YENİ GÜVENLİK PARADİGMASI VE YAPAY ZEKÂ: GÜVENLİ TOPLUM MU, GÖZETİM TOPLUMU MU?

THE NEW SECURITY PARADIGM AND ARTIFICIAL INTELLIGENCE: A SECURE SOCIETY OR A SURVEILLANCE SOCIETY?

Yahya GENÇAY, Canan KATILMIŞ

119

Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
Yıl: 2026, Sayfa: 1-19.

Makale Türü: Araştırma Makalesi

DOI: 10.35379/cusosbil.1695483

Geliş Received: **08.05.2025**
Kabul Accepted: **04.11.2025**

YENİ GÜVENLİK PARADİGMASI VE YAPAY ZEKÂ: GÜVENLİ TOPLUM MU, GÖZETİM TOPLUMU MU?

THE NEW SECURITY PARADIGM AND ARTIFICIAL INTELLIGENCE: A SECURE SOCIETY OR A SURVEILLANCE SOCIETY?

Yahya GENÇAY [1], **Canan KATILMIŞ** [2]

Anahtar Kelimeler:
Yapay Zekâ (YZ),
Güvenlik
Gözetim Toplumu

Keywords:
Artificial Intelligence (AI),
Security,
Surveillance Society

ÖZ

Bu çalışma, yapay zekâ (YZ) çağında güvenlik ve gözetim ilişkisini "güvenlik-gözetim paradoksu" çerçevesinde ele almaktadır. Devletler, ulusal güvenlik ve kamu düzenini sağlamak amacıyla gözetim teknolojilerini kullanırken; özel sektör aktörleri veri temelli uygulamalarla ekonomik kazanç ve davranış manipülasyonu hedeflemektedir. Bu bağlamda, "gözetim toplumu" devlet merkezli gözetimi, "gözetim kapitalizmi" ise özel sektörün veri odaklı gözetim pratiklerini tanımlamaktadır. Çalışmanın amacı, YZ'nin güvenlik alanındaki etkilerini ve bireysel özgürlükler ile demokratik değerler üzerindeki potansiyel risklerini analiz etmektir. Literatür taraması ve kuramsal inceleme yöntemiyle yürütülen çalışmada, YZ uygulamalarının etik ve toplumsal boyutları tartışılmıştır. Bulgular, YZ'nin güvenlik kapasitesini artıran fırsatlar sunduğunu; ancak demokratik denetim ve insan haklarına dayalı yönetişim ile dengelenmediğinde, güvenlik-gözetim paradoksunun gözetim toplumuna doğru kayabileceğini göstermektedir. Bu bağlamda çalışma, YZ çağında güvenliğin sağlanması ile gözetim riskleri arasındaki dengenin önemini vurgulamaktadır.

ABSTRACT

This study examines the relationship between security and surveillance in the age of artificial intelligence (AI) within the framework of the "security-surveillance paradox." While states employ surveillance technologies to ensure national security and public order, private sector actors pursue economic profit and behavioral manipulation through data-driven applications. In this context, the concept of the "surveillance society" refers to state-centered surveillance, whereas "surveillance capitalism" denotes data-oriented surveillance practices by the private sector. The aim of the study is to analyze the impact of AI on the field of security, along with its potential risks to individual freedoms and democratic values. Employing a literature review and theoretical analysis, the study discusses the ethical and societal dimensions of AI applications. The findings indicate that AI offers opportunities to enhance security capacity; however, without democratic oversight and governance grounded in human rights, the security-surveillance paradox may shift toward a surveillance society. Accordingly, the study emphasizes the importance of maintaining a balance between ensuring security and addressing the risks of surveillance in the AI era.

[1] Dr. Öğr. Üyesi, Malatya Turgut Özal Üniversitesi, yahya.gencay@ozal.edu.tr, 0000-0003-1304-2245.

[2] Dr., İnönü Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, canan.katilmis@inonu.edu.tr, 0000-0001-5978-2674.

Alıntılamak için/Cite as: Gencay Y. & Katılmış C. (2026). Yeni Güvenlik Paradigması Ve Yapay Zekâ: Güvenli Toplum Mu, Gözetim Toplumu Mu?, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, s. 1-19.

GİRİŞ

21.yüzyılın ikinci çeyreği, dijitalleşme, yapay zekâ (YZ), büyük veri analitiği ve siber uzayın dönüşümüyle şekillenen; güvenlik kavrayışının köklü biçimde yeniden tanımlandığı bir dönemi işaret etmektedir. Geleneksel güvenlik anlayışı, uzun yıllar boyunca devlet merkezli, askerî odaklı ve ulusal egemenliği temel alan bir bakış açısıyla şekillenmiştir (David & Verbakel, 2022; Buzan, 2015). Ancak küreselleşmenin hızlanması ve teknolojik devrimlerle birlikte bu anlayış, tehdit aktörlerinin çeşitlenmesi ve tehditlerin çok katmanlı, ağ temelli bir yapıya bürünmesi nedeniyle hem analitik hem de pratik düzeyde önemli bir dönüşüm geçirmektedir.

YZ teknolojileri, algoritmik karar alma sistemleri ve sürekli veri toplama uygulamaları, bireylerin yalnızca fiziksel güvenliğini değil, mahremiyetini, ifade özgürlüğünü ve demokratik özerkliğini de tehdit eder hale gelmiştir (Zuboff, 2019; Deibert, 2013). Bu bağlamda, birey artık sadece korunması gereken bir özne değil, sürekli gözetlenen ve kontrol edilen bir nesne konumundadır. Bu durum, güvenlik ve özgürlük ikileminin YZ çağında yeniden düşünülmesini gerekli kılmaktadır.

Çalışma, YZ'nin güvenlik anlayışını nasıl dönüştürdüğünü ve bu dönüşümün demokratik rejimler açısından doğurduğu etik, politik ve toplumsal sorunları analiz etmeyi amaçlamaktadır. Özellikle "güvenlik-gözetim paradoksu" çerçevesinde, devlet merkezli gözetim uygulamalarının ve özel sektörün veri temelli uygulamalarının, güvenlik ile bireysel özgürlükler arasındaki gerilimi nasıl şekillendirdiği incelenmektedir. Çalışmanın temel sorunsalı, "YZ çağında güvenli bir toplum yaratılabilir mi, yoksa güvenlik arayışı daha derin bir gözetim toplumuna mı yol açıyor?" sorusu etrafında yapılandırılmıştır.

Gözetim tartışmalarının düşünsel kökeni, modern dönemin en etkili iki yaklaşımında somutlaşmaktadır: Bentham'ın "panoptikon" modeli ve Foucault'nun "disipliner iktidar" analizi. Bentham, panoptikon mimarisiyle bireylerin görünmeden gözetlenebileceği, bu nedenle kendi davranışlarını sürekli olarak kontrol altında tutacağı bir gözetim düzenini tasvir etmiştir (Bentham, 1995). Foucault ise bu modeli yalnızca hapishane gibi kurumlarla sınırlı görmeyip, modern toplumun genelinde işleyen disiplin ve iktidar ilişkilerinin bir metaforu olarak ele almış, gözetimi toplumsal kontrolün merkezine yerleştirmiştir (Foucault, 1995). Bu kuramsal miras, gözetim toplumunu devlet merkezli ve disipliner pratikler bağlamında açıklarken; dijital çağda gözetim kapitalizmi (Zuboff, 2019) bireylerin ekonomik çıkarlar doğrultusunda veri temelli olarak denetlenmesiyle yeni bir boyut kazanmıştır. Dolayısıyla çalışmanın kuramsal çerçevesi, Bentham ve Foucault'dan başlayarak günümüzde YZ ve büyük veri teknolojilerinin dönüştürdüğü gözetim-güvenlik ilişkilerini anlamaya yönelmektedir.

Araştırma yöntemi olarak nitel bir yaklaşım benimsenmiş; literatür taraması ve kuramsal analiz aracılığıyla YZ ve gözetim teknolojilerinin güvenlik politikalarına etkisi değerlendirilmiştir. Çalışmada, güvenlik ve yapay zekâ literatüründe öne çıkan çalışmalar sistematik biçimde incelenmiştir. Kuramsal çerçeve oluşturulurken geleneksel ve eleştirel güvenlik kuramları, gözetim toplumu (Lyon, 2007) ve gözetim kapitalizmi (Zuboff, 2019) yaklaşımları ile Foucault ve Bentham'ın erken eleştirel perspektiflerinden yararlanılmıştır. Böylece çalışmada, hem kavramsal hem de güncel örnekler üzerinden güvenlik–gözetim paradoksu çok boyutlu bir analizle ele alınmıştır.

Çalışma, YZ çağında güvenlik söylemlerinin yalnızca koruma değil, aynı zamanda kontrol boyutunu da içerdiğini ve bu durumun bireysel haklar ile güvenlik politikalarının doğasında paradoksal bir kırılma yarattığını göstermeyi hedeflemektedir. Bu yönüyle çalışma, güvenlik-gözetim paradoksunu YZ çağında sistematik olarak irdeleyerek, literatürdeki kuramsal tartışmalara hem kavramsal hem de eleştirel bir katkı sunmaktadır.

GÜVENLİK KAVRAMI VE TARİHSEL GELİŞİMİ

Güvenlik, çok boyutlu bir kavram olup psikoloji, sosyoloji, hukuk, finans, bilgi teknolojileri, savunma ve kamu yönetimi gibi birçok disiplini ilgilendiren geniş kapsamlı bir inceleme alanı sunmaktadır. Bireylerin, toplulukların ve devletlerin varlıklarını sürdürme ihtiyacından doğan bu kavram, hem bireysel hem de kolektif davranışları şekillendiren temel bir unsurdur.

Modern dönemde güvenlik kavramı, özellikle siyasal söylemlerde esnek ve çok anlamlı bir içerik kazanmıştır.

Türkçedeki "güvenlik" kelimesi, "inanmak" anlamındaki "küven" kökünden gelirken; Batı dillerindeki karşılığı olan "securitas", Latince "kaygısızlık" anlamına gelen *se-curus* kökünden türetilmiştir. Bu kavram, zamanla bireyin iç huzurundan daha fazlasını ifade ederek toplumsal ve siyasal düzenle ilişkilendirilmiştir (Nişanyan, 2009; Liddell & Scott, 1940).

Securitas, siyasal anlamda ilk kez Romalı filozof Cicero tarafından sistematik olarak kullanılmıştır. Cicero, bu kavramı "aklın sükûneti, korkunun ve endişenin yokluğu" olarak tanımlarken; onun bireysel olduğu kadar kamusal bir içeriğe sahip olduğunu da göstermiştir. Nitekim *Pax Romana* döneminde *securitas*, hem bireysel yaşamın hem de kamu düzeninin teminatı olarak görülmüştür (Cicero, 1999).

Modern güvenlik anlayışı ise, Thomas Hobbes ile kurumsallaşmıştır. Hobbes, *Leviathan* adlı eserinde güvenliği, doğa durumunun anarşik ortamından çıkışın ve siyasal toplumun inşasının temel güdüsü olarak tanımlamaktadır. Güvenliğin, bireylerin hayatlarını korumak için kolektif bir otoriteyi kabul etmeleriyle sağlandığını savunmaktadır. Bu düşünce çizgisi, İbn Haldun'da da benzer şekilde görülmektedir. İbn-i Haldun bireylerin doğası gereği çatışmaya yatkın olduğunu ve güvenliğin ancak bir otorite altında sağlanabileceğini belirtmiştir (Hobbes, 1992, Haldun, 2004).

Machiavelli (2005), Bodin (2008) ve Hobbes (1992) gibi düşünürler güvenliği güçlü otoriteyle ilişkilendirirken, Locke (2002), Rousseau (2004), Montesquieu (1998) ve Mill (2008) gibi isimler özgürlükle tamamlayıcı bir ilişki içinde değerlendirmiştir. Özellikle Locke (2002), devletin sınırsız bir güçle donatılmasına karşı çıkarak bireysel hakların güvence altına alınması gerektiğini vurgulamıştır.

Modern siyaset felsefesi; eşitlik, hak ve adalet gibi kavramları derinlemesine ele almış olsa da güvenlik kavramı üzerine yapılan felsefi analizlerin daha sınırlı olduğu görülmektedir. Bu bağlamda, güvenlik anlayışının kuramsal gelişimine siyaset felsefecileri önemli katkılar sunmuş olmakla birlikte, kavramın sistematik olarak ele alınışı daha sonraları uluslararası ilişkiler disiplini içerisinde gelişmiştir. Bu çerçevede güvenlik, bir ulusun kendisini dış tehditlere karşı koruma, ulusal çıkarlarını muhafaza etme ve halkının refahını sağlama kapasitesine işaret etmektedir. Güvenlik, yalnızca fiziksel korumayı değil, aynı zamanda ekonomik, toplumsal ve siyasal istikrarı da kapsamaktadır.

Ogaba (2010) güvenliği, bir ülkenin temel kurumlarını sürdürebilme, sosyo-politik hedeflerine ulaşabilme, iç uyumu zayıflatacak tehditleri bertaraf edebilme ve halkın meşru beklentilerini karşılayabilme yeteneği olarak tanımlamaktadır. Bu tanım, güvenliğin yalnızca bir savunma refleksi olmadığını, aynı zamanda bir kapasite ve meşruiyet meselesi olduğunu vurgulamaktadır. Wolfers (1962) ise, güvenliğin iki yönüne dikkat çekmektedir. Nesnel anlamda güvenlik, edinilmiş değerlere yönelik tehditlerin yokluğu; öznel anlamda ise bu değerlere saldırı korkusunun hissedilmemesi halidir. Ona göre güvenlik ve güvensizlik, hem ulusal hem de kurumsal düzeyde tehditler ve kırılganlıklar çerçevesinde şekillenmektedir.

Farklı düşünürler güvenliği değişen bağlamlarda ele almıştır. Bellany (1981) savaşsızlıkla, Lippmann (1943) direnme kapasitesiyle, Luciani (1989) dış tehditlere karşı koyma becerisiyle tanımlarken; Ullman (1983) bir aktörün politika üretme kapasitesini tehdit eden durumların yokluğu olarak tanımlamaktadır. Martin (1983) ise güvenliği gelecekteki refahın teminatı olarak görmektedir.

Sosyal inşacı yaklaşım güvenliği maddi tehditlerden çok, kimlikler, değerler ve normlarla şekillenen bir toplumsal süreç olarak ele almaktadır (Wendt, 1992; Adler, 1997). Bu çerçevede güvenlik, öznel bir anlam taşır ve aktörlerin algılarına göre inşa edilir. Booth'a (1997) göre güvenlik, bireylerin potansiyellerini gerçekleştirmesini engelleyen tüm kısıtların kaldırılmasıdır. Kolodziej (2005) ise güvenliği, tehditlerin işbirliği fırsatına dönüştüğü bir ikna süreci olarak değerlendirmektedir.

Sonuç olarak, güvenlik kavramı tarihsel olarak sürekli evrilmiş; bireylerin iç huzurundan ulusların bekasına, maddi tehditlerden toplumsal değerlerin korunmasına uzanan çok katmanlı bir yapıya bürünmüştür. Bu çok boyutluluk, güvenliğin sabit değil, sürekli yeniden tanımlanan ve algılarla şekillenen bir kavram olduğunu ortaya koymaktadır.

Güvenlik Anlayışının Kuramsal Dönüşümü

Güvenlik anlayışları tarihsel olarak, devletlerin askeri kapasitesi ve güç politikaları üzerinden şekillenmiş ve devletin varlığının korunması, geleneksel güvenlik paradigmasında en önemli hedef olarak kabul edilmiştir. 20. yüzyılın ortalarına kadar güvenlik, çoğunlukla askeri tehditler, güç dengesi ve sınırların korunması ile ilişkilendirilmiştir (Herz, 1950). Geleneksel güvenlik anlayışı, devlet merkezli bir bakış açısını benimseyerek, sadece askeri tehditlere odaklanmış ve güvenlik, bu tehditlere karşı devletin savunma kapasitesini artırma çabalarıyla sınırlı tutulmuştur.

Bu dönemde güvenliğin doğası, bazı erken eleştirel perspektifler tarafından da sorgulanmıştır. Jeremy Bentham, "panoptikon" fikri ile gözetim ve disiplin mekanizmalarının hem bireylerin hem de toplumların davranışlarını nasıl şekillendirdiğini tartışmış, devletin güvenliği sağlama işlevinin aynı zamanda kontrol ve denetim boyutu taşıdığını göstermiştir (Bentham, 1791/1995). Michel Foucault ise, modern devletin iktidar pratikleri çerçevesinde güvenliği ve gözetimi ele almış; "disiplin toplumları ve biyopolitik" yaklaşımıyla, güvenlik ile kontrol arasındaki ilişkileri analiz etmiştir (Foucault, 1995). Bu düşünceler, güvenlik çalışmalarına erken bir eleştirel boyut kazandırmış ve sonraki eleştirel güvenlik kuramcıları için kuramsal bir zemin oluşturmuştur.

Geleneksel güvenlik anlayışının dönüşümü ve eleştirel güvenlik çalışmaları, özellikle küreselleşme ile birlikte devlet sınırlarının giderek daha belirsiz hale gelmesi; ekonomik, çevresel, kültürel gibi çeşitli faktörlerin güvenlik tehditlerini etkilemesine yol açması ile gelişme göstermiştir. Küreselleşme, devlet sınırlarını aşan ekonomik, çevresel ve kültürel etkileşimleri artırırken, güvenlik tehditlerini sadece askeri alanda değil, aynı zamanda toplumsal yapıları tehdit eden çok daha karmaşık dinamiklerle şekillendirmiştir.

Özellikle 20. yüzyılın ikinci yarısından sonra, devletler arasındaki askeri çatışmaların yanı sıra, küresel ölçekteki ekonomik krizler, çevresel değişimler ve sağlık tehditleri gibi yeni güvenlik sorunları gündeme gelmiştir. Küreselleşme, güvenliği sadece devlet odaklı bir güvenlik anlayışında öteye taşıyarak; ekonomik, siyasal, toplumsal ve çevresel güvenliği de güvenlik literatürüne dâhil etmiştir. Artan ekonomik bağımlılıklar, çevresel felaketler, terörizm ve pandemiler gibi transnasyonal tehditler, geleneksel güvenlik paradigmasını sorgulatmış ve daha geniş bir güvenlik anlayışına duyulan ihtiyacı ortaya koymuştur. Küreselleşmenin etkisiyle, ulusal güvenlik sadece askeri tehditler ile değil, aynı zamanda ticaret yollarının güvenliği, doğal kaynakların korunması ve çevre felaketlerinin önlenmesi gibi unsurlarla da ilişkilendirilmiştir. Bu süreç, geleneksel güvenlik anlayışlarının dar sınırlarını aşarak, çok daha geniş bir güvenlik anlayışının gelişmesine olanak sağlamıştır (Poku & Graham 2000).

Bu bağlamda geleneksel güvenlik anlayışına yönelik eleştiriler, özellikle Soğuk Savaş sonrası dönemde daha da güçlenmiştir. Eleştirel güvenlik yaklaşımları, güvenliğin yalnızca askeri tehditlerle sınırlı bir olgu olarak görülmemesi gerektiğini savunmuş ve güvenlik anlayışlarını daha geniş, toplumsal ve bireysel boyutlara taşıyarak güvenliğin çok yönlü bir mesele olduğunu ortaya koymuştur (Krause & Williams, 1997). Bu perspektife göre, güvenlik sadece devletin askeri varlığını koruma çabası değil; bireylerin, toplumların ve toplumsal yapıların güvenliğini de içeren bir olgudur. Eleştirel güvenlik anlayışı, güvenliği sübjektif bir olgu olarak ele almış, toplumsal eşitsizlikler, ekonomik adaletsizlikler, kültürel çatışmalar ve çevresel tehditler gibi unsurları da güvenlik tehditleri olarak tanımlamıştır (David & Verbakel, 2022).

Eleştirel güvenlik anlayışının en önemli katkısı bu bağlamda güvenlik kavramının genişletilmesidir. Krause ve Williams, güvenliği bireylerin yaşam koşulları, toplumsal normlar ve ekonomik eşitsizlikler gibi unsurlarla ilişkilendiren bir perspektiften ele almıştır. Güvenliğin yalnızca devletin gücüyle ölçülemeyeceği, bireylerin ve toplumların güvenliğiyle de ilgisi olduğu ifade edilmiştir (Krause & Williams, 1997). Eleştirel güvenlik çalışmalarına sınırlı fakat önemli bir katkı sağlayan Ayoob (1997) ise, güvenlik çalışmalarının yalnızca devletin bekasına odaklanmasının yeterli olmayacağını öne sürerken, bu yaklaşımı "subaltern realist" bir çerçevede ele almıştır. Devleti tek referans nesnesi olarak kabul eden geleneksel güvenlik anlayışını sorgulayan Ayoob, güvenlik ve güvensizliği; hem iç hem de dış kaynaklı olmak üzere,

bölgesel ve kurumsal devlet yapıları ile rejimleri tehdit eden veya zayıflatma potansiyeline sahip unsurlarla ilişkilendirerek tanımlamaktadır.

Eleştirel güvenlik çalışmalarına önemli katkılarından bir diğeri Barry Buzan'ın güvenliği farklı sektörler çerçevesinde analiz etmeye olanak tanıyan kuramsal bir çerçeve geliştirmesidir. Bu yaklaşım, özellikle Kopenhag Okulu'nun güvenlik kuramı içinde ele alınmakta ve güvenlik olgusunun sadece askeri tehditlerle sınırlı olmadığını savunmaktadır. Güvenliği, çok boyutlu ve disiplinler arası bir alan olarak görmektedir. Sektörel analiz, devlet dışı aktörlerin, bireylerin ve toplumların da güvenliğin referans nesnesi olabileceğini savunarak, güvenlik çalışmalarında paradigmatik bir dönüşümün önünü açmıştır. Buzan, devletlerin askeri kapasitesinin ötesinde, çevresel felaketler, sosyal eşitsizlikler ve ekonomik krizler gibi küresel tehditlerin güvenlik siyaseti açısından dikkate alınması gerektiğini savunmaktadır. Bu yaklaşım, devletler arasındaki askeri çatışmaların yanı sıra, transnasyonal tehditleri de güvenlik tehditleri olarak ele alarak güvenlik anlayışının çok boyutlu hale gelmesine olanak tanımıştır (Buzan ve diğerleri, 1998).

Geleneksel güvenlik anlayışının bu dönüşümü, küreselleşme, yeni güvenlik tehditlerinin yükselmesi ve eleştirel güvenlik yaklaşımlarının etkisiyle daha geniş, kapsayıcı bir perspektife evrilmiştir. Bu dönüşüm, güvenliği yalnızca askeri tehditlerle sınırlamayan, aynı zamanda bireylerin, toplumların ve çevrenin güvenliğini de gözeten çok boyutlu bir anlayışa yöneltmiştir. Küresel tehditlerin doğası, devletlerin geleneksel güvenlik paradigmalarındaki rollerini sorgulatarak, güvenlik anlayışının daha kapsamlı ve dinamik bir hale gelmesini sağlamıştır. Bu bağlamda, eleştirel güvenlik yaklaşımları, güvenlik kavramının genişletilmesi ve çoklu tehdit unsurlarının dikkate alınması gerektiğini ortaya koymuş ve güvenlik teorilerine yeni bir derinlik kazandırmıştır.

Teknolojik Dönüşüm ve Yeni Güvenlik Paradigması

Güvenliğin sağlanmasında devletin tekelinin sarsılması, küreselleşmeden ve teknolojik gelişmelerin güvenlik alanını dönüştürmesinden bağımsız değildir. Dupont (2007), güvenlik alanındaki iktidar mücadelelerini analiz ederek, özellikle siber güvenlik gibi yeni alanların, güvenlik hizmetlerinin yalnızca devletin tekelinde kalamayacağı bir yapı yarattığını ortaya koymuştur. Güvenliğin sağlanmasında bilgi teknolojilerinin kullanımı, devlet-dışı aktörlerin etkisini artırmakta ve böylece geleneksel egemenlik anlayışını yeniden tanımlamaktadır. Bu durum, yalnızca güvenlik politikalarının uygulama düzeyinde değil, aynı zamanda demokratik hesap verebilirlik ve şeffaflık ilkeleri açısından da derin bir dönüşümü anlamına gelmektedir. Eleştirel güvenlik çalışmaları açısından bu dönüşüm, güvenlik alanında kimlerin yetkiye sahip olduğu, hangi tehditlerin tanımlandığı ve bunların kimin çıkarına hizmet ettiğine dair soruları ön plana çıkarmaktadır.

Louise Amoore (2013), *The Politics of Possibility* adlı çalışmasında, günümüz güvenlik politikalarının yalnızca mevcut tehditlere değil, henüz gerçekleşmemiş fakat olası tehdit senaryolarına göre yapılandığını göstererek geleneksel güvenlik anlayışının ötesine geçmektedir. Amoore'a göre, YZ temelli algoritmalar, büyük veri analizleri ve tahminsel modellemeler artık güvenlik politikalarının temel belirleyicisi haline gelmiştir. Bu yaklaşım, devletlerin ve kurumların bireyleri, toplulukları veya hareketleri önceden riskli olarak sınıflandırmasına imkân verirken, güvenliğin öznesi ve nesnesi üzerinde ciddi etik ve politik etkiler yaratmaktadır. Böylece güvenlik, geçmişin değil, "geleceğin hesaplanabilirliği" üzerine kurulu, sürekli tetikte olmayı dayatan bir yönetsel rejime dönüşmektedir.

Bu noktada, söz konusu yönetsel rejimin pratikte nasıl işlediğini anlamak için gözetim kavramına yönelmek önemlidir. Devlet merkezli gözetim uygulamaları, David Lyon'un (2007) "gözetim toplumu" yaklaşımı çerçevesinde ele alınabilir. Lyon'a göre, devletler kamu düzeni, ulusal güvenlik ve vatandaş davranışlarını izleme amacıyla gözetim teknolojilerini kullanmaktadır; bu uygulamalar genellikle merkezi ve kamusal güvenlik odaklıdır.

Öte yandan, Shoshana Zuboff'un (2019) "gözetim kapitalizmi" kavramı, özel sektör aktörlerinin (Google, Facebook vb.) veri temelli gözetim uygulamaları aracılığıyla ekonomik çıkar elde etmesini vurgulamaktadır. Zuboