin ayrıntılar —teşhis konulmadan önceki dönem de dâhil— resmi web sitelerinde kamuya açık şekilde erişilebilir hale getirilmiştir [41].

Güney Kore'de Covid – 19 döneminde kullanılan bu uygulamanın teknolojik iz sürmede ulaştığı nokta hakkında fikir verirken, uygulamanın olağan hayat dönemleri için bu seviyede takip edilebilirlik teknolojik alt yapısına sahip olması da yine gizlilik ve kişisel veri alanlarında kaygıların artmasına neden olduğunu söylemek mümkündür.

Hindistan, tarih boyunca bol ve ucuz iş gücüyle ilişkilendirilmiş olsa da son yıllarda bu genel kabul değişmeye başlamış ve ülke teknoloji ve yazılım konusunda atılım yapan ülkelerden biri

konumuna gelmiştir. Ayrıca yapay zekâ ve akıllı şehir imar proje ve planları ile halihazırda devam eden teknolojik dönüşüm, ülkeye ekonomik büyüme basamaklarını tırmanma fırsatı sunmaktadır [44].

Hindistan hükümeti, Covid – 19 tedbirleri kapsamında Nisan 2020'de temaslıları belirlemek amacıyla Aarogya Setu adlı bir temas takip uygulaması kullanıma sunuldu. Bu uygulama, kullanıcıların yaşı, mesleği, sağlık bilgileri ve yurt dışı seyahat geçmişi gibi verileri temel alarak hastalanma riskini hesaplamaktadır. Mayıs ayı sonuna kadar 116 milyondan fazla kişi tarafından indirilen uygulama, Hindistan hükümeti tarafından resmi olarak zorunlu hale getirilmiştir. Ancak, Aarogya Setu'nun gizlilik kurallarına ve anayasal düzenlemelere uygun olmadığı, yasal bir çerçevesinin bulunmadığı ve kurumlar arası veri paylaşımını engellemediği gerekçeleriyle mahkemelere şikayet edilmiş olmasına rağmen, hükümet uygulamayı zorunlu tutmaya devam etmiştir [38].

Aarogya Setu, uygulamasının kişisel birçok veriye ulaşabilmesi, bu verilerin kamu kurumları dahi olsa ilgili kurum harici başka kurumlarla paylaşılması ve uygulamanın kullanımının zorunlu olması anti – demokratik bir tedbir olarak nitelendirilmesi sonucunu doğurmuştur.

6. SONUÇ

Güvenlik insanlığın ilk ihtiyaçlarından biri olarak tarih boyunca süregelmiş, gelişen ve değişen zamanlara göre tanımı, aktörleri ve unsurları da değişmiştir. İnsanlığın ilk zamanlarında korunaklı bir barınak ve uzun bir mızrak güvenlik kaygılarını yok edebiliyorken günümüzde ise neredeyse her geçen gün kavram yeni bir boyut kazanabilmektedir.

Kent güvenliği en yalın haliyle kentlilerin her şart ve koşulda kendilerini güven içinde hissetme halinin süreklilik göstermesidir. Yine kentlerin ilk ortaya çıkışındaki kent güvenliği kavramı daha somut ve daha sınırlı iken günümüzde özellikle dijitalleşmenin de etkisiyle soyut ve geniş kavramları da barındırmaya başlamıştır. Teknolojik gelişimler dijitalleşmeyi ortaya çıkarırken aynı zamanda yeni tehdit ve riskler de beraberinde ortaya çıkmıştır. Bu tehdit ve riskler fiziksel ortamdan daha ziyade sanal ortam ile ilgili olmaktadır. Devletlerin kamu hizmetlerinde gelişen teknoloji doğrultusunda dijitalleşmesi ise bürokrasinin hızlanması, kırtasiyeciliğin azalması gibi çok temel avantajlarının yanı sıra vatandaş verilerinin gizliliği ve ihlali gibi dezavantajlı durumları da beraberinde getirmiştir.

Türkiye'de bu dezavantajlı durumların önlenebilmesi için yapılan çalışmalardan ilkler arasında yer alan ve en somut olanı 2013 yılında Bakanlar Kurulu kararıyla resmi gazetede yayımlanan "Ulusal Siber Güvenlik Stratejileri ve Eylem Planı"dır. Bu eylem planı ile tüm kamu kurum ve kuruluşlarına dijital hizmetlerinin dijital güvenliğinin de sağlanması gerektiği vurgulanmış, kurum ve kuruluşları ilgilendiren eylem maddeleri açıklanmıştır. Ayrıca yine bu eylem planı doğrultusunda Siber Olaylara Müdahale Ekipleri (SOME) kurulmuştur. Bu eylem planı haricinde 2014 – 2018 yıllarını kapsayan 10. Kalkınma Planında da siber güvenlik konusu vurgulanmış ve siber suçlarla mücadele için Emniyet Genel Müdürlüğü bünyesinde özel bir birim kurulduğu belirtilmiştir. İlk eylem planının süresinin sona ermesi ve sonraki eylem planlarının hazırlanması görevinin Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiş olması nedeniyle 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ilgili bakanlıkça hazırlanmıştır. Bakanlıkça hazırlanan ikinci eylem planında yine kurum ve kuruluşları ilgilendiren eylem maddeleri sıralanmıştır.

