



DİJİTAL ÇAĞDA DEVLETİN ROLÜ VE SINIRLARI: MODERN TEKNOLOJİLERLE YENİDEN TANIMLANAN GÜVENLİK VE YÖNETİŞİM UNSURLARI ÜZERİNDEN BİR İNCELEME

Alp Cenk ARSLAN¹

Öz

Dijital dünyada yapay zekâ (YZ), büyük veri analitiği ve siber güvenlik, devletin geleneksel işlevlerini ve güvenlik kapasitesini yeniden şekillendirmektedir. Bu makale, bu teknolojilerin gözetim, tehdit tespiti ve risk yönetimi gibi alanlardaki potansiyelini ve bu süreçte ortaya çıkan etik, mahremiyet ve veri güvenliği sorunlarını ele almaktadır. Modern teknolojiler, devletlere daha etkin güvenlik önlemleri ve yenilikçi kamu hizmetleri sağlama imkânı sunarken, bireysel hakların ihlali, veri manipülasyonu ve önyargılı algoritmalar gibi sınamalara yol açmaktadır. Çalışma, bu dönüşümün devletin egemenliği, bireysel mahremiyet ve etik yönetim üzerindeki etkilerini tartışarak, dijital çağın karmaşıklıkları karşısında devletin rolünün yeniden tanımlanması gerektiğini vurgulamaktadır.

Anahtar Kelimeler: Yapay Zekâ ve Devlet, Güvenlik Yönetimi, Güvenlik Stratejileri, Kamu Güvenliği, Dijital Devlet, Yönetişim

JEL Sınıflandırması: F52, D73, O33

THE ROLE AND LIMITS OF THE STATE IN THE DIGITAL AGE: AN ANALYSIS OF SECURITY AND GOVERNANCE ELEMENTS REDEFINED BY MODERN TECHNOLOGIES

Abstract

In the digital world, artificial intelligence (AI), big data analytics, and cybersecurity are reshaping the traditional functions and security capacities of the state. This article examines the potential of these technologies in areas such as surveillance, threat detection, and risk management, while addressing the ethical, privacy, and data security challenges they bring. Modern technologies offer states the opportunity to implement more effective security measures and deliver innovative public services. However, they also raise concerns about violations of individual rights, data manipulation, and biased algorithms. Furthermore, while digitization accelerates decision-making processes, it creates challenges for governance principles such as transparency and accountability. This study explores the impact of this transformation on state sovereignty, individual privacy, and ethical governance, emphasizing the need to redefine the state's role in light of the complexities brought about by the digital age.

Keywords: Artificial Intelligence and State, Security Management, Security Strategies, Public Security, Digital State, Governance

JEL Classification: F52, D73, O33

¹ Dr. Öğr. Üyesi, Polis Akademisi, alpcentkarслан@gmail.com, ORCID: 0000-0002-5526-2089

1. Giriş

Devlet olgusunun yönetim ve güvenlik unsurları üzerinden yürütülen bir tartışmanın odak noktası modern teknolojilerin devletin güvenlik ve yönetim alanlarındaki rolünü yeniden tanımlama mekanizmaları ve bu yeniden tanımlanan mekanizmalar bağlamında ortaya çıkan yeni sınırlılıklardır. Bu sorunsal, klasik devlet teorilerinden hareketle ele alınmalıdır; Max Weber'in bürokrasi teorisi, devletin rasyonel ve merkeziyetçi yapısını vurgularırken, dijital çağda bu yapı, e-devlet ve yönetim paradigmatlarıyla (örneğin, dijital yönetim) esneyerek dönüşüme uğramaktadır. Michel Foucault'un 'gözetim toplumu' kavramı, yapay zekâ ve büyük veri analitiğinin güvenlik mekanizmalarını nasıl güçlendirdiğini, ancak bireysel mahremiyeti tehdit ettiğini teorik olarak açıklamaktadır. Modern yaklaşımlarda ise, dijital devlet teorisi (Çatlı, 2021), geleneksel egemenlik unsurlarını (ulus, saha, egemenlik) dijital unsurlarla (dijital ulus, veri egemenliği) yeniden yorumlayarak, devletin rolünün paradigmatik bir değişim yaşadığını savunmaktadır. Çalışmanın amacı çerçeve, makalenin odaklandığı dönüşümü, etik ve hukukî boyutlarıyla birlikte analiz etmek için temel oluşturmaktır.

Makale modern teknolojilerin devletin güvenlik ve yönetim kabiliyetlerini zenginleştirdiğini, ancak aynı zamanda devletin işlevlerinin yeniden değerlendirilmesini gerektiren yeni sınamalar ve sınırlılıklar yarattığını savunmaktadır. Bu argüman üç temel boyuta dayanmaktadır. Bunlar devletin güvenlik mekanizmalarının zenginleşmesi, yönetim şablonlarının yeniden yapılandırılması ve dijital teknolojilerin artan kullanımıyla ortaya çıkan etik ve mahremiyet içerikli sınamalardır.

Dijital çağ, teknolojik gelişmelerin hızla ilerlediği ve toplumların hayatlarını köklü şekilde etkilediği bir dönemdir. Bilgi teknolojileri, yapay zekâ, büyük veri ve nesnelerin interneti gibi yenilikçi teknolojiler, bilginin üretimi, paylaşımı ve işlenmesi süreçlerini dönüştürmüş, devletlerin güvenlik ve yönetim işlevlerini yeniden şekillendirmiştir. Dijitalleşme süreci, devletin sadece vatandaşlara hizmet sunma biçimini değil, aynı zamanda güvenlik ve yönetim mekanizmalarını da köklü şekilde dönüştürmektedir. Geleneksel devlet işlevleri, fiziksel sınırlar, bürokratik yapılar ve merkeziyetçi otoriteye dayanırken, dijitalleşme bu yapıların esnemesine yol açmış ve yeni stratejiler geliştirilmesi ihtiyacını doğurmuştur.

Dijital çağın devlet üzerindeki etkilerini anlamak için bilgi ve iletişim teknolojilerinin rolünü daha yakından incelemek gerekir. Bu teknolojiler, devlet işlevlerini şeffaf, erişilebilir ve hızlı hale getirirken, güvenlik ve mahremiyet gibi kritik alanlarda yeni sorunlar yaratmıştır. Bir örnek vermek gerekirse, yapay zekâ ve büyük veri analitiği, devletlerin güvenlik alanında tehdit algılama ve risk yönetimi süreçlerinde iyileşme sağlarken, bu teknolojilerin kötüye kullanılması, temel hak ve özgürlüklere müdahale riskini gündeme getirmiştir.

Devletin rolü, geleneksel bürokrasi teorisinde tanımlandığı üzere, egemenlik, güvenlik sağlama ve kamu hizmetleri sunumu gibi işlevlerle sınırlı bir merkezi otorite olarak görülmüştür; ancak dijital çağda bu rol, teknolojilerin etkisiyle köklü bir dönüşüm geçirmektedir (Hanna, 2018). Dijital dönüşüm, devletin görevlerini yalnızca verimlilik artışı ile sınırlı kalmayıp, vatandaş-odaklı değer yaratma süreçlerine evrilerek yeniden tanımlamakta; örneğin, hükümet-vatandaş ilişkilerinde değer ortak yaratımı, dijital platformlar aracılığıyla devletin rolünü daha katılımcı ve şeffaf hale getirmektedir (Guo ve Zhang, 2024). Tarihsel perspektiften bakıldığında, dijital dönüşüm toplumun bilgi düzenini yeniden yapılandırarak devletin egemenlik ve güvenlik görevlerini genişletmiş, yapay zeka ve büyük veri gibi araçlarla proaktif bir yönetim modeline geçişi hızlandırmıştır (Hilbert, 2020). Bu dönüşüm, aynı zamanda jeopolitik bağlamda egemenliği dijital alana taşımakta, devletlerin veri egemenliği ve siber güvenlik gibi yeni görevlerle yüzleşmesini gerektirmektedir (Timmers, 2024). Ancak, bu değişim bireysel haklar ve etik sorunlar gibi sınırlılıkları da beraberinde getirmekte, devletin rolünü dengeli bir şekilde yeniden tanımlama ihtiyacını vurgulamaktadır.

Dijitalleşme aynı zamanda yönetim pratiklerini de dönüştürmektedir. E-devlet ve dijital hizmet uygulamaları sayesinde devletler, vatandaşlarına daha hızlı ve etkin hizmet sunmakta, yönetim modelleri merkeziyetçilikten uzaklaşıp daha yatay ve esnek bir yapıya evrilmektedir. Ancak bu

durum, devletin sorumluluklarını yeniden tanımlamayı ve dijitalleşmenin getirdiği riskleri dikkate almayı zorunlu kılmaktadır. Veri güvenliği, dijital altyapıların korunması ve siber tehditlerle mücadele, dijital çağda devletin rolünü ve sorumluluklarını yeniden şekillendiren kritik unsurlar haline gelmiştir.

Dijital çağda devletin sadece fiziksel güvenliği sağlaması ve kamu hizmetleri sunması yeterli değildir; dijital dünyanın getirdiği karmaşıklıklarla başa çıkması da gerekmektedir. Devletlerin teknolojik gelişmelere ayak uydurması ve dijital dönüşüm süreçlerini etkin şekilde yönetebilmesi için stratejiler geliştirmesi şarttır. Dijitalleşme süreçleri, devletin meşruiyeti, sorumlulukları ve sınırları üzerindeki etkileriyle birlikte ele alınmalı, bu dönüşümün devletin rolünü nasıl yeniden tanımladığını kavramak açısından kritik öneme sahip olduğu unutulmamalıdır (Ağırdil, 2025a; Ağırdil 2025b).

Dijital çağ, güvenlik ve yönetim kavramlarının hem anlamını hem de işleyişini köklü şekilde dönüştürmektedir. Devletlerin karşılaştığı tehditlerin niteliği değişmiş, yeni stratejiler geliştirilmesi gereği doğmuştur. Geleneksel güvenlik anlayışları, dijital tehditler karşısında yetersiz kalmakta; siber saldırılar, dijital casusluk ve veri ihlalleri gibi tehditler devlet güvenliğini daha karmaşık hale getirmektedir. Siber güvenlik, devletlerin dijital altyapılarını koruma ve kritik veri sistemlerini savunma kapasitesini geliştirmiştir. Ancak bu yeni güvenlik paradigması, bireylerin mahremiyetinin korunması ve dijital özgürlüklerin güvence altına alınmasını da içermektedir. Dijital çağda güvenlik sadece askeri tehditlerle sınırlı değildir; siber saldırılara karşı alınan önlemler, devletin güvenlik anlayışını genişletmiş ve daha katmanlı bir yapıya dönüştürmüştür.

Yönetim süreçleri de dijital çağda yeniden tanımlanmaktadır. Dijitalleşme, devletlerin vatandaşlarla daha hızlı ve etkin iletişim kurmasına olanak tanımış, yönetim süreçlerini daha şeffaf ve hesap verebilir hale getirmiştir. E-devlet uygulamaları, vatandaşlara daha iyi hizmet sunmanın yanı sıra yönetim süreçlerinin daha demokratik ve katılımcı olmasını sağlamaktadır. Ancak bu yeni yönetim şablonları, veri güvenliği ve etik sorumluluklar açısından yeni soruları da gündeme getirmektedir. Dijitalleşme aynı zamanda yönetim süreçlerinin daha katılımcı hale gelmesi için fırsatlar sunmaktadır. Dijital araçlar, vatandaşların yönetime daha fazla katılımını sağlamaktadır. Ancak bu katılımın sürdürülebilir olması için dijital hizmetlere erişimin yaygınlaştırılması ve dijital okuryazarlığın artırılması gerekmektedir. Dijitalleşme, daha demokratik bir yönetim modeli inşa etmek için büyük bir fırsat sunarken, bu sürecin adil ve kapsayıcı olması büyük önem taşımaktadır.

Dijital çağda devletin rolünü yeniden tanımlarken üç ana boyut önem kazanmaktadır: güvenlik mekanizmalarının zenginleşmesi, yönetim şablonlarının yeniden yapılanması ve etik ve mahremiyetle ilgili yeni sınamaların ortaya çıkması. Dijital teknolojilerin güvenlik alanında kullanımı, devletlerin tehdit algılama ve savunma stratejilerini dönüştürmüştür. Geleneksel güvenlik mekanizmaları fiziksel sınırların korunmasına dayanırken, dijitalleşme güvenliği daha karmaşık hale getirmiştir. Siber güvenlik, büyük veri analizleri ve yapay zekâ destekli gözetim sistemleri, devletlerin güvenlik kapasitelerini artırmıştır. Ancak bu yeni tehditlere karşı geliştirilen stratejiler, sürekli güncellenmeyi gerektirmektedir.

Yapay zekâ, güvenlik alanında tehditleri daha hızlı algılayabilmekte ve devletlerin savunma kapasitelerini güçlendirmektedir. Ancak bu teknolojilerin kullanımı, etik sorunları ve bireysel özgürlüklere yönelik tehditleri beraberinde getirmektedir. Devletler, güvenlik ve özgürlükler arasında denge kurma sorumluluğuyla karşı karşıya kalmıştır. Yönetim, dijitalleşmenin etkisiyle daha esnek ve şeffaf bir yapıya kavuşmuştur. E-devlet uygulamaları, kamu hizmetlerini daha erişilebilir ve kullanıcı dostu hale getirirken, yönetim süreçlerinin daha veriye dayalı ve sonuç odaklı olmasını sağlamaktadır. Bu yeni yönetim modelleri, devletlerin vatandaşlarına daha iyi hizmet sunmasını sağlarken, aynı zamanda hesap verebilirliği artırmaktadır.

Büyük veri analizleri ve yapay zekâ tabanlı karar mekanizmaları, kamu politikalarının daha etkili şekilde şekillendirilmesini sağlamaktadır. Ancak bu süreç, devletin şeffaflık ve hesap verebilirlik

konusundaki sorumluluklarını da artırmaktadır. Dijitalleşme, devletlerin gözetim yeteneklerini artırmıştır. Ancak bu gözetim yetenekleri, bireylerin mahremiyet haklarına müdahale riskini beraberinde getirmektedir. Devletler, dijital teknolojileri kullanırken etik kurallara uygun hareket etmek zorundadır. Yapay zekâ tabanlı sistemlerin kamusal alanda kullanımı, şeffaflık ve hesap verebilirlik sorunlarını da beraberinde getirmektedir. Dijital çağda devletin güvenlik ve yönetim kapasiteleri zenginleşirken, bu süreçte etik ve mahremiyet sınamaları önemli bir yer tutmaktadır.

Dijital çağın devletin işlevleri üzerindeki etkilerini ele alan bu makale, dijitalleşmenin güvenlik ve yönetim alanlarındaki dönüşümlere odaklanarak, literatüre önemli katkılar sunmayı amaçlamaktadır. Öncelikle, dijitalleşmenin devletin yönetim ve güvenlik işlevlerini nasıl yeniden tanımladığını teorik bir çerçevede inceleyerek bu alanlarda yapılmış önceki çalışmalara yenilikçi bir perspektif kazandırmayı hedeflemektedir. Ayrıca, yapay zekâ, büyük veri analitiği ve siber güvenlik gibi modern teknolojilerin devletin karar alma mekanizmaları ve güvenlik politikaları üzerindeki etkilerini değerlendirmekte, bu teknolojilerin bireysel haklar ve etik yönetim bağlamında doğurduğu riskleri analiz etmektedir.

Makale üç temel amacı gerçekleştirmeyi hedeflemektedir: (1) dijitalleşmenin devlet işlevlerini dönüştürme biçimlerini detaylı bir şekilde ortaya koymak, (2) modern teknolojilerin güvenlik ve yönetim süreçlerine sağladığı fırsatlar ile beraberinde getirdiği sınırlılıkları analiz etmek ve (3) bu dönüşümün bireysel özgürlükler ve toplumsal haklar üzerindeki etkilerini tartışarak, devletin rolü ve sorumluluklarına dair yeniden tanımlama ihtiyacını vurgulamak.

Makalenin içeriği şu şekilde yapılandırılmıştır: İlk bölümde, dijitalleşmenin devletin güvenlik ve yönetim işlevlerine etkisi teorik bir çerçevede ele alınacaktır. İkinci bölümde, yapay zekâ ve büyük veri analitiği gibi teknolojilerin yönetim süreçlerindeki yeni şablonlar oluşturması tartışılacaktır. Üçüncü bölümde ise hukukilik ve mahremiyet konusunda devletlerin karşılaştığı sınamalar ele alınacaktır.

2. Devletin Güvenlik Mekanizmalarının Zenginleşmesi

Dijital çağ, devletlerin güvenlik mekanizmalarını köklü bir şekilde değiştirmiş, yeni teknolojilerin sunduğu imkanlarla bu mekanizmaları daha kapsamlı ve etkili hale getirmiştir. Yapay zekâ, biyometri ve gelişmiş gözetim sistemleri gibi modern teknolojiler, güvenlik alanında devrim niteliğinde yenilikler getirmiş, tehdit tespiti ve yanıt verme süreçlerinden sınır kontrollerine ve siber güvenlik önlemlerine kadar birçok alanda zenginleşme sağlamıştır. Dijital çağda güvenlik mekanizmalarının zenginleşmesi üç ana noktada toplanmaktadır. Bunlar gelişmiş tehdit tespiti ve buna yanıt verme, güçlendirilmiş sınır kontrolü ve göç yönetimi ve güçlendirilmiş siber güvenlik önlemleridir (Chaar-López, 2019). Gelişmiş tehdit tespiti, yapay zekâ ve büyük veri analitiğiyle desteklenen sistemler aracılığıyla, potansiyel güvenlik risklerinin proaktif olarak belirlenmesini ve hızlı müdahale süreçlerini mümkün kılmaktadır; örneğin, makine öğrenimi algoritmaları, geçmiş verilerden öğrenerek tehdit modellerini öngörebilmekte ve güvenlik birimlerine anlık uyarılar sağlayabilmektedir (Andrejevic ve Gates, 2014). Güçlendirilmiş sınır kontrolü ve göç yönetimi, biyometrik teknolojiler ve dijital veri tabanlarının kullanımıyla, sınır geçişlerinde kimlik doğrulama süreçlerini daha güvenli ve verimli hale getirmektedir; bu sistemler, sahte kimlik kullanımını azaltarak yasadışı göçle mücadelede devletlere önemli avantajlar sunmaktadır (Gelb ve Clark, 2013). Güçlendirilmiş siber güvenlik önlemleri ise, kritik altyapıların korunması ve siber tehditlere karşı savunma kapasitesinin artırılması için hayati öneme sahiptir; yapay zekâ tabanlı siber güvenlik sistemleri, anormal ağ aktivitelerini tespit ederek saldırıların erken önlenmesini sağlamaktadır (Sarker, 2021). Bu üç alan, dijital teknolojilerin devletlerin güvenlik kapasitelerini nasıl dönüştürdüğünü ve aynı zamanda yeni etik ve mahremiyet sınamalarını ortaya çıkardığını göstermektedir.

Yapay zekâ, büyük veri ve makine öğrenimi gibi teknolojiler, devletlerin tehdit tespiti ve buna yanıt verme kapasitesini büyük ölçüde artırmıştır. Geleneksel güvenlik yöntemleri genellikle reaktif bir yapıya sahipken, modern teknolojiler proaktif bir yaklaşımı mümkün kılmakta, devletlerin

potansiyel tehditleri önceden tespit etmesine ve hızla müdahale etmesine olanak tanımaktadır. Özellikle büyük veri analizleri sayesinde devletler, güvenlik tehditlerini daha geniş bir perspektiften ele alabilmekte ve gelecekteki tehditleri daha hızlı ve doğru bir şekilde öngörebilmektedir (Andrejevic ve Gates, 2014).

Güvenlik yönetimi, dijital çağda devletlerin karşılaştığı yeni tehditlere yanıt verme kapasitesini güçlendirmek için kritik bir unsur haline gelmiştir. Yapay zekâ ve büyük veri analitiği, güvenlik yönetiminde proaktif yaklaşımları desteklerken, devletlerin tehdit algılama, risk analizi ve kriz müdahale süreçlerini daha etkin hale getirmektedir (Wiranata, 2024). Ancak, bu süreçte veri güvenliği ve bireysel hakların korunması gibi etik sorunlar, güvenlik yönetiminin sürdürülebilirliğini zorlaştırmaktadır.

Yapay zekâ destekli güvenlik sistemleri, büyük veri ile entegre şekilde çalışarak, devletlere tehditleri daha hızlı ve daha doğru bir şekilde tespit etme imkânı sunmaktadır. Yapay zekâ ile donatılmış gözetim sistemleri, potansiyel terörist faaliyetleri ya da toplumsal huzursuzlukları önceden belirleyebilmekte ve ilgili güvenlik birimlerine uyarılar gönderebilmektedir. Bu sistemler, insan gözetiminin yetersiz kaldığı yerlerde devreye girerek, güvenlik açıklarını minimize eder. Ayrıca, makine öğrenimi algoritmaları, geçmişteki güvenlik olaylarını analiz ederek benzer tehditlerin gelecekte nasıl ortaya çıkabileceği konusunda tahminlerde bulunmaktadır. Böylece devletler, güvenlik politikalarını daha stratejik bir şekilde planlamakta ve potansiyel tehditlere karşı daha hazırlıklı hale gelmektedir (Lyon, 2014).

Biyometrik teknolojiler, güvenlik mekanizmalarını daha kişiselleştirilmiş ve kesin hale getiren bir diğer önemli gelişmedir. Parmak izi, yüz tanıma, iris taraması gibi biyometrik yöntemler, güvenlik tehditlerinin tespitinde ve bireylerin kimlik doğrulamasında yaygın olarak kullanılmaktadır. Özellikle havaalanları, sınır kapıları ve yüksek güvenlik gerektiren alanlarda biyometrik sistemler, potansiyel tehditleri daha hızlı ve güvenilir bir şekilde belirlemek için kullanılır. Gözetim sistemleri de benzer şekilde gelişmiş teknolojilerle donatılmış olup, sürekli izleme, davranış analizi ve riskli durumların tespitinde önemli noktadadır. Bu teknolojiler, insan hatasını minimize ederek tehditlere karşı daha etkili ve zamanında müdahaleyi mümkün kılar (Jain vd., 2004). Dijital çağda güvenlik stratejileri, yalnızca fiziksel tehditlerle sınırlı kalmayıp, siber güvenlik, veri koruma ve bireysel mahremiyet gibi alanları da kapsayacak şekilde genişlemiştir. Devletler, güvenlik stratejilerini yapay zekâ destekli analizler ve biyometrik teknolojilerle güçlendirerek hem ulusal hem de uluslararası düzeyde daha esnek ve dinamik bir savunma yaklaşımı benimsemektedir. Bu stratejiler, teknolojik yeniliklerin sunduğu fırsatları en üst düzeye çıkarırken, bireysel özgürlüklerin korunması gerekliliğini de gündeme getirmiştir.

Dijital teknolojiler, devletlerin sınır güvenliği ve göç yönetimi alanında da önemli ilerlemeler kaydetmesine olanak tanımıştır. Sınır kontrollerinde kullanılan biyometrik sistemler, yapay zekâ destekli gözetim teknolojileri ve dijital veri tabanları, sınır geçişlerini daha güvenli ve kontrollü hale getirmiştir. Bu teknolojiler, devletlerin sınırlarında daha sıkı denetim yapmalarına, yasadışı göçü engellemelerine ve ulusal güvenliği sağlamalarına yardımcı olmaktadır (Broeders ve Dijstelbloem, 2015).

Biyometrik veriler, sınır kontrollerinde kimlik doğrulama sürecini daha hızlı ve güvenilir hale getirmektedir. Yüz tanıma, parmak izi taraması ve iris tarama teknolojileri, sınır geçişlerinde sahte kimlik kullanımı ve insan kaçakçılığı gibi tehditlerin önlenmesine yardımcı olmaktadır. Bu sistemler, geleneksel kimlik doğrulama yöntemlerine göre çok daha güvenli olmakla birlikte kimlik sahtekarlığına karşı daha dirençli bir yapıdadır (Gelb ve Clark, 2013). Sınır güvenliğinde kullanılan yapay zekâ destekli gözetim sistemleri, sınır bölgelerindeki hareketliliği sürekli izlemekte ve potansiyel tehditleri analiz etmektedir. Bu sistemler, olağandışı hareketleri tespit etmekte ve güvenlik birimlerine uyarılar göndermektedir. Sınır boyunca yerleştirilen kamera sistemleri, insan davranışlarını analiz ederek yasadışı giriş teşebbüslerini önceden tespit etmektedir. Ayrıca, insansız hava araçları ve sensörler gibi teknolojiler de sınır güvenliğinde yaygın olarak kullanılmakta ve devletlere daha geniş bir gözetim alanı sunmaktadır (Aas, 2013).

Göç yönetiminde dijital veri tabanları ve uluslararası bilgi paylaşımı, yasadışı göçle mücadelede hayati bir noktaya evrilmiştir. Devletler, biyometrik veriler ve dijital kimlik doğrulama sistemleri sayesinde göçmenlerin kimliklerini daha hızlı ve doğru bir şekilde tespit etmektedir (McAuliffe vd., 2021). Ayrıca, dijital veri tabanları aracılığıyla uluslararası güvenlik birimleri arasında bilgi paylaşımı yapılması, uluslararası suç örgütleri ve insan kaçakçılığıyla mücadelede önemli avantajlar sağlamaktadır (Grabosky, 2007).

Siber güvenlik, dijital sistemlerin, ağların ve verilerin yetkisiz erişim, siber saldırılar ve veri ihlalleri gibi tehditlere karşı korunmasını amaçlayan teknolojiler, süreçler ve uygulamalar bütünüdür. Devletlerin ulusal güvenliği ve kritik altyapılarının korunmasında merkezi bir rol oynayan siber güvenlik, yapay zekâ ve makine öğrenimi gibi teknolojilerle desteklenerek tehdit tespiti ve müdahale süreçlerini daha etkin hale getirmektedir (Chowdhury ve Gkioulos, 2021). Özellikle enerji, sağlık ve ulaşım gibi sektörlerdeki kritik altyapıların korunması, siber güvenlik stratejilerinin önemini artırmakta; ancak, bu süreçte bireysel mahremiyetin korunması ve etik sorunlar gibi sınırlılıklar da ortaya çıkmaktadır (Taddeo vd., 2019).

Siber güvenlik, dijital çağın en önemli güvenlik bileşenlerinden biri olmakla birlikte modern devletlerin ulusal güvenlik stratejilerinin merkezinde yer almaktadır. Devletler, kritik altyapılarını korumak ve siber saldırılara karşı savunma mekanizmaları geliştirmek için kapsamlı siber güvenlik önlemleri uygulamaktadır. Dijital altyapıların güvenliği, ulusal güvenlik, ekonomi ve toplumsal düzen açısından büyük önem taşımaktadır (Chowdhury ve Gkioulos, 2021). Yapay zekâ, siber güvenlik alanında tehditlerin tespit edilmesi ve saldırılara hızlı müdahale edilmesi için kullanılmaktadır. Geleneksel güvenlik sistemleri genellikle saldırılara yanıt vermede yavaş kalırken, yapay zekâ tabanlı sistemler, anormal ağ hareketlerini tespit etmekte ve olası siber saldırıları önceden belirlemektedir. Bu sistemler, makine öğrenimi algoritmaları sayesinde sürekli kendini güncelleyerek yeni saldırı türlerine karşı daha etkili koruma sağlamaktadır. Yapay zekâ tabanlı güvenlik yazılımları, siber saldırıları tespit edip anında müdahale etmekte ve daha büyük zararların önüne geçmektedir (Sarker, 2021).

Siber güvenlik önlemleri, devletlerin enerji, iletişim, ulaşım ve sağlık gibi kritik altyapılarını korumak için büyük bir öneme sahiptir. Bu altyapılara yönelik siber saldırılar, sadece ekonomik kayıplara değil, aynı zamanda ulusal güvenlik risklerine yol açmaktadır. Devletler, bu altyapıları korumak için yapay zekâ destekli izleme ve analiz sistemleri kullanarak, saldırıların erken tespit edilmesini ve etkili şekilde önlenmesini sağlamaktadır. Ayrıca, devletler siber tatbikatlar ve simülasyonlar yaparak siber güvenlik kapasitelerini sürekli geliştirmekte ve olası tehditlere karşı hazırlıklı olmaktadır (Brilingaitė vd., 2020). Siber güvenlik alanında devletler arasındaki iş birliği de giderek önem kazanmaktadır. Uluslararası siber güvenlik tehditleri, ulusal sınırları aşan bir yapıya sahip olduğundan, devletler arasındaki bilgi paylaşımı ve koordinasyon, siber saldırılara karşı daha etkili bir savunma mekanizması oluşturulmasına yardımcı olmaktadır. Uluslararası siber güvenlik anlaşmaları ve ortak operasyonlar, devletlerin siber tehditlerle mücadelede daha güçlü ve dirençli hale gelmesini sağlamaktadır (Heinl, 2014).

Dijital çağın sunduğu teknolojiler, devletlerin güvenlik mekanizmalarını daha zengin ve kapsamlı hale getirmiştir. Yapay zekâ, biyometri ve gelişmiş gözetim sistemleri gibi teknolojiler, güvenlik tehditlerine karşı daha proaktif bir yaklaşım benimsemeyi mümkün kılmakta, sınır güvenliği ve siber güvenlik gibi alanlarda önemli avantajlar sağlamaktadır. Bahsi geçen yeni güvenlik mekanizmaları sayesinde kamu güvenliği gelişme potansiyeli göstermekte, ekonomik verimlilik artmakta ve ulusal güvenlik güçlenmektedir. Yapay zekâ, biyometri ve gözetim teknolojileri, devletlerin güvenlik tehditlerine karşı daha hızlı ve etkili önlemler almasına olanak tanırken, aynı zamanda toplumsal düzenin korunmasına ve ekonomik kalkınmanın desteklenmesine katkıda bulunmaktadır (Burton ve Soare, 2019). Dolayısıyla, bahsi geçen güvenlik mekanizmalarının yararları üç temel başlık altında ele alınmalıdır. Bunlar geliştirilmiş kamu güvenliği, güçlendirilmiş ekonomik verimlilik ve tahkim edilmiş ulusal güvenliktir.

Geliştirilmiş kamu güvenliği, dijital güvenlik mekanizmalarının yararları arasında temel bir başlık olarak, kamu malları teorisi perspektifinden ele alınabilir. Bu teori, güvenlik gibi kolektif faydaların toplumun tüm üyelerine eşit şekilde sağlanması gerektiğini vurgular; dijital teknolojiler, yapay zekâ tabanlı gözetim sistemleri aracılığıyla tehditleri proaktif olarak önleyerek, kamu güvenliğini bir kamu malı olarak güçlendirmektedir (OECD, 2015). Örneğin, biyometrik sistemler suç oranlarını azaltmada etkili olurken, bu yaklaşım bireysel özgürlüklerle dengelenme durumunu ortaya çıkarmaktadır, zira aşırı gözetim toplumsal güveni zedeleyebilmektedir (Brayne ve Christin, 2020).

Güçlendirilmiş ekonomik verimlilik, bilgi güvenliği ekonomisi teorisi üzerinden açıklanabilir; bu teori, güvenlik yatırımlarının işlem maliyetlerini azaltarak ekonomik kaynakların daha verimli kullanılmasını sağladığını savunmaktadır (Anderson ve Moore, 2007). Dijital güvenlik mekanizmaları, örneğin siber güvenlik önlemleriyle kritik altyapıları koruyarak, ekonomik kayıpları minimize etmekte ve ticaret akışını hızlandırmaktadır. Öte yandan, bu verimlilik asimetrik bilgi sorunları nedeniyle piyasa başarısızlıklarına yol açabilmektedir (Gordon ve Loeb, 2002).

Tahkim edilmiş ulusal güvenlik, dijital dönüşüm ve ulusal güvenlik teorileri bağlamında tartışılabilir; bu perspektif, teknolojilerin ulusal egemenliği siber alanda genişleterek tehditlere karşı direnci artırdığını belirtmektedir. Yapay zekâ destekli sistemler, ulusal güvenlik stratejilerini güçlendirirken, jeopolitik riskleri de beraberinde getirmektedir. Platform tabanlı güvenlik modelleri, devletlerin veri egemenliğini korumasını sağlamakta, ancak uluslararası iş birliği gerektirmektedir (Chachko, 2021).

Yapay zekâ, biyometrik sistemler ve gelişmiş gözetim teknolojileri, kamu güvenliğinin sağlanmasında önemli bir rol oynamaktadır. Bu teknolojiler, suçların önlenmesi, tehditlerin tespit edilmesi ve toplumsal huzurun korunması gibi alanlarda devletlere yeni araçlar sunmaktadır. Özellikle şehirlerde güvenlik kameraları ve gözetim sistemleri, suç oranlarını azaltmada etkili olmuş, yapay zekâ tabanlı analizler ise suç eğilimlerini önceden belirleyerek kamu güvenliğini artırma potansiyeli yaratmıştır (Brayne ve Christin, 2020). Kamu güvenliği, dijital teknolojilerin devlet tarafından kullanımında temel bir hedef olarak öne çıkmaktadır. Yapay zekâ tabanlı gözetim sistemleri ve biyometrik teknolojiler, suç önleme ve toplumsal huzurun korunması gibi alanlarda devletlerin kapasitesini artırmaktadır. Ancak, kamu güvenliğini sağlama çabaları, bireylerin mahremiyet haklarına saygı gösterilmesi ve teknolojinin etik kullanımı ile dengelenmesi durumunu da doğurmaktadır.

Gelişmiş gözetim sistemleri, yoğun nüfuslu bölgelerde kamu güvenliğini sağlamada kilit bir role sahiptir. Bu sistemler, suç teşebbüslerinin erken tespit edilmesine ve hızlı müdahale edilmesine olanak tanımaktadır. Güvenlik kameraları, yüz tanıma teknolojisi ve biyometrik analizler, suçluların tespit edilmesini kolaylaştırırken, kamu alanlarındaki güvenlik risklerini azaltmaktadır. Kalabalık etkinlikler, büyük şehirler ve kritik altyapıların bulunduğu alanlarda bu teknolojilerin kullanımı, halkın güvenlik hissini artırmakta ve suç oranlarını azaltmaktadır. Yapay zekâ tabanlı sistemler, doğal afetler, terör saldırıları veya toplumsal huzursuzluklar gibi acil durumlarda hızlı kararlar alınmasını sağlamaktadır. Yapay zekâ algoritmaları, tehditlerin hızla analiz edilmesine ve en uygun müdahale stratejilerinin belirlenmesine yardımcı olmaktadır. Böylece kriz anlarında kamu güvenliğinin hızla sağlanmasına ve can kayıplarının en aza indirilmesine katkı sağlamaktadır (Khalil vd., 2008).

Modern Güvenlik Teknolojileri ve Ekonomik Verimlilik

Modern güvenlik teknolojileri, devletlerin güvenlik ve gözetim işlevlerini daha etkin bir şekilde yerine getirmesine olanak tanırken, aynı zamanda ekonomik verimliliği artırma potansiyeline de sahiptir. Teknolojilerin sunduğu hız, doğruluk ve otomasyon özellikleri, güvenlik süreçlerinde insan gücü gereksinimini azaltmakta ve maliyetleri düşürmektedir. Dolayısıyla, kaynakların daha verimli kullanılmasını sağlayarak hem kamu hem de özel sektör için ekonomik kazançlar yaratmaktadır. Yapay zekâ ve büyük veri analitiği, kamu yönetiminde karar alma süreçlerini hızlandırırken, güvenlik kaynaklarının daha etkin kullanılmasına katkı sağlamaktadır (Laufs vd., 2020). Güvenlik

personelinin hangi bölgelerde yoğunlaşması gerektiği, hangi alanlarda daha fazla yatırım yapılması gerektiği gibi stratejik kararlar, veri analizlerine dayalı olarak optimize edilmektedir. Böylece devletlerin kaynaklarını daha iyi yönetmesine olanak tanımakta ve uzun vadede ekonomik verimliliği artırmaktadır.

Biyometrik sistemler ve dijital gözetim araçları, sınır kontrollerini hızlandırarak uluslararası ticaretin akışını kolaylaştırmaktadır. Hızlı ve güvenilir kimlik doğrulama sistemleri sayesinde sınır geçişleri daha hızlı ve güvenli hale gelirken, ticaretin aksamadan devam etmesi sağlanır. Bu da ekonomik büyümeyi destekleyen bir faktör olarak öne çıkar. Limanlar, havaalanları ve gümrüklerde kullanılan teknolojiler, ticaret hacmini artırırken güvenliği de sağlamaktadır (Crampton, 2019).

Modern güvenlik teknolojileri, devletlerin ulusal güvenliği sağlamada önemli rol oynamaktadır. Yapay zekâ tabanlı tehdit tespit sistemleri, biyometrik gözetim ve siber güvenlik çözümleri, ulusal güvenliği artırmak için kullanılan en önemli araçlar haline gelmiştir. Bu teknolojiler, devletlerin sınırlarını daha etkili bir şekilde korumasına, siber saldırılara karşı daha dirençli hale gelmesine ve terörist faaliyetlere karşı daha hızlı yanıt vermesine olanak tanımaktadır (Zeadally, 2020).

Siber güvenlik önlemleri, modern devletlerin ulusal güvenlik stratejilerinde merkezi bir yer tutmaktadır. Yapay zekâ tabanlı siber güvenlik sistemleri, devletlerin kritik altyapılarını koruyarak enerji, iletişim, sağlık ve ulaşım gibi sektörlerde güvenliğin sağlanmasına katkıda bulunmaktadır. Bu altyapıların korunması, ulusal güvenliğin temel unsurlarından biri haline gelmiş olup, devletler siber saldırılara karşı daha dirençli hale gelmektedir (Taddeo vd., 2019).

Yapay zekâ destekli tehdit tespit sistemleri, terör saldırılarının önlenmesinde ve iç güvenliğin korunmasında önemli bir role sahiptir. Güvenlik güçleri, bu teknolojiler sayesinde terörist faaliyetleri önceden yakalamakta ve hızlı müdahalelerde bulunmaktadır. Büyük veri analitiği, potansiyel teröristlerin hareketlerini izlemek ve bu tehditleri daha erken aşamalarda durdurmak için kullanılmaktadır (Al-Hawawreh vd., 2021).

Güvenlik Teknolojilerinin Sınırlılıkları

Her ne kadar dijital çağın sunduğu güvenlik teknolojileri önemli avantajlar sağlasa da bu mekanizmalarla ilişkili bazı riskler ve sınırlılıklar da mevcuttur. Teknolojiye aşırı güven, iktidarın istismar potansiyeli ve bireysel özgürlükler üzerindeki olumsuz etkilemekte, bu yeni güvenlik mekanizmalarının yaratabileceği başlıca sorunlardandır. Yapay zekâ ve biyometrik sistemler gibi teknolojiler, güvenlik süreçlerinde hız ve doğruluk sağlasa da bu sistemlere aşırı güven duyulması birtakım sorunlara yol açmaktadır. Teknolojik sistemler her ne kadar büyük bir potansiyele sahip olsa da yanlış veri analizi veya yazılım hataları sonucunda güvenlik süreçlerinde hatalar meydana gelmektedir. Bu durum, hususen biyometrik sistemlerde hatalı kimlik doğrulama gibi ciddi sonuçlar doğurmaktadır (Nguyen-Duc ve Chirumamilla, 2019).

Yapay zekâ tabanlı sistemler, yanlış veri analizi veya algoritmik önyargılar nedeniyle hatalı sonuçlar üretebilmektedir. Yüz tanıma sistemleri bazen ırk veya cinsiyet gibi biyometrik özelliklere dayalı hatalar yapmaktadır. Bu tür hatalar, yanlış kişilerin suçlanmasına veya güvenlik tehditlerinin gözden kaçmasına yol açmaktadır (Singh vd., 2021). Teknolojiye aşırı güven, sistemlerin saldırılara veya teknik arızalara karşı korunamaması durumunda ciddi güvenlik riskleri doğurmaktadır. Siber saldırılar, güvenlik sistemlerini devre dışı bırakmakta ve ulusal güvenlik açıklarına neden olmaktadır. Dolayısıyla, devletlerin siber güvenlik altyapılarını sürekli güncelleme ve güçlendirme gerekliliğini doğurmaktadır (Aleem vd., 2013).

Güvenlik Teknolojilerinin Dezavantajları

Modern güvenlik teknolojileri, devletlere geniş gözetim ve denetim yetkileri sağlamaktadır. Ancak bu yetkiler, kötü niyetli kullanımlar veya iktidarın gücünü artırmak için istismar etmektedir. Çeşitli ülkelerde, güvenlik teknolojilerinin kullanımı, iktidarın muhalefeti bastırmak veya toplumu kontrol etmek için kullanılabileceği bir araç haline gelmektedir. Yapay zekâ ve gözetim teknolojileri, devletlerin vatandaşlarını sürekli izleme ve bireysel mahremiyeti ihlal etme potansiyeline sahiptir

(Lyon, 1992). Dolayısıyla, bir gözetim toplumu yaratmakta ve vatandaşların özgürlükleri üzerinde ciddi bir tehdit oluşturmaktadır. Gözetim sistemlerinin yaygınlaşması, bireylerin hareketlerinin sürekli izlenmesi ve dijital aktivitelerinin takip edilmesiyle sonuçlanmaktadır. Böylelikle, vatandaşların özel hayatlarına yönelik bir müdahale anlamına gelmekte ve kişisel mahremiyet haklarının ihlal edilmesine yol açabilmektedir. Mahremiyetin aşındırılması, toplumda güvensizlik yaratma potansiyelini doğurmakta ve vatandaşların devlete olan inancını zayıflatabilmektedir (Dyson, 2008).

Gelişmiş gözetim sistemleri, çeşitli örneklerde muhalif hareketlerin izlenmesi ve bastırılması amacıyla kullanılabilir. Sosyal medya üzerinden yapılan izleme faaliyetleri, muhalif seslerin tespit edilmesi ve susturulması için araçsallaştırılabilir (Owen, 2017). Gözetim teknolojilerinin devletler tarafından kötüye kullanılması, iktidarın siyasi muhalefeti baskı altına almasına ve vatandaşlar üzerinde sürekli bir baskı kurmasına neden olmaktadır. Bu da demokratik süreçleri zayıflatmakta ve bireysel hakların korunmasını zorlaştırmaktadır. Modern güvenlik teknolojilerinin bireysel özgürlükler üzerinde önemli etkileri olmaktadır. Güvenlik önlemlerinin artırılması, devletlerin bireylerin davranışlarını izleme ve kontrol etme kapasitesini artırmaktadır. Bu durum bireylerin hareket, düşünce ve ifade özgürlüğü gibi temel haklarını kısıtlayabilmektedir. Bu güvenlik teknolojilerinin geniş çapta kullanımı, bireyler üzerindeki devlet kontrolünü artırarak özgürlüklerin sınırlandırılmasına yol açabilmektedir (Taddeo, 2013).

Yüz tanıma teknolojileri, toplu gösteriler, protestolar veya kamusal alanlarda insanların kimliklerini hızlıca tespit etmektedir. Neticede, bireylerin protesto yapma, kamusal alanda kendilerini ifade etme gibi haklarını sınırlandırabilmektedir. Bireyler, sürekli izlendikleri bir ortamda düşüncelerini özgürce ifade etmekten kaçınmakta ve bu durum demokratik süreçlerin işleyişini olumsuz yönde etkileyebilmektedir (Balkin, 2003). Bu tür sistemler, sosyal medya platformlarında vatandaşların çevrimiçi aktivitelerini izlemek ve kişisel verilerini toplamak için kullanılabilir. Böyle bir durumda bireyler, hareket özgürlüklerinin kısıtlandığını hissetmekte ve devletin sürekli izleme altında olması nedeniyle sosyal kontrol mekanizmaları güçlenmektedir. Bu da toplumda yaygın bir korku ve güvensizlik atmosferine neden olabilmektedir (Starr vd., 2008).

Güvenlik teknolojilerinin geniş çapta uygulanması, dijital hakların korunması konusunda da önemli riskler taşımaktadır. Kişisel verilerin işlenmesi ve saklanmasıyla ilgili ciddi güvenlik açıkları ve etik sorunlar ortaya çıkmaktadır. Devletlerin bu teknolojileri kullanırken vatandaşların dijital haklarına saygı göstermesi ve bu hakları koruma altına alması kritik önem taşımaktadır. Veri ihlalleri, kişisel bilgilerin kötüye kullanılması ve vatandaşların izinsiz olarak izlenmesi gibi durumlar, bireylerin güvenliğini zedelemekte ve devletin meşruiyetini sorgulatmaktadır (Kostyuk ve Wayne, 2020).

Güvenlik teknolojilerinin geniş çapta uygulanması, dijital hakların korunması konusunda önemli riskler taşımaktadır; bu nedenle, kişisel verilerin işlenmesi ve saklanmasına ilişkin düzenlemeler kritik bir rol oynamaktadır. Türkiye’de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), bireylerin kişisel verilerinin işlenmesinde şeffaflık, hesap verebilirlik ve veri minimizasyonu ilkelerini benimseyerek, güvenlik teknolojilerinin kötüye kullanımını önlemeyi amaçlamaktadır (KVKK, 2016). Avrupa Birliği’nde ise Genel Veri Koruma Tüzüğü (GDPR), veri sahiplerine veri işleme süreçlerinde daha fazla kontrol hakkı tanıyarak, özellikle yapay zekâ ve biyometrik sistemler gibi teknolojilerin kullanımında sıkı etik ve hukuki standartlar getirmiştir (EU GDPR, 2016). Bu mevzuat, devletlerin veri ihlalleri, kişisel bilgilerin kötüye kullanılması ve izinsiz gözetim gibi riskleri en aza indirmesini sağlamaktadır. Öte yandan, teknolojinin hızlı gelişimi karşısında bu düzenlemelerin sürekli güncellenmesi gerekliliği ortaya çıkmaktadır (Hoofnagle vd., 2019). GDPR’nin biyometrik verilerin işlenmesine yönelik sıkı kuralları, devletlerin güvenlik teknolojilerini kullanırken mahremiyet haklarını koruma yükümlülüğünü artırmakta, ancak uygulama zorlukları ve uluslararası uyum sorunları bu düzenlemelerin etkinliğini sınırlandırabilmektedir.

Özetle, dijital çağın sunduğu güvenlik teknolojileri, devletlerin kamu güvenliği, ekonomik verimlilik ve ulusal güvenlik açısından önemli kazanımlar elde etmesine olanak tanımaktadır. Ancak

bu teknolojilerin aşırı kullanımı, bireysel özgürlüklerin ve mahremiyetin korunması açısından ciddi riskler doğurabilmektedir. Teknolojiye aşırı güven, iktidarın bu teknolojileri istismar etme potansiyeli ve bireysel haklar üzerindeki olumsuz etkilemekte, bu mekanizmaların dikkatli ve etik çerçevede kullanılmasını zorunlu kılmaktadır. Devletler, modern güvenlik teknolojilerini kullanırken, bireysel hak ve özgürlükleri gözetmek ve teknolojinin sınırlarını belirlemek zorundadır. Güvenlik ve özgürlükler arasındaki dengeyi sağlamak, dijital çağın getirdiği fırsatlarla birlikte ortaya çıkan bu yeni zorlukların üstesinden gelmek için hayati bir gereklilik haline gelmiştir.

3. Yönetişim Şablonlarının Yeniden Yapılandırılması

Dijital çağ, sadece güvenlik ve ekonomi alanında değil, aynı zamanda yönetim süreçlerinde de köklü değişikliklere yol açmıştır. Blokzincir teknolojisi, akıllı kontratlar ve dijital kimlikler gibi yenilikçi çözümler, devletlerin yönetim şablonlarını yeniden inşa etmekte, merkeziyetçilikten uzak, daha şeffaf, hesap verebilir ve katılımcı bir yönetim anlayışını desteklemektedir. Bu durumun analiz edilmesi için, modern teknolojilerin yönetim şablonlarını nasıl dönüştürdüğü ele alınmalıdır. Bu yönetim şablonları merkeziyetsiz karar alma süreçleri, güçlendirilmiş şeffaflık ve hesap verebilirlik ile geliştirilmiş yurttaş katılımı başlıkları altında sıralanmaktadır.

Yönetişim, devletin geleneksel otorite ve hiyerarşi temelli yönetim anlayışından farklı olarak, çok paydaşlı, şeffaf ve katılımcı bir karar alma sürecini ifade etmektedir. 1990'larda ortaya çıkan yönetim kavramı, özellikle küreselleşme ve teknolojik gelişmelerin etkisiyle, devletlerin merkeziyetçi yapılarından uzaklaşarak daha esnek ve iş birliğine dayalı modeller benimsemesini sağlamıştır (Rhodes, 1996). Geleneksel yönetimde devlet, tek yönlü bir otorite olarak hareket ederken, yönetim, sivil toplum, özel sektör ve vatandaşların karar alma süreçlerine katılımını teşvik eder. Dijital çağda, blokzincir, akıllı kontratlar ve e-devlet uygulamaları gibi teknolojiler, yönetim süreçlerini dönüştürerek devletin rolünü yeniden tanımlamaktadır. Örneğin, blokzincir tabanlı sistemler, şeffaf ve merkeziyetsiz bir yönetim modeli sunarak devletin vatandaşlarla ilişkisini daha demokratik ve hesap verebilir hale getirmektedir. Ancak, bu dönüşüm, dijital okuryazarlık ve teknolojiye erişim eşitsizlikleri gibi yeni sınamaları da beraberinde getirmektedir, bu da devletin kapsayıcı yönetim politikaları geliştirme sorumluluğunu artırmaktadır.

Blokzincir, verilerin merkezi bir otoriteye bağlı olmadan dağıtık bir ağ üzerinde güvenli, şeffaf ve değiştirilemez bir şekilde kaydedilmesini sağlayan bir teknolojidir. Bu teknoloji, işlemlerin doğruluğunu kriptografik yöntemlerle garanti altına alarak, özellikle yönetim süreçlerinde şeffaflık ve hesap verebilirlik sağlamaktadır (Nakamoto, 2008). Devletlerin kamu hizmetlerinde blokzincir kullanımı, örneğin akıllı kontratlar aracılığıyla bürokrasiyi azaltmakta ve vatandaşların devletle olan etkileşimlerini daha verimli hale getirmektedir. Ancak, blokzincirin yaygınlaşması, veri gizliliği ve teknolojik altyapı gereksinimleri gibi yeni düzenleyici ihtiyaçları da beraberinde getirmektedir (Pereira vd., 2019). Blokzincir teknolojisi, verilerin merkezi bir otoriteye bağlı olmadan depolanmasını ve doğrulanmasını mümkün kılan yapısıyla yönetim süreçlerinde merkeziyetçiliği ortadan kaldırma potansiyeline sahiptir (Pereira vd., 2019). Geleneksel yönetim sistemlerinde karar alma süreçleri genellikle hiyerarşik bir yapıya dayanırken, blokzincir gibi merkeziyetsiz teknolojiler, kararların dağıtık bir ağ üzerinde alınmasını sağlamaktadır. Bu teknolojiler, bilgiye erişimi demokratikleştirmekte ve merkezi otoritenin gücünü dengeleyerek karar alma süreçlerinin daha katılımcı ve şeffaf olmasına katkıda bulunmaktadır (Farnaghi ve Mansourian, 2020).

Örnek vermek gerekirse akıllı kontratlar, devletlerin işleyişinde bürokrasiyi azaltma potansiyeline sahiptir. Bu kontratlar, belirli şartlar sağlandığında otomatik olarak devreye girer ve insan müdahalesini en aza indirmektedir. Böylece kamu hizmetleri daha hızlı ve verimli bir şekilde yürütülmektedir. Sosyal yardım ödemelerinin otomatikleştirilmesi gibi uygulamalar, vatandaşların ihtiyaç duyduğu hizmetleri beklemeden almasını sağlamak ve kamu kaynaklarının israfını engellemektedir (Ahmadisheykhsarmast ve Sonmez, 2020).

Blokzincir teknolojisi, işlemlerin değiştirilemez ve geriye dönük izlenebilir olmasını sağladığı için şeffaflığı artırır. Bu teknoloji, kamu hizmetlerinde yapılan harcamalar, verilen sözleşmeler ve diğer yönetsel işlemlerle ilgili bilgilerin herkes tarafından izlenebilir olmasını sağlayarak, yönetim süreçlerinde hesap verebilirliği artırmaktadır. Şeffaflık, yolsuzluk ve kötü yönetim risklerini azaltır ve vatandaşların devlete olan güvenini güçlendirmektedir. Akıllı kontratlar, kamu ihalelerinde ve harcamalarda suistimalin önüne geçebilmektedir. İhale süreçlerinde kullanılan akıllı kontratlar, önceden belirlenmiş kriterlere dayalı olarak işlemleri otomatikleştirmekte ve süreci şeffaf hale getirmektedir. Böylece hem kamu kaynaklarının doğru kullanımı hem de hesap verebilirliğin artırılması açısından önemli bir avantaj ortaya çıkmaktadır (Weingärtner vd., 2021).

Dijital kimlik sistemleri de şeffaflık ve hesap verebilirlik açısından kilit bir role sahiptir. Vatandaşlar, dijital kimlikleri sayesinde devletin sunduğu hizmetlere daha kolay erişim sağlayabilirken, devletler de vatandaşların kimlik bilgilerini güvenilir bir şekilde doğrulayıp işlemleri hızlandırmaktadır. Bu, özellikle sosyal güvenlik ve sağlık hizmetleri gibi alanlarda önemli bir gelişme sağlamaktadır (Sung ve Park, 2021).

Teknoloji, vatandaşların yönetime katılımını artırma potansiyeline de sahiptir. Dijital kimlikler, yurttaşların devletle olan etkileşimlerini kolaylaştırarak, kamu karar alma süreçlerine daha fazla katılım sağlamalarına olanak tanımaktadır. E-oylama ve dijital platformlar aracılığıyla vatandaşlar, kamu politikalarının oluşturulmasında daha aktif bir rol oynamaktadır. Bu teknolojiler, halkın iradesini daha doğrudan yansıtır ve demokratik süreçlerin daha geniş bir tabana yayılmasını sağlamaktadır (Aichholzer ve Rose, 2019).

Blokzincir tabanlı oylama sistemleri, seçimlerin güvenli ve şeffaf bir şekilde yapılmasını sağlayarak, halkın yönetime olan güvenini artırma potansiyeline sahiptir. Bu sistemlerde oylar değiştirilemez bir şekilde kaydedildiği için seçim sonuçları üzerinde manipülasyon yapılması imkansız hale gelebilmektedir. Böylece seçimlerin meşruiyeti ve güvenliği de garanti altına alınmaktadır (Vladucu vd., 2023). Dijital çağın getirdiği bu yeni yönetim şablonları, devlet yönetiminde önemli avantajlar sunmaktadır. Güçlendirilmiş verimlilik ve etkinlik, geliştirilmiş kamu güveni ve zenginleştirilmiş inovasyon, modern teknolojilerin yönetim süreçlerine kazandırdığı başlıca yararlar arasındadır.

Blokzincir, akıllı kontratlar ve dijital kimlikler gibi teknolojiler, devletlerin verimliliğini artırmakta ve hizmet sunumunu hızlandırmaktadır. Merkezîyetçi yapının azalması ve süreçlerin otomatikleştirilmesi, kamu hizmetlerinde gereksiz bürokratik engellerin ortadan kalkmasına ve kaynakların daha verimli kullanılmasına olanak tanımaktadır. Akıllı kontratlar, devletlerin iş süreçlerini hızlandırarak, hizmetlerin daha kısa sürede sunulmasını sağlamaktadır. Böylece kamu hizmetlerinde maliyetler düşmekte ve verimlilik artmaktadır. Teknoloji, yönetim süreçlerinde şeffaflığı ve hesap verebilirliği artırarak, vatandaşların devlete olan güvenini güçlendirmektedir. Blokzincir tabanlı sistemler, vatandaşların devletin harcamalarını ve yönetsel süreçlerini izleyebilmesini sağlamaktadır. Bu tür şeffaflık, vatandaşların devletin kaynaklarını nasıl kullandığı konusunda daha fazla bilgi sahibi olmasına ve devlete duyulan güvenin artmasına yol açmaktadır (Grimmelikhuijsen, 2012).

Blokzincir ve dijital kimlik teknolojileri, kamu sektöründe inovasyonu teşvik eder. Bu teknolojiler, devletlerin daha yenilikçi politikalar geliştirmesine olanak tanımaktadır. Dijital kimliklerin kullanılması, vatandaşların sağlık hizmetlerine daha hızlı erişimini sağlayabilmektedir. Ayrıca, blokzincir tabanlı projeler, devletlerin farklı alanlarda yenilikçi çözümler üretmesine katkıda bulunmaktadır. Akıllı şehirler, dijital yönetim sistemleri ve sürdürülebilir kalkınma politikaları, bu teknolojilerin sunduğu inovatif çözümler arasında yer almaktadır (Ahad vd., 2020).

Her ne kadar bu teknolojiler yönetim süreçlerini dönüştürse de, belirli riskler ve sınırlılıklar da söz konusudur. Teknolojiye eşitsiz erişim, geleneksel iktidar yapıları üzerindeki etkiler ve yeni düzenleyici çerçevelere duyulan ihtiyaç, bu yeni yönetim şablonlarıyla ilişkili başlıca riskler arasında yer almaktadır. Teknolojinin geniş çapta benimsenmesi, toplumdaki dijital uçurumu

artırma riski taşımaktadır. Düşük gelirli bölgelerde ve dijital okuryazarlığın düşük olduğu yerlerde, bu teknolojilere erişim sınırlı olabilmektedir. Blokzincir ve dijital kimlik gibi teknolojiler, erişimi olmayan bireyler için yeni engeller yaratabilmektedir. Böylesi durumlar, dijital hizmetlerden faydalanamayan kesimlerin yönetim süreçlerinden dışlanmasına neden olabilmektedir. Eşitsiz erişim, toplumdaki fırsat eşitliğini zedeleyerek, sosyal adaletsizlikleri derinleştirme riskini taşımaktadır (Schuetz ve Venkatesh, 2020).

Merkeziyetçiliği azaltan teknolojiler, geleneksel iktidar yapıları üzerinde önemli bir baskı yaratma ihtimalini taşımaktadır. Blokzincir gibi merkeziyetsiz teknolojiler, geleneksel yönetim otoritelerinin gücünü zayıflatabilme potansiyeline sahiptir. Dolayısıyla, bu durum devletlerin kontrolünü kaybetme korkusuna neden olmaktadır. Özellikle otoriter devlet sistemleriyle bilinen ülkelerde, bu tür teknolojilere direnç gösterilmesi muhtemeldir. Merkeziyetsizlik, mevcut iktidar yapılarının yeniden şekillendirilmesini gerektirmekte ve dolayısıyla siyasi ve toplumsal çatışmalara yol açmaktadır (Busygina vd., 2018).

Blokzincir ve akıllı kontratlar gibi yenilikçi teknolojiler, mevcut yasal ve düzenleyici çerçevelerle uyumlu olmama durumunu da doğurmaktadır. Bu teknolojilerin güvenli ve adil bir şekilde kullanılabilmesi için yeni düzenleyici çerçevelere ihtiyaç söz konusudur. Blokzincir tabanlı işlemler ve akıllı kontratlar, geleneksel yasal sistemlerin dışında çalışan, otomatik ve merkeziyetsiz yapılar sunduğundan, bu teknolojilerin nasıl denetleneceği ve yasal olarak nasıl ele alınacağı konusunda belirsizlikler mevcuttur. Akıllı kontratların hukuki geçerliliği, yargı süreçlerinde nasıl ele alınacağı veya blokzincir üzerinden yapılan işlemlerin regülasyonlara uygunluğu gibi konular, mevcut düzenleyici yapıların yeniden şekillendirilmesini zorunlu kılmaktadır (Goldenfein ve Leiter, 2018).

Blokzincir ve akıllı kontrat gibi teknolojilerin kullanımı, geleneksel sorumluluk kavramlarını sınamaktadır. Bu teknolojilerin merkeziyetsiz yapıları, bir sorun ya da anlaşmazlık durumunda kimin sorumlu tutulacağını belirlemeyi zorlaştırmaktadır. Blokzincir tabanlı sistemlerde işlemler değiştirilemez olduğu için, hatalı veya yanlış işlemler karşısında hukuki başvuru yolları belirsiz kalabilmektedir. Bu nedenle, yeni teknolojilerin devletler ve uluslararası kuruluşlar tarafından düzenlenmesi, güvenlik ve hakların korunması açısından hayati önem taşımaktadır (Zhang vd., 2019).

Blokzincir ve akıllı kontrat gibi teknolojilerin merkeziyetsiz yapıları, klasik kamu yönetimi anlayışıyla kıyaslandığında, sorumluluk kavramlarını köklü bir şekilde sınamaktadır. Klasik kamu yönetimi, Max Weber'in bürokrasi teorisine dayalı olarak hiyerarşik, merkeziyetçi ve kurallara bağlı bir yapı sunmaktadır. Bu yapıda, sorumluluk net bir şekilde tanımlı otoriteler ve devlet kurumları arasında paylaştırılmaktadır (Weber, 2009). Buna karşın, blokzincir tabanlı sistemler, işlemlerin değiştirilemez ve dağıtık bir ağ üzerinde otomatik olarak yürütülmesi nedeniyle, sorumluluk zincirini belirsizleştirmektedir. Örnek vermek gerekirse, akıllı kontratlar, insan müdahalesi olmadan işlemleri gerçekleştirdiğinden, bir hata veya anlaşmazlık durumunda kimin sorumlu tutulacağı hukuki bir boşluk yaratmaktadır (Giancaspro, 2017). Klasik kamu yönetiminde, devlet hatalı işlemler için yargı yoluyla hesap verebilirken, blokzincirin merkeziyetsiz yapısı bu tür bir hesap verebilirlik mekanizmasını zorlaştırmakta ve yeni düzenleyici çerçeveler gerektirmektedir (Goldenfein ve Leiter, 2018). Bu nedenle, devletlerin ve uluslararası kuruluşların, blokzincir ve akıllı kontrat teknolojilerini klasik kamu yönetiminin hiyerarşik sorumluluk modeline entegre etmek için yeni hukuki ve düzenleyici yaklaşımlar geliştirmesi, hem güvenlik hem de bireysel hakların korunması açısından kritik önem taşımaktadır (Zhang vd., 2019).

Merkeziyetsiz teknolojiler, bireylerin kişisel verilerinin işlenmesi ve saklanması konusunda da yeni sorunlar yaratma ihtimalini taşımaktadır. Dijital kimlikler ve blokzincir tabanlı sistemler, kişisel verilerin dijital ortamda geniş çapta depolanmasını gerektirmektedir. Ancak bu verilerin güvenliği konusunda belirsizlikler söz konusudur. Merkeziyetsiz yapılar, verilerin yanlış ellere geçmesi durumunda geri dönülmesi zor sorunlar yaratabilmektedir. Bu tür teknolojilerin kullanımı sırasında veri gizliliğinin sağlanması ve bireylerin haklarının korunması için uluslararası standartlara uygun düzenlemeler getirilmesi gerekmektedir (Bernabe vd., 2019).

ISO/IEC 27001 standardı bu noktada örnek verilebilir. Bu standart, bilgi güvenliği yönetim sistemleri için küresel bir çerçeve sunarak, özellikle blokzincir gibi merkeziyetsiz teknolojilerde veri güvenliğini sağlamaya yönelik en iyi uygulamaları tanımlamaktadır (ISO/IEC, 2022). Ayrıca, OECD'nin Veri Koruma ve Mahremiyet İlkeleri, kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerinde şeffaflık, hesap verebilirlik ve veri minimizasyonu gibi prensipleri benimseyerek, devletlerin ve özel sektörün veri gizliliğini korumasına rehberlik etmektedir (OECD, 2013). Avrupa Birliği'nin GDPR mevzuatı ise, özellikle biyometrik veriler ve blokzincir tabanlı sistemlerde bireylerin rızasına dayalı veri işleme süreçlerini zorunlu kılarak, uluslararası bir referans noktası oluşturmaktadır (EU GDPR, 2016). Bu standartlar, blokzincir teknolojilerinin güvenli ve etik bir şekilde kullanılmasını desteklerken, veri ihlalleri ve mahremiyet ihlallerini önlemek için devletlere ve kuruluşlara rehberlik etmektedir. Fakat, bu standartların uygulanmasında küresel uyum ve teknolojik altyapı farklılıkları gibi zorluklar devam etmektedir.

Teknoloji, blokzincir, akıllı kontratlar ve dijital kimlikler gibi yenilikçi çözümlerle yönetim süreçlerini yeniden inşa etmektedir. Merkeziyetsiz karar alma süreçleri, güçlendirilmiş şeffaflık ve hesap verebilirlik ile geliştirilmiş yurttaş katılımı gibi yönetim şablonları, daha verimli, etkili ve güvenilir bir kamu yönetimi modeli oluşturma potansiyeline sahiptir. Ancak, bu teknolojilerin sunduğu yararların yanında, dijital uçurum, geleneksel iktidar yapılarındaki dönüşümler ve düzenleyici boşluklar gibi potansiyel riskler ve sınırlılıklar da söz konusudur.

Ancak, bu teknolojilerin sunduğu yararların yanında, dijital uçurum, geleneksel iktidar yapılarındaki dönüşümler ve düzenleyici boşluklar gibi potansiyel riskler ve sınırlılıklar da söz konusudur. Dijital uçurum, internet erişimi, dijital araçlar ve becerilerde eşitsizlik olarak tanımlanmaktadır. Bu durum, özellikle düşük gelirli ve kırsal bölgelerde yaşayan bireyleri etkileyerek eğitim, istihdam ve sağlık erişiminde ayrılıklar yaratmakta ve sosyal, ekonomik ile siyasi eşitsizlikleri derinleştirmektedir. Ülkeler, bu riski azaltmak için altyapı yatırımları ve eğitim programları düzenlemekte; örneğin, ABD'de Genişbant Eşitliği, Erişimi ve Yaygınlaştırma Programı (Broadband Equity Access and Deployment Program) erişimi yaygınlaştırırken, AB'de Dijital Eğitim Eylem Planı (Digital Education Action Plan) dijital okuryazarlığı artırılmakta ve gelişmekte olan ülkelerde Dünya Bankası destekli projeler (örneğin, Hindistan'da Digital India) benzer önlemler almaktadır (European Commission, 2025; National Telecommunications and Information Administration, n.d.; World Economic Forum, 2024). Geleneksel iktidar yapılarındaki dönüşümler, dijital teknolojilerin (AI, platformlar) merkeziyetçi otoriteleri zayıflatması ve güç dengelerini değiştirmesi olarak tanımlanır; bu, demokrasiyi tehdit ederek otoriter eğilimleri artırabilir veya katılımcı yönetim fırsatları yaratabilir, ancak eşitsizlikleri pekiştirir. Ülkelerin yanıtları arasında, AB'nin Digital Services Act ile platformları düzenlemesi, Çin'in dijital hükümet dönüşümü ve Türkiye'nin Ulusal Yapay Zekâ Stratejisi gibi politikalar yer alır, bunlar iktidar yapılarını dijital çağda yeniden şekillendirerek şeffaflık ve hesap verebilirliği artırmayı hedefler. Düzenleyici boşluklar, dijital teknolojilerin hızlı gelişimine ayak uyduramayan yasal çerçeveler olarak tanımlanmaktadır. Bu, veri güvenliği, rekabet ve inovasyon sorunlarına yol açarak ekonomik ve sosyal riskleri artırmaktadır (SIFMA, 2023). Ülkeler, bu boşlukları kapatmak için düzenlemeler yapmakta; örneğin, ABD'de Federal Trade Commission'ın dijital varlık kuralları, AB'de Yapay Zeka Yasası (AI Act) ve GDPR'nin genişletilmesi, Çin'de veri güvenliği yasaları ile uluslararası işbirlikleri (WEF raporları) riskleri yönetmeyi amaçlamaktadır (World Bank, n.d.; World Economic Forum, 2024). Bu risklerin yönetimi, kapsayıcı ve uyumlu politikalarla dijital dönüşümün sürdürülebilirliğini sağlamaktadır.

Devletlerin, bu teknolojilerin sunduğu avantajlardan yararlanırken, aynı zamanda adil ve kapsayıcı bir dijital yönetim modeli geliştirmesi büyük önem taşımaktadır. Teknolojiye erişimde eşitsizliklerin azaltılması, yeni düzenleyici çerçevelerin oluşturulması ve bireylerin haklarının korunması için gerekli düzenlemelerin yapılması, dijital çağın getirdiği fırsatları daha sürdürülebilir hale getirilmesi doğrultusunda önem taşımaktadır.

4. Hukukilik ve Mahremiyet Merkezli Sınamalar

Dijital teknolojilerin devlet tarafından yaygın olarak kullanımı, vatandaşlara daha verimli hizmetler sunma, güvenliği artırma ve kamu yönetiminde yenilikçi çözümler geliştirme açısından önemli avantajlar sağlamaktadır. Ancak bu teknolojilerin devlet yapılarında kullanımı, hukukilik ve mahremiyet merkezli birçok sınamayı da beraberinde getirmiştir. Veri güvenliği, gözetim uygulamaları, biyometrik veri toplama ve kullanımı, çevrimiçi tehditler ve siber zorbalık, bu bağlamda öne çıkan başlıca tartışma konuları arasındadır. Dijital teknolojilerin kullanımının hızla artmasıyla birlikte, devletlerin bu süreçleri hukuk çerçevesinde nasıl denetleyebileceği ve vatandaşların temel haklarını nasıl koruyacağı üzerine ciddi bir düşünce oluşmuştur. Bu doğrultuda, dijital teknolojilerin devlette kullanımında karşılaşılan hukukilik ve mahremiyet odaklı sınamalar detaylandırılmalıdır.

Dijital teknolojilerin devlete entegrasyonu, büyük miktarda verinin toplanması ve işlenmesi sürecini doğurmuştur. Devletler, vatandaşlara sundukları hizmetler kapsamında kişisel verileri toplamakta ve bu verileri farklı kamu hizmetlerinde kullanmaktadır. Ancak bu veri toplama süreci, beraberinde ciddi güvenlik ve mahremiyet sorunları getirmektedir. Devletin geniş çapta gözetim yapma yetkisi ve toplanan verilerin güvenli bir şekilde saklanıp saklanamayacağı konusundaki belirsizlikler, vatandaşların özel yaşamına yönelik tehditleri artırmaktadır.

Devletin geniş çapta gözetim yapma yetkisi ve toplanan verilerin güvenli bir şekilde saklanıp saklanamayacağı konusundaki belirsizlikler, vatandaşların özel yaşamına yönelik tehditleri artırmaktadır. Bu riskleri azaltmak için, kişisel verilerin korunmasına yönelik mevzuat ve önlemler kritik bir rol oynamaktadır. Türkiye’de KVKK, veri işleme süreçlerinde şeffaflık, sınırlama ve hesap verebilirlik ilkelerini zorunlu kılarak, devletin gözetim faaliyetlerini düzenlemeyi ve bireylerin mahremiyetini korumayı hedeflemektedir (KVKK, 2016). Avrupa Birliği’nde ise GDPR, özellikle biyometrik veriler ve gözetim teknolojilerinin kullanımında sıkı kurallar getirerek, veri sahiplerinin rızasını ve veri güvenliğini önceliklendirmektedir (EU GDPR, 2016). Bunun yanı sıra, veri güvenliğini artırmak için pratik önlemler arasında güçlü şifreleme protokolleri, düzenli güvenlik denetimleri ve anonimleştirme teknikleri yer almaktadır; bu önlemler, veri ihallerini ve izinsiz gözetimi önlemede etkili olmaktadır (Tao vd., 2019). Ancak, bu mevzuatın ve önlemlerin etkinliği, teknolojik gelişmelerin hızına ayak uydurma ve uluslararası uyum gibi zorluklara bağlıdır, bu da devletlerin sürekli güncellenen politikalar geliştirmesini gerektirmektedir.

Gözetim teknolojileri, devletlere vatandaşların dijital aktivitelerini izleme ve takip etme olanağı sunmaktadır. Güvenlik adına yapılan bu gözetim faaliyetleri, vatandaşların hareketlerini izlemek ve dijital ortamda yaptıkları her türlü aktiviteyi takip etmek gibi yetkilere dayanmaktadır. Devletlerin terörle mücadele ya da ulusal güvenlik amacıyla dijital iletişimlerini izleme yetkisi, gözetim faaliyetlerinin sınırlarını zorlamaktadır. Nihayetinde bireylerin mahremiyet haklarına yönelik büyük bir tehdit oluşmaktadır. Demokratik toplumlarda gözetim faaliyetleri, vatandaşların özgürlüklerini kullanmalarına engel olacak bir korku ortamı yaratabilmekte ve toplumda güvensizlik yayılmasına neden olabilmektedir (Newell, 2014).

Devletlerin büyük miktarda veriyi dijital ortamda toplaması, bu verilerin güvenli bir şekilde korunmasını zorunlu kılmaktadır. Ancak siber saldırılar, veri hırsızlığı ve veri sızıntıları gibi riskler, devletlerin vatandaşlara ait bilgileri koruma yükümlülüğünü zorlaştırmaktadır. Sağlık, finans ve kimlik bilgileri gibi hassas verilerin ele geçirilmesi, vatandaşların güvenliği için büyük bir tehdit oluşturmaktadır (Tao vd., 2019). Bu tür verilerin siber saldırılara karşı korunamaması, devletlerin veri güvenliği konusunda ciddi yaptırımlarla karşılaşmasına yol açma ihtimalini taşımaktadır. Bu bağlamda, dijital verilerin güvenliği için devletlerin güçlü siber güvenlik altyapılarına sahip olması ve bu alanda sürekli olarak kendini güncellemesi gerekmektedir.

Dijital teknolojilerin yaygınlaşmasıyla birlikte, çevrimiçi tehditler ve siber zorbalık gibi yeni tehlikeler de ortaya çıkmıştır. Devletler, bu tür tehditlerle mücadele etmek için çeşitli dijital güvenlik önlemleri almakta, siber zorbalık ve dijital tehditleri önlemek için yasal düzenlemeler

yapmaktadır. Ancak bu süreçte, devletlerin çevrimiçi tehditleri kontrol etme amacıyla aldığı bazı önlemler, ifade özgürlüğü ve dijital mahremiyet üzerinde olumsuz etkilere sebep olmaktadır (Asam vd., 2016). Bu önlemler arasında, sosyal medya platformlarında içerik filtreleme ve kaldırma işlemleri (örneğin, sahte haberlere karşı otomatik sansür araçları), çevrimiçi aktivitelerin izlenmesi (gözetim yazılımları ve veri toplama), erişim kısıtlamaları (site engelleme veya IP blokajı) ve zorunlu veri paylaşımı gereklilikleri yer almaktadır. Örneğin, Avrupa Birliği'nde GDPR'ye dayalı veri koruma kuralları, bireylerin mahremiyetini korumayı amaçlasa da, devletlerin gözetim yetkilerini genişleterek özel hayata müdahaleye yol açabilmektedir. Bu önlemler, ulusal güvenlik adına gerekli olsa da, KVKK gibi yerel mevzuat ve uluslararası insan hakları standartları (örneğin, Avrupa İnsan Hakları Sözleşmesi'nin 8. ve 10. maddeleri) ile dengelenmek durumundadır. Aksi takdirde toplumda güvensizlik ve sansür algısını artırabilmektedir.

Devletler, çevrimiçi tehditlere karşı vatandaşlarını koruma yükümlülüğüne sahiptir. Ancak bu koruma, bireylerin dijital mahremiyetini ihlal etmeyecek şekilde yapılmak durumundadır. Çocuklar ve gençler gibi savunmasız grupların çevrimiçi tehditlerden korunması amacıyla yapılan devlet müdahaleleri, dijital güvenlik ve mahremiyet dengesi göz önünde bulundurularak tasarlanma zorunluluğundadır. Bununla birlikte, çevrimiçi platformlar üzerindeki gözetim faaliyetleri artırılırken, bireylerin dijital aktivitelerinin sürekli izlenmesi, devlete yönelik güvensizliklerin artmasına yol açmaktadır (Murthy vd., 2021).

Dijital teknolojilerin devletler tarafından geniş çapta kullanımı, hukukilik ve mahremiyet açısından önemli sınamaları beraberinde getirmektedir. Devletlerin bu süreçleri yönetirken vatandaşların mahremiyet haklarını koruma sorumluluğu büyük önem taşımaktadır. Hukuki düzenlemeler ve veri güvenliği politikaları, dijital teknolojilerin sunduğu fırsatlarla beraber, vatandaşların temel hak ve özgürlüklerinin korunmasını sağlayacak şekilde tasarlanmak durumundadır (Weber, 2015).

Mahremiyet ve hukukilik arasındaki dengeyi sağlamak, dijital çağın getirdiği en büyük sınavlardan biri olup, devletlerin bu süreci etik ilkeler doğrultusunda yönetmesi, vatandaşlarla devlet arasındaki güven ilişkisinin korunması açısından kritik bir rol oynamaktadır. Dijital teknolojilerin devlet yönetiminde yarattığı sınamalara yanıt vermek, devletlerin güvenliği sağlamada ve vatandaşların haklarını korumada daha etkili ve etik çözümler üretmesine olanak tanımaktadır (Joshi vd., 2002). Bu yanıtların bazı önemli yararları arasında güçlendirilmiş kamu güveni, geliştirilmiş şeffaflık ve hesap verebilirlik ile zenginleştirilmiş insan hakları ve saygınlığı yer almaktadır. Dolayısıyla, dijital çağın getirdiği sınamalara yönelik çözüm yaklaşımlarının bu açılardan nasıl fayda sağladığı incelenmeyi hak etmektedir.

Dijital teknolojilerin gözetim, veri toplama ve biyometrik sistemler gibi güvenlik alanlarında kullanılması, vatandaşların kişisel haklarına yönelik endişelere yol açsa da, bu uygulamalara karşı geliştirilecek doğru çözümler kamu güvenliğini büyük ölçüde artırabilmektedir. Devletler, bu teknolojileri kullanırken vatandaşlarının mahremiyetine saygı gösteren, verileri koruyan ve güvenlik mekanizmalarını daha şeffaf hale getiren politikalar geliştirdikleri durumda, toplumun devlete olan güveni de artmaktadır (McGraw vd., 2009).

Yapay zekâ destekli gözetim sistemleri, kalabalık etkinliklerde, şehir merkezlerinde veya sınır bölgelerinde anormallikleri tespit ederek kamu güvenliğini artırmaktadır. Bu tür teknolojilerin sorumlu ve denetimli kullanımı, vatandaşların kamusal alanlarda kendilerini daha güvende hissetmelerini sağlamaktadır. Aynı zamanda bu sistemlerin denetlenebilir ve hesap verebilir olması, güvenlik önlemlerinin keyfi kullanılmasını engelleyerek kamu güvenine katkıda bulunmaktadır. Veri güvenliği ve çevrimiçi tehditlerle mücadelede kullanılan siber güvenlik önlemleri, vatandaşların dijital dünyada kendilerini daha güvende hissetmelerine olanak tanımaktadır. Devletlerin siber güvenlik altyapılarını güçlendirmesi ve bireylerin kişisel verilerini koruma konusundaki çabaları, toplumun dijital ortama olan güvenliğini artırmaktadır. Ayrıca, çevrimiçi tehditlere karşı etkili önlemler almak, dijital alanı daha güvenli bir yer haline getirmekte ve vatandaşların bu ortamda daha özgürce hareket etmelerini sağlamaktadır (Baldini vd., 2014).

Dijital teknolojilerin kamu yönetiminde kullanılması, aynı zamanda yönetim süreçlerinin daha şeffaf ve hesap verebilir hale gelmesine yardımcı olmaktadır. Verilerin dijital ortamda depolanması ve blokzincir gibi teknolojilerin kullanılması, devletin işlemlerini daha izlenebilir kılmakta ve vatandaşların devletin faaliyetlerine daha fazla erişim sağlamasına olanak tanımaktadır. Bu durum, yolsuzlukların önlenmesi ve kamu kaynaklarının adil şekilde kullanılmasının sağlanmasında önemli bir kolaylaştırıcı olarak görülmektedir (Pelt vd., 2021).

Blokzincir tabanlı sistemler, devlet işlemlerinin ve kamu ihalelerinin şeffaf bir şekilde yürütülmesini sağlayarak, yolsuzluk riskini azaltmaktadır. Blokzincir teknolojisi kullanılarak yapılan devlet harcamaları, vatandaşlar tarafından kolayca izlenebilir hale gelmektedir. Bu tür uygulamalar, devletin mali süreçlerinin şeffaflaşmasına katkı sağlayarak kamu kaynaklarının daha doğru ve etkili kullanılmasını teşvik etmektedir. Ayrıca, bu şeffaflık vatandaşların devlete olan güvenini güçlendirmekte ve hesap verebilirliği artırmaktadır (Beck vd., 2018).

Dijital teknolojilerin devlet hizmetlerinde etkin kullanımı, insan haklarının korunması ve vatandaşların onurunun gözetilmesi açısından da büyük önem taşımaktadır. Mahremiyet haklarının korunması, bireylerin kişisel verilerinin güvenliğini sağlamak ve devletin bu verileri kötüye kullanmasını engellemek, vatandaşların insan haklarına saygı duyulan bir yönetim sisteminde yaşama hakkını güvence altına almaktadır (Ke ve Sudhir, 2022).

Dijital teknolojilere dayalı güvenlik ve yönetim çözümleri, çeşitli yararlar sağlasa da, beraberinde önemli riskler ve zorluklar da getirmektedir. Bu teknolojilerin sorumlu bir şekilde yönetilmesi, bireysel özgürlükler ile ulusal güvenlik endişeleri arasında denge sağlanmasını, teknoloji ve dijital hizmetlere eşit erişimin güvence altına alınmasını ve etkili düzenleyici çerçevelerin oluşturulmasını gerektirmektedir.

Dijital teknolojilerin gözetim ve veri toplama süreçlerinde yaygın olarak kullanılması, devletlerin ulusal güvenlik adına bireylerin özgürlüklerini kısıtlayıcı adımlar atmasına yol açabilmektedir. Bu noktada, ulusal güvenlik ve bireysel haklar arasındaki dengeyi sağlamak, devletlerin karşılaştığı en büyük zorluklar arasındadır. Devletlerin güvenlik adına gözetim teknolojilerini yoğun bir şekilde kullanması, bireylerin özel yaşamına yönelik tehditleri artırabilmektedir. Yüz tanıma sistemleri ve biyometrik gözetim teknolojileri, vatandaşların sürekli izlenmesine ve mahremiyet haklarının ihlal edilmesine neden olabilmektedir. Bu tür teknolojilerin aşırı kullanımı, bireysel özgürlüklerin kısıtlanmasına ve demokratik süreçlerin zarar görmesine yol açabilmektedir.

Dijital teknolojilerin kullanımı, toplumun tüm kesimlerine eşit şekilde yayılmadığında, sosyal ve ekonomik eşitsizlikleri derinleştirebilir. Düşük gelirli bölgelerde veya kırsal alanlarda yaşayan bireyler, dijital hizmetlere ve güvenlik teknolojilerine erişimde zorluklar yaşayabilir. Dolayısıyla, toplumda dijital uçurumun büyümesine ve kamu hizmetlerinden faydalanma konusunda eşitsizliklerin artmasına neden olabilir.

Blokzincir, akıllı kontratlar ve biyometrik sistemler gibi teknolojiler, teknolojiye erişim imkanı olmayan bireyler için yeni engeller yaratabilmektedir. Bu tür sistemler, toplumun belirli kesimlerine hitap ederken, düşük gelirli ve dijital okuryazarlığı düşük bireyler için yeni bir ayrımcılık kaynağı olabilmektedir. Dijital hizmetlerin herkes tarafından eşit erişilebilir olmasını sağlamak için devletlerin, altyapı yatırımları yapması ve dijital kapsayıcılığı artırması gerekmektedir (Cong ve He, 2018).

Dijital teknolojilerin hukuki olarak nasıl yönetileceği ve düzenleneceği konusunda büyük bir belirsizlik mevcuttur. Blokzincir ve yapay zekâ gibi teknolojilerin gelişmesiyle birlikte, mevcut düzenleyici çerçeveler yetersiz kalmaktadır. Bu nedenle, devletlerin bu yeni teknolojilere uygun etkili düzenleyici çerçeveler geliştirmesi gerekmektedir. Yeni teknolojiler, mevcut hukuki sistemlerde boşluklar yaratmakta ve bu boşluklar, bireylerin haklarının yeterince korunamamasına neden olmaktadır. Blokzincir tabanlı işlemler ve akıllı kontratlar, mevcut hukuk sistemlerine uymayan yapılar sunmaktadır. Dolayısıyla, işlemlerin denetlenmesi, sorumlulukların belirlenmesi ve yanlış uygulamaların önlenmesi konusunda zorluklar yaratmaktadır (Giancaspro, 2017).

5. Sonuç

Dijital teknolojilerin devlet yönetiminde kullanılmasına yönelik sınamalara getirilen çözümler, kamu güvenliği, şeffaflık ve insan hakları açısından önemli avantajlar sunmaktadır. Güçlendirilmiş kamu güveni, geliştirilmiş şeffaflık ve hesap verebilirlik ile insan haklarının geliştirilmesi gibi yararlar, bu teknolojilerin doğru yönetildiğinde topluma ve devlete nasıl olumlu katkılar sağlayabileceğini göstermektedir. Ancak, bu yararların yanında potansiyel risk ve zorluklar da söz konusudur. Bireysel hürriyetlerin ulusal güvenlik endişeleriyle dengelenmesi, dijital hizmetlere ve teknolojiye eşit erişimin güvence altına alınması ve etkili düzenleyici çerçevelerin oluşturulması, bu teknolojilerin toplum üzerindeki olası olumsuz etkilerini minimize etmek için hayati öneme sahiptir.

Devletler, dijital teknolojiler aracılığıyla ulusal güvenliği sağlamaya çalışırken, bireysel özgürlükleri koruma sorumluluğuna da sahiptir. Gözetim teknolojileri ve veri toplama süreçleri, güvenlik açısından gerekli olsa da, vatandaşların özel hayatlarına müdahale riski taşımaktadır. Bu riskli durum, devletlerin güvenlik ve özgürlükler arasındaki dengeyi iyi kurmasını gerektirmektedir. Aşırı güvenlik tedbirleri ve izleme sistemleri, bireylerin demokratik haklarını kullanmalarını zorlaştırmakta ve toplumda korku ve baskı ortamı yaratabilmektedir. Bu nedenle, devletlerin ulusal güvenlik endişeleri doğrultusunda gözetim ve veri toplama süreçlerini denetim altında tutması, bu süreçleri hukuk çerçevesinde düzenlemesi ve vatandaşların temel haklarını koruyan mekanizmalar oluşturması büyük önem taşımaktadır.

Bireysel özgürlüklerin korunması, demokratik toplumların temel taşıdır ve devletlerin bu hakları ihlal etmemesi için şeffaf ve hesap verebilir politikalar geliştirmesi gerekmektedir. Bu bağlamda, devletin yaptığı gözetim faaliyetlerinin sınırlarının net olarak belirlenmesi ve bu faaliyetlerin yargı denetimine tabi tutulması, vatandaşların güvenini artırmaktadır. Aynı zamanda, mahremiyet ve veri güvenliğine yönelik yasal düzenlemeler, bireylerin haklarını koruma altına alırken, devletin güvenlik önlemlerini aşırıya kaçmadan uygulamasına olanak tanımaktadır.

Dijital teknolojiler devlet yönetiminde büyük yenilikler ve verimlilik sağlasa da, bu teknolojilere erişimde yaşanan eşitsizlikler toplumsal adaletsizliği derinleştirme potansiyeli taşımaktadır. Kırsal kesimde yaşayan veya düşük gelirli vatandaşlar, dijital hizmetlere ve teknolojiye erişim konusunda dezavantajlı konumda olabilmektedir. Neticede, toplumda dijital uçurumun büyümesine ve vatandaşlar arasındaki eşitsizliklerin artmasına neden olmaktadır. Dijital erişim eksikliği, sadece bireylerin kamu hizmetlerine ulaşmasını zorlaştırmakla kalmamakta, aynı zamanda yönetim süreçlerine katılımı da sınırlamaktadır. Bu da, demokratik süreçlerde fırsat eşitliği ve temsil hakkı açısından sorunlar yaratmaktadır.

Devletler, dijital hizmetlerin ve teknolojilerin toplumun tüm kesimlerine eşit şekilde ulaşabilmesini sağlamak için altyapı yatırımları yapma ve dijital okuryazarlığı artırmaya yönelik politikalar geliştirme sorumluluğundadır. Kırsal ve dezavantajlı bölgelerde yaşayan vatandaşların, dijital hizmetlere erişimini kolaylaştıracak programlar oluşturulması gerekmektedir. Dijital kapsayıcılığı artırmak, toplumda fırsat eşitliğini sağlamakla birlikte, kamu hizmetlerinin daha etkin bir şekilde sunulmasına da katkıda bulunmaktadır.

Dijital teknolojilerin devlet yönetiminde kullanımı, hukuki düzenlemeler konusunda ciddi bir boşluk yaratmıştır. Blokzincir, yapay zekâ, biyometrik veriler ve dijital kimlik sistemleri gibi teknolojilerin yaygınlaşması, mevcut hukuki çerçevelerin yetersiz kalmasına neden olmaktadır. Bu nedenle, devletlerin bu teknolojilere uygun düzenleyici çerçeveler oluşturması gerekmektedir. Aksi takdirde, vatandaşların haklarının ihlal edilmesi, veri güvenliği açıkları ve sorumlulukların belirsizliği gibi ciddi sorunlarla karşılaşılabilir.

Yeni dijital teknolojiler, geleneksel hukuk sistemlerinde boşluklar yaratmakta ve bu boşluklar vatandaşların haklarının yeterince korunamamasına neden olmaktadır. Yapay zekâ tabanlı sistemlerin verdiği kararların nasıl denetleneceği, biyometrik verilerin nasıl işleneceği ve bu verilere kimlerin erişim sağlayabileceği gibi konular, net düzenlemeler gerektirmektedir. Blokzincir tabanlı işlemler ve akıllı kontratlar, merkezi olmayan yapıları nedeniyle mevcut hukuki düzenlemelerin

dışında kalan sistemlerdir. Bu sistemlerde sorumluluğun nasıl belirleneceği, yanlış işlemler durumunda başvurulacak hukuki yolların olup olmadığı gibi sorular, düzenleyici eksiklikler nedeniyle belirsiz kalmaktadır.

Devletler, bu teknolojilerin güvenli ve adil bir şekilde kullanılmasını sağlamak amacıyla yeni ve kapsamlı düzenlemeler geliştirmek durumundadır. Veri güvenliği, mahremiyet, yapay zekâ etik kuralları gibi alanlarda güçlü düzenlemeler oluşturulması, hem devletlerin bu teknolojileri etkin şekilde kullanmasına hem de vatandaşların haklarının korunmasına katkı sağlama potansiyelini taşımaktadır. Ayrıca, uluslararası işbirliği ve koordinasyon, dijital teknolojilere dair düzenleyici çerçevelerin etkinliğini artırmak için önemli bir adım olmaktadır. Dijitalleşmenin küresel boyutu düşünüldüğünde, sınır ötesi veri transferleri ve siber güvenlik konularında uluslararası standartlar oluşturulması, devletler için kritik öneme sahiptir.

Dijital teknolojilerin devlette kullanımı, kamu güvenliği, şeffaflık, hesap verebilirlik ve insan haklarının korunması açısından önemli yararlar sağlarken, beraberinde hukukilik ve mahremiyet konusunda ciddi sınamaları da getirmektedir. Devletlerin bu sınamalara yanıt verirken güvenlik ve bireysel özgürlükler arasında denge kurması, dijital hizmetlere eşit erişimi sağlaması ve etkili düzenleyici çerçeveler oluşturması gerekmektedir. Bu süreçlerin doğru yönetilmesi, vatandaşların devlete olan güvenini artırmakta, yönetim süreçlerinin daha adil ve şeffaf olmasını sağlamaktadır. Devletlerin dijital dönüşüm süreçlerinde bireylerin haklarını koruma sorumluluğu, demokrasilerin sürdürülebilirliği ve toplumların refahı açısından büyük önem taşımaktadır. Teknolojik gelişmelerin getirdiği fırsatları değerlendirirken, toplumsal eşitlik, insan hakları ve etik sorumluluklar göz ardı edilmemeli, devletler bu konuda güçlü ve kapsamlı politikalar geliştirmelidir.

Kaynakça

- Aas, K. F. (2013). 'Getting Ahead of the Game': Border Technologies and the Changing Space of Governance. *Global Surveillance and Policing*, 194-214, Willan.
- Ahmadisheykhsarmast, S., & Sonmez, R. (2020). A Smart Contract System for Security of Payment of Construction Contracts. *Automation in Construction*, 120, 103401. <https://doi.org/10.1016/j.autcon.2020.103401>
- Ahad, M., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling Technologies and Sustainable Smart Cities. *Sustainable Cities and Society*. <https://doi.org/10.1016/j.scs.2020.102301>
- Ağırdil, O. (2025a). Almanya'nın Kamu Güvenliği Politikaları: Strateji Belgeleri Üzerinden Bir İnceleme. *Liberal Düşünce Dergisi*, (118), 199-230. <https://doi.org/10.36484/liberal.1683028>
- Ağırdil, O. (2025b). Fransa'nın Kamu Güvenliği Politikaları: Strateji Belgeleri Üzerinden Bir İnceleme. *İletişim Ve Diplomasi*, (14), 23-44. <https://doi.org/10.54722/iletisimvediplomasi.1667005>
- Aleem, A., Wakefield, A., & Button, M. (2013). Addressing the Weakest Link: Implementing Converged Security. *Security Journal*, 26, 236-248. <https://doi.org/10.1057/sj.2013.14>
- Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. (2021). Deep Learning-Enabled Threat Intelligence Scheme in the Internet of Things Networks. *IEEE Transactions on Network Science and Engineering*, 8, 2968-2981. <https://doi.org/10.1109/tnse.2020.3032415>
- Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, 314(5799), 610-613.
- Andrejevic, M., & Gates, K. (2014). Big Data Surveillance: Introduction. *Surveillance & Society*, 12(2), 185-196.
- Balkin, J. (2003). Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. <https://doi.org/10.2139/ssrn.470842>

- Beck, R., Müller-Bloch, C., & King, J. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, 19, 1. <https://doi.org/10.17705/1jais.00518>
- Bernabe, J., Cánovas, J., Hernández-Ramos, J., Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, 7, 164908-164940. <https://doi.org/10.1109/access.2019.2950872>
- Brayne, S., & Christin, A. (2020). Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts. *Social Problems*. <https://doi.org/10.1093/socpro/spaa004>
- Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A Framework for Competence Development and Assessment in Hybrid Cybersecurity Exercises. *Computers & Security*, 88, 101607. <https://doi.org/10.1016/j.cose.2019.101607>
- Broeders, D., & Dijstelbloem, H. (2015). The Datafication of Mobility and Migration Management: The Mediating State and Its Consequences. In *Digitizing Identities*, 242-260, Routledge.
- Burton, J., & Soare, S. (2019). Understanding the Strategic Implications of the Weaponization of Artificial Intelligence. *2019 11th International Conference on Cyber Conflict (CyCon)*, 1-17. IEEE. <https://doi.org/10.23919/cycon.2019.8756866>
- Busygina, I., Filippov, M., & Taukebaeva, E. (2018). To Decentralize or to Continue on the Centralization Track: The Cases of Authoritarian Regimes in Russia and Kazakhstan. *Journal of Eurasian Studies*, 9, 61-71. <https://doi.org/10.1016/j.euras.2017.12.008>
- Chachko, E. (2021). National Security by Platform. *Stan. Tech. L. Rev.*, 25, 55.
- Chaar-López, I. (2019). Sensing Intruders: Race and the Automation of Border Control. *American Quarterly*, 71, 495 - 518.
- Chowdhury, N., & Gkioulos, V. (2021). Cyber Security Training for Critical Infrastructure Protection: A Literature Review. *Computer Science Review*, 40, 100361. <https://doi.org/10.1016/j.cosrev.2021.100361>
- Cong, L., & He, Z. (2018). Blockchain Disruption and Smart Contracts. Kauffman: Entrepreneurship Scholars Initiatives (Topic). <https://doi.org/10.2139/ssrn.2985764>
- Crampton, J. W. (2019). Platform Biometrics. *Surveillance & Society*, 17(1/2), 54-62.
- Dunn Cavelty, M. (2012). The Militarisation of Cyberspace: Why Less May Be Better. In *4th International Conference on Cyber Conflict (CYCON 2012)*, 141-153. IEEE. https://ccdcoc.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf
- Çatlı, M. (2021). *Dijital Devlet Teorisi*. Ankara: Adalet Yayınevi.
- Dyson, E. (2008). Reflections on Privacy 2.0. *Scientific American*, 299(3), 50-55. <https://doi.org/10.1038/scientificamerican0908-50>
- EU GDPR. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (EU)*, 679(2016), 10-13.
- European Commission, Directorate-General for Education, Youth, Sport and Culture. (2025). *About the Digital Education Action Plan*. European Education Area. <https://education.ec.europa.eu/focus-topics/digital-education/plan>
- Farnaghi, M., & Mansourian, A. (2020). Blockchain, an Enabling Technology for Transparent and Accountable Decentralized Public Participatory GIS. *Cities*, 105, 102850. <https://doi.org/10.1016/j.cities.2020.102850>

- Gelb, A., & Clark, J. (2013). Identification for Development: The Biometrics Revolution. *Center for Global Development Working Paper*, 315. <https://doi.org/10.2139/ssrn.2226594>
- Giancaspro, M. (2017). Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective. *Computer Law & Security Review*, 33, 825-835. <https://doi.org/10.1016/j.clsr.2017.05.007>
- Goldenfein, J., & Leiter, A. (2018). Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique*, 29, 141-149. <https://doi.org/10.1007/s10978-018-9224-0>
- Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.
- Grabosky, P. (2007). The Internet, Technology, and Organized Crime. *Asian Journal of Criminology*, 2(2), 145-161. <https://doi.org/10.1007/s11417-007-9034-z>
- Grimmelikhuijsen, S. (2012). Linking Transparency, Knowledge and Citizen Trust in Government: An Experiment. *International Review of Administrative Sciences*, 78, 50-73. <https://doi.org/10.1177/0020852311429667>
- Guo, J., & Zhang, H. (2024). Digital age: The Path Choice of Government-Citizen Value Co-Creation. *Heliyon*, 10(15).
- Hanna, N. (2018). A Role for the State in the Digital Age. *Journal of Innovation and Entrepreneurship* 7(5). <https://doi.org/10.1186/s13731-018-0086-3>
- Heinl, C. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy*, 18, 131-159. <https://doi.org/10.1353/asp.2014.0026>
- Hilbert, M. (2020). Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective. *Dialogues in Clinical Neuroscience*, 22(2), 189-194.
- Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law*, 28(1), 65-98.
- ISO/IEC. (2022). *ISO/IEC 27001: Information Security Management Systems*. International Organization for Standardization. <https://www.iso.org/standard/54534.html>
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20. <https://doi.org/10.1109/tcsvt.2003.818349>
- Joshi, J., Ghafoor, A., Aref, W., & Spafford, E. (2002). Security and Privacy Challenges of a Digital Government. *Proceedings of the National Conference on Digital Government*, 121-136. https://doi.org/10.1007/0-306-47374-7_7
- Ke, T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*. <https://doi.org/10.1287/mnsc.2022.4614>
- Khalil, K., Abdel-Aziz, M., Nazmy, T., & Salem, A. (2008). The Role of Artificial Intelligence Technologies in Crisis Response. *ArXiv, abs/0806.1280*
- Kostyuk, N., & Wayne, C. (2020). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*. <https://doi.org/10.1093/jogss/ogz077>
- KVKK. (2016). 6698 Sayılı Kişisel Verilerin Korunması Kanunu. *Resmî Gazete*, 29677. <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-9.htm>
- Laufs, J., Borrión, H., & Bradford, B. (2020). Security and the Smart City: A Systematic Review. *Sustainable Cities and Society*, 55, 102023. <https://doi.org/10.1016/j.scs.2020.102023>

- Lyon, D. (1992). The New Surveillance: Electronic Technologies and The Maximum-Security Society. *Crime, Law and Social Change*, 18, 159-175. <https://doi.org/10.1007/bf00230629>
- Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society*, 1(2), 1-13. <https://doi.org/10.1177/2053951714541861>
- McAuliffe, M., Blower, J., & Beduschi, A. (2021). Digitalization and Artificial Intelligence in Migration and Mobility: Transnational Implications of the COVID-19 Pandemic. *Societies*, 11(4), 135.
- Murthy, S., Bhat, K., Das, S., & Kumar, N. (2021). Individually Vulnerable, Collectively Safe. *Proceedings of the ACM on Human-Computer Interaction*, 5, 1-24. <https://doi.org/10.1145/3449212>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>
- National Telecommunications and Information Administration. (n.d.). *Broadband Equity, Access, and Deployment (BEAD) Program*, U.S. Department of Commerce. <https://broadbandusa.ntia.gov/funding-programs/broadband-equity-access-and-deployment-bead-program>
- Nguyen Duc, A., & Chirumamilla, A. (2019). Identifying security risks of digital transformation-an engineering perspective. In *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18*, 677-688. Springer International Publishing.
- OECD. (2013). *The OECD Privacy Framework*. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
- OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. OECD.
- Owen, S. (2017). Monitoring social media and protest movements: Ensuring Political Order through Surveillance and Surveillance Discourse. *Social Identities*, 23(6), 688-700.
- Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-based Platforms: Decentralized Infrastructures and Its Boundary Conditions. *Technological Forecasting and Social Change*, 146, 94-102.
- Rhodes, R. A. W. (1996). The New Governance: Governing without Government. *Political Studies*, 44(4), 652-667. <https://doi.org/10.1111/j.1467-9248.1996.tb01747.x>
- Sarker, I. (2021). CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks. *ArXiv, abs/2104.08080*. <https://doi.org/10.1016/j.iot.2021.100393>
- Schuetz, S., & Venkatesh, V. (2020). Blockchain, Adoption, and Financial Inclusion in India: Research Opportunities. *International Journal of Information Management*, 52, 101936. <https://doi.org/10.1016/j.ijinfomgt.2019.04.009>
- SIFMA. (2023). *Addressing Regulatory Gaps in the Digital Asset Ecosystem*. <https://www.sifma.org/resources/news/addressing-regulatory-gaps-in-the-digital-asset-ecosystem/>
- Singh, R., Majumdar, P., Mittal, S., & Vatsa, M. (2021). Anatomizing Bias in Facial Analysis. *Proceedings of the AAAI Conference on Artificial Intelligence*, 36, 12351-12358. <https://doi.org/10.1609/aaai.v36i11.21500>

- Starr, A., Fernandez, L., Amster, R., Wood, L., & Caro, M. (2008). The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis. *Qualitative Sociology*, 31, 251-270. <https://doi.org/10.1007/s11133-008-9107-z>
- Sung, C., & Park, J. (2021). Understanding of Blockchain-Based Identity Management System Adoption in the Public Sector. *Journal of Enterprise Information Management*, 34, 1481-1505. <https://doi.org/10.1108/jeim-12-2020-0532>
- Taddeo, M. (2013). Cyber Security and Individual Rights, Striking the Right Balance. *Philosophy & Technology*, 26, 353-356. <https://doi.org/10.1007/s13347-013-0140-9>
- Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting Artificial Intelligence in Cybersecurity is a Double-Edged Sword. *Nature Machine Intelligence*, 1-4. <https://doi.org/10.1038/s42256-019-0109-1>
- Tao, H., Bhuiyan, M., Rahman, M., Wang, G., Wang, T., Ahmed, M., & Li, J. (2019). Economic Perspective Analysis of Protecting Big Data Security and Privacy. *Future Generation Computer Systems*, 98, 660-671. <https://doi.org/10.1016/j.future.2019.03.042>
- Timmers, P. (2024). Sovereignty in the digital age. *Introduction to Digital Humanism*, 571-592.
- Vladucu, M., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. *IEEE Access*, 11, 23293-23308. <https://doi.org/10.1109/access.2023.3253682>
- Weber, M. (2009). *The Theory of Social and Economic Organization*. Simon and Schuster.
- Weber, R. (2015). The digital future - A challenge for privacy? *Computer Law & Security Review*, 31, 234-242. <https://doi.org/10.1016/j.clsr.2015.01.003>
- Weingärtner, T., Batista, D., Köchli, S., & Voutat, G. (2021). Prototyping a Smart Contract Based Public Procurement to Fight Corruption. *Computers*, 10, 85. <https://doi.org/10.3390/computers10070085>
- Wiranata, A. J. (2024). Utilization of Artificial Intelligence in Monitoring and Mitigating National Security Threats. *Security Intelligence Terrorism Journal*, 1(2), 122–127.
- World Bank. (n.d.). *Digital Transformation Overview*. <https://www.worldbank.org/en/topic/digital/overview>
- World Economic Forum. (2024). *How Countries are Navigating Uncertainty of Digital Asset Regulation*. <https://www.weforum.org/stories/2024/10/different-countries-navigating-uncertainty-digital-asset-regulation-election-year/>
- Zeadally, S., Adi, E., Baig, Z., & Khan, I. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, 8, 23817-23837. <https://doi.org/10.1109/access.2020.2968045>
- Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys (CSUR)*, 52, 1-34. <https://doi.org/10.1145/3316481>

THE ROLE AND LIMITS OF THE STATE IN THE DIGITAL AGE: AN ANALYSIS OF SECURITY AND GOVERNANCE ELEMENTS REDEFINED BY MODERN TECHNOLOGIES

Extended Abstract

Aim: The aim of this paper is to investigate how modern technologies such as artificial intelligence (AI), big data analytics, and cybersecurity are redefining the state's role in security and governance, emphasizing both the opportunities for enhanced efficiency and proactive threat management, and the critical ethical and privacy challenges they pose, including algorithmic bias, data manipulation, and threats to individual rights.

Artificial intelligence and big data analytics have introduced powerful tools for states to enhance their capabilities in surveillance, threat detection, and risk management. These technologies enable states to act more proactively in anticipating threats and taking appropriate measures to prevent security incidents. However, this level of capability also comes with risks. The use of AI in security raises concerns about bias in decision-making processes, data manipulation, and the potential infringement of individual privacy rights. These ethical challenges are central to the debate about how states should leverage technology while preserving citizens' fundamental freedoms and rights.

The increasing use of digital technologies in governance has fundamentally changed how the state interacts with its citizens. E-government and digital public services have accelerated service delivery, improved efficiency, and made governance processes more transparent. Digital tools such as blockchain and smart contracts have enabled decentralized decision-making, which can reduce bureaucracy and enhance citizen trust in government. However, the adoption of these technologies also raises critical questions about the changing nature of state power, data governance, and accountability.

Method: This study adopts a qualitative and theoretical approach. A literature review was conducted to analyze existing research on the impacts of artificial intelligence, big data analytics, and digital technologies on the state's security and governance capacities. Additionally, a critical assessment was undertaken regarding the ethical and privacy challenges posed by these technologies. The study establishes a theoretical framework to illustrate how digitalization is redefining state mechanisms. An analytical approach was employed in evaluating the data, offering a comprehensive examination of the effects of digital technologies on security and governance processes.

Findings: One of the key arguments of this paper is that digitalization has prompted a reconsideration of traditional governance models, pushing for decentralization and increased public participation. Technologies such as blockchain have the potential to dismantle centralized authority by democratizing access to information and distributing decision-making across multiple stakeholders. This is particularly important in the context of governance, as it reshapes the power dynamics between the state and its citizens. Nonetheless, the transition to digital governance must address issues of digital inequality to ensure that the benefits of technology are accessible to all segments of society.

The state's security mechanisms have also undergone a substantial transformation. Technologies like biometric systems, AI-based surveillance, and enhanced cybersecurity measures have provided new opportunities for improving national security. AI-supported systems allow for faster threat detection and real-time analysis, enhancing public safety and resilience against potential threats. Yet, the use of these technologies has also contributed to the emergence of surveillance states, where governments can monitor individuals extensively, posing risks to individual freedoms. The

balance between enhancing security and protecting privacy is a critical issue that needs careful consideration to avoid creating a "Big Brother" society.

The paper delves into the ethical implications of state-driven surveillance and data collection practices. It highlights the risks associated with large-scale data gathering, including data breaches, potential misuse of sensitive information, and the erosion of privacy. While digital technologies can increase state capabilities, they must be managed ethically to prevent abuses of power. Regulation and governance frameworks must be established to ensure that these technologies are used responsibly and transparently.

Conclusion: To effectively navigate the complexities of the digital age, states must strike a balance between leveraging technological advancements for security and governance while safeguarding citizens' rights and privacy. This paper argues that effective regulatory frameworks are essential to addressing these challenges. Legal standards must be developed to address the nuances of AI, blockchain, and biometric data in state functions. This will not only help mitigate the risks associated with technology but also foster public trust in digital transformation efforts.

The digital age presents both opportunities and challenges for state functions in governance and security. While technologies such as AI, big data, and blockchain have the potential to make governance more efficient and security mechanisms more robust, they also bring significant ethical, privacy, and legal challenges. This paper emphasizes the need for states to rethink their roles and responsibilities in the face of these complexities, ensuring that digital transformation does not come at the cost of fundamental human rights and freedoms. The effective integration of technology into state functions requires a balanced approach that prioritizes transparency, accountability, and inclusivity, while safeguarding individual privacy and dignity.