2019 – 2023 yıllarını kapsayan 11. Kalkınma Planı'nda ise dijitalleşmenin artırılması, kamu ve tüm sektörlerde etkin bir şekilde kullanımının yaygınlaştırılması, siber güvenlik alanında hem kamu hem de toplumun tüm kesimi için bilinçlendirici ve geliştirici politikalar üretileceği vurgulanmıştır. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda ilk iki eylem

planına ek olarak ülke ekonomisinin geliştirilmesinde ve korunmasında siber güvenliğin önemine değinilmiş ve ulusal düzeydeki bütün kurum ve kuruluşların koordineli bir şekilde çalışmaları gerektiği vurgulanmıştır. Dördüncü eylem planı olan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda (2024-2028) ise diğer eylem planlarında belirtilen hususlara ek olarak, insan odaklı siber güvenlik yaklaşımı ve siber alanda yapılan çalışmaların uluslararası alanda örnek teşkil etmesi hedeflenmiştir. Yine 2024 – 2028 yıllarını kapsayan 12. Kalkınma Planı'nda önceki kalkınma planlarından farklı olarak dijital devlet alt başlığı oluşturulmuş, bu başlık altında amaç ve hedefler belirlenmiş ve dijitalleşme ve siber güvenlik konularına daha çok vurgu yapıldığı görülmektedir.

Türkiye'de dijitalleşme ve güvenlik ile ilgili yapılan çalışmalar Kalkınma ve Eylem Planları ile sınırlı değildir. Özellikle 2018 yılında Türkiye'de Cumhurbaşkanlığı Hükümet Sistemine geçilmesiyle birlikte merkezi idare yeniden şekillenmiştir. Bu geçişle birlikte Cumhurbaşkanlığına bağlı ofisler oluşturulmuş, bakanlıkların görev ve yetki alanları yeniden mevzuatla düzenlenmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Sanayi ve Teknoloji Bakanlığı ve Ulaştırma ve Altyapı Bakanlığı ve bu bakanlıklara bağlı ve ilgili olan kamu kurum ve kuruluşlarına dijitalleşme, dijitalleşme ve güvenlik, teknoloji gelişimi ve siber güvenlik konularında önemli görev ve sorumluluklar yüklenmiştir. İlk olarak Cumhurbaşkanlığına bağlı, özel bütçeli, kamu tüzel kişiliğini haiz, idarî ve malî özerkliğe sahip Dijital Dönüşüm Ofisine; kamunun dijital dönüşümüne öncülük etmek ve siber güvenliği artırıcı projeler geliştirmek gibi önemli görevler verilmiştir. Ofis, Sanayi ve Teknoloji Bakanlığı iş birliğinde ve ilgili tüm paydaşların katılımıyla Türkiye'nin ilk yapay zekâ belgesinin (Ulusal Yapay Zekâ Stratejisi 2021-2025) hazırlanmasına öncülük etmiştir. 2025 yılı Mart ayında ise ofis kapatılarak bazı görev ve yetkileri Cumhurbaşkanlığına bağlı, kamu tüzel kişiliğine haiz ve özel bütçeli olarak kurulan Siber Güvenlik Başkanlığı'na devredilmiştir. Siber Güvenlik Başkanlığı kurulduktan iki ay sonra 7545 Sayılı Siber Güvenlik Kanunu çıkartılmış ve siber güvenlik alanında yapılacak olan tüm çalışmalar için en üst kurum olarak nitelendirilebilecek görev, yetki ve sorumluluklar verilmiştir. İkinci olarak, Sanayi ve Teknoloji Bakanlığı ve ilgili kuruluşlarına "siber güvenlik alanında yerli ve milli ürünlerin üretilmesine, yerli ve milli ürünlerin ülke genelinde kullanımının yaygınlaştırılmasına, veri merkezi ve veri işleme altyapısının güçlendirilmesine ve siber güvenlik ekosisteminin geliştirilmesine katkı sağlama" gibi kritik bir görev verilmiştir. Üçüncü olarak, Ulaştırma ve Altyapı Bakanlığı ve ilgili kuruluşlarının "siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirleme, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirleme, eylem planlarını hazırlama, ilgili faaliyetlerin koordinasyonunu sağlama, kritik altyapılar ile ait oldukları kurumları ve konumları belirleme, gerekli müdahale merkezlerini kurma, kurdurma ve denetleme görevleri verilmiştir. Bu görevlerin yanı sıra siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmalarını yürütme, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlama" görevleri de bulunmaktadır. Ayrıca Bakanlığın ilgili kuruluşlarından olan Bilgi Teknolojileri ve İletişim Kurumu bünyesinde siber saldırı ve tehditlere karşı Ulusal Siber Olaylara Müdahale Merkezi (USOM) faaliyetlerine devam etmektedir.

Gelişen teknolojinin ve dijitalleşmenin kent güvenliğine olumsuz olarak yansımalarını minimize etmek için kent güvenliğini sağlamakla görevli baş aktörlerden biri olan Emniyet Genel Müdürlüğü'de yapmış olduğu geleneksel polisiye tedbirlere ek olarak, teknolojik gelişmeler ve dijitalleşmenin beraberinde getirmiş olduğu siber güvenlik ihtiyacını da gidermeye çalışmakla birlikte suçların azaltılması ve suçluların yakalanması için gelişen bu teknolojileri aktif olarak kullanmaktadır. Örneğin proaktif polislik modeliyle teknolojik veri temelli tahminlerle suç kalıpları, suç bölgeleri ve bölgede yaşayan toplumun analiz edilerek suç gerçeklemeden önce önlenmesi amaçlanmaktadır. Yine, sıcak nokta polislik modeliyle

teknolojik veri ve analizlere dayalı olarak suç oranlarının yüksek olduğu bölgelerde ekstra tedbirler alınabilmektedir. Yüz tanıma teknolojisi ve Coğrafi Suç Haritalama modelleri tamamen teknolojik temellidir. Bu modeller sayesinde yine kent güvenliğinin sağlanmasına katkı sunulmakta ve suçluların çok daha kısa sürelerde yakalanması mümkün olabilmektedir.
Teknolojinin gelişimi sayesinde insan hayatını kolaylaştıran mobil uygulamalar, sosyal medya platformları ve kamunun dijitalleşmesi sürecinde kamu hizmetlerine erişim uygulamaları ortaya çıkmıştır. Bu uygulama ve platformları kullanabilmek için bireyin kişisel verilerini, konum bilgilerini de içeren bazı bilgiler uygulama üreticisi ile paylaşılmaktadır. Paylaşılan bu bilgi ve verilerin uygulama üreticisi tarafından gizlilikle korunması gerekirken Covid – 19 virüsünün ortaya çıkması ve pandemi sürecinin ilan edilmesiyle birlikte pandemi mücadelesi kapsamında Amerika Birleşik Devletleri, Çin, İsrail, Güney Kore ve Hindistan gibi ülkelerde hükümetlerin mobil uygulamalar ve sosyal medya platformlarının uygulama üreticisinden vatandaşlarının kişisel verilerini temin ettikleri veya satın aldıkları ya da kamunun ürettiği mobil uygulamalardaki verileri pandemi tedbirleri kapsamında kullandıkları ve hatta mücadele dönemine özel devletlerin birey takibi yapabilmesi için mobil uygulama geliştirip kullanımını zorunlu tuttukları dönemler yaşanmış bu da beraberinde kişisel haklar, veri ihlali başta olmak üzere bazı hukuki tartışmaları doğurmuştur.

Teknoloji gelişimi devam ettiği süre boyunca hem bireyler hem devletler dijitalleşmeye devam edecek bu durumda bazı risk ve tehditleri beraberinde getirecektir. Dijital çağda kent güvenliğinin sağlanabilmesi, kentlinin gelişen teknolojinin risk ve tehditlerinden korunabilmesi bütünüyle mümkün olmasa bile artırılan siber güvenlik tedbirleri, teknolojik gelişmelerin kamu tarafından takibi ve kullanımı, vatandaşlara yönelik eğitim ve bilinçlendirme faaliyetleri ile minimize edilmesi mümkün olabilecektir.

7. KAYNAKLAR

[1] Göksu, T. (2004). Türkiye'de kentleşme ve güvenlik hizmetleri, demografik bir yaklaşım. Uluslararası İç Güvenlik Yönetimi Konferansı (s. 1-19). Ankara, Türkiye.

[2] Kaypak, Ş. (2016). ''Kentsel Bir Sorun Olarak Kentsel Güvenlik'', Akademik Sosyal Araştırmalar Dergisi, (33), 33-50.

[3] Ertan, A. K. (2014). Kent ve Kentli Hakları. (1. Baskı). TODAİE Yayınları.

[4] Özer, A. M. (2013). ''İmajını Yöneten Örgütler Daha mı Başarılı Oluyor?'', TÜHİS İş Hukuku ve İktisat Dergisi, (3) 24.

[5] Çifçi, O. (2024). "Güvenlik Paradigmasının Dönüşümü ve 21.Yüzyılda Uluslararası Güvenliğin Yeni Gündemi", Liberal Düşünce Dergisi(113), 143-170.

[6] Yıldırım, A. (2024). "Türkiye'nin Siber Güvenlik Politikasının Eylem Planları Üzerinden Analizi", Organizasyon Ve Yönetim Bilimleri Dergisi, 16 (1), 23-47.

[7] Uslu, H. (2023). "Dijital Dönüşüm ve Kamu Hizmetleri Yönetimde Yenilikçi Yaklaşımlar ve Zorluklar", Uluslararası Politik Araştırmalar Dergisi, 9 (3), 15-31.

[8] Ölmez, M. (2021). "Türkiye'de Kamu Politikalarında Dijital Dönüşüm ve E-Ticaret: Bir Model Önerisi", Kamu Yönetimi ve Teknoloji Dergisi, 3 (1), 9-33.

[9] Akmeşe, S. (2020). "Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü", Denetişim(20), 108-119.

[10] Gürbüz, A. (2019). "Vatandaş Odaklı Kamu Hizmet Yönetimi. Yeni Kamu İşletmeciliğine Eleştirel Bir Bakış", Erzincan Binali Yıldırım Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1 (2), 34-41.

[11] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2025). Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Hakkında. https://cbddo.gov.tr/, 11 Haziran 2025 tarihinde alınmıştır.

[12] Uysal, Y. Kurban, S. ve Çığman, Z. M. (2023). "Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Ve E-Yönetişim", Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 211-31.

[13] Resmi Gazete. (2025). Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılmasına Dair Cumhurbaşkanlığı Kararnamesi. https://www.resmigazete.gov.tr/eskiler/2025/03/20250328-11.pdf, 12 Ağustos 2025 tarihinde alınmıştır.

[14] Kavut, S. (2024). "Toplumların Dijital Dönüşüm Aracı Olarak Yapay Zekâ Çalışmaları: Türkiye'nin ve Türk Devletleri Teşkilatının Yapay Zekâ Kullanımı Üzerine Bir Analiz", Erciyes İletişim Dergisi, 11 (1), 325-344.

[15] Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2025). Ulusal Yapay Zeka Stratejisi. https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf, 18 Nisan2025 tarihinde alınmıştır.

[16] Resmi Gazete. (2025). Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi. https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf, 12 Ağustos 2025 tarihinde alınmıştır.

[17] Resmi Gazete. (2025). Siber Güvenlik Kanunu. https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, 15 Ağustos 2025 tarihinde alınmıştır.

[18] Resmi Gazete. (2025). Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi. https://www.resmigazete.gov.tr/eskiler/2018/07/20180710.htm, 18 Ağustos 2025 tarihinde alınmıştır.

[19] Sanayi ve Teknoloji Bakanlığı. (2025). Faaliyet Raporları. https://www.sanayi.gov.tr/assets/pdf/plan-program/STB-2023YiliFaaliyetRaporuV4.pdf, 12 Temmuz 2025 tarihinde alınmıştır.

[20] Sanayi ve Teknoloji Bakanlığı. (2025). Performans Programları. https://www.sanayi.gov.tr/assets/pdf/plan-program/2024YiliPerformansProgrami.pdf, 12 Temmuz 2025 tarihinde alınmıştır.

[21] Türkiye Bilimsel ve Teknolojik Araştırma Kurumu. (2025). Kurumsal Hakkında. https://bilgem.tubitak.gov.tr/kurumsal/, 2 Ağustos 2025 tarihinde alınmıştır.

[22] Ulaştırma ve Altyapı Bakanlığı. (2025). Eylem Planları. https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf, 7 Ağustos 2025 tarihinde alınmıştır.

[23] Bilgi Teknolojileri ve İletişim Kurumu. (2025). Bilgi Teknolojileri ve İletişim Kurumu Hakkında. https://www.btk.gov.tr/kurulus, 19 Haziran 2025 tarihinde alınmıştır.

[24] Mevzuat Bilgi Sistemi. (2025). Elektronik Haberleşme Kanunu. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5, 30 Eylül 2025 tarihinde alınmıştır.

[25] Ulusal Siber Olaylara Müdahale Merkezi. (2025). Kurumsal Hakkımızda. https://www.usom.gov.tr/hakkimizda, 13 Ağustos 2025 tarihinde alınmıştır.

[26] Gündoğdu, S. (2023). "Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik Ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM)", Fırat Üniversitesi Sosyal Bilimler Dergisi, 33(3), 1325-1337.

[27] Türkiye Büyük Millet Meclisi. (2025). Dijital Mecralar Komisyonu. https://www.tbmm.gov.tr/ihtisas-komisyonlari/Icerik/ihtisas-komisyonlari-dijital-mecralar-komisyonu-hakkinda/dijital-mecralar-komisyonu/f72877d1-b4c7-037b-e050-007f01005610, 12 Ağustos 2025 tarihinde alınmıştır.

[28] Resmi Gazete. (2025). Dijital Mecralar Komisyonu Kurulması İle Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun. https://www.resmigazete.gov.tr/eskiler/2020/07/20200728-15.htm, 19 Temmuz 2025 tarihinde alınmıştır.

[29] Strateji ve Bütçe Başkanlığı. (2025). Onuncu Kalkınma Planı. https://www.sbb.gov.tr/wp-content/uploads/2022/08/Onuncu_Kalkinma_Plani-2014-2018.pdf, 11 Nisan 2025 tarihinde alınmıştır.

[30] Strateji ve Bütçe Başkanlığı. (2025). Projeler Hakkında. https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=363&LangID=1, 11 Nisan 2025 tarihinde alınmıştır.

[31] Çakır, H. Uzun, A. S. (2021). "Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi", Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7(2), 353-379.

[32] Emniyet Genel Müdürlüğü. (2025). Emniyet Genel Müdürlüğü Performans Programları. https://www.egm.gov.tr/kurumlar/egm.gov.tr/IcSite/strateji/MaliDurum/2025_Performans_Programi.pdf, 3 Eylül 2025 tarihinde alınmıştır.

[33] Polis Akademisi Başkanlığı (2022). Önleyici Polislik Tedbirleri, Rapor, Ankara: Polis Akademisi Yayınları.

[34] Akbaş, M. (2023). "İç Güvenlik İstihbaratı ve Polis İstihbaratı Arasındaki İlişki: Türk Polis Teşkilatı/İstihbarat Başkanlığı Örneği", Güvenlik Çalışmaları Dergisi, 25(2), 149-164.

[35] İçişleri Bakanlığı. (2025). Analiz Sistemleri Narkotik Ağı (ASENA). https://www.icisleri.gov.tr/analiz-sistemleri-narkotik-agi-asena-yazilimi-sayesinde-15-yilda-6-bin-636-mudahale-edildi, 30 Eylül 2025 tarihinde alınmıştır.

[36] Emniyet Genel Müdürlüğü. (2025). Toplum Destekli Polislik. https://www.egm.gov.tr/toplum-destekli-polislik, 30 Eylül 2025 tarihinde alınmıştır.

[37] Manioğlu, O. (2023). "Kısa Amerika Tarihi Işığında Amerikan Siyasi Sistemine Bakış", UPA Strategic Affairs 4 (1), 108-28.

[38] Nasırova, S. (2024). Dijital Gözetim Sisteminde Devlet Egemenliği, Doktora Tezi, Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara.

[39] Timurtaş, M. E. (2018). "Çin Halk Cumhuriyetinin Ekonomik Ve Siyasi Geçmişinin Bugünkü Gelişim Sürecindeki Rolü", Sakarya Üniversitesi İktisat Dergisi, 7(1), 52-69.

[40] Mozur, P., Zhong, R., Krolik, A. (2021). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html, 5 Mayıs 2025 tarihinde alınmıştır.

[41] Tan, S. (2023). Türkiye'de Verileştirme, Veri Adaleti Ve Sivil Toplum Kuruluşları, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

[42] Saatçioğlu, C. (2005). "Ulusal Yenilik Sistemi Çerçevesinde Uygulanan Bilim Ve Teknoloji Politikaları: İsrail, AB, Türkiye Örneği", Sosyal Bilimler Dergisi, 5 (1), 179-198.

[43] Kozlu, C. (1994). Türkiye Mucizesi İçin Vizyon Arayışları ve Asya Modelleri (6. Baskı), İstanbul: İş Bankası Yayınları.

[44] Angın, M., Doğmazer, O. (2023). "Hindistan'ın Yapay Zekâ Gelişimi Üzerine Bir İnceleme", Mevzu – Sosyal Bilimler Dergisi 9 (1), 323-349.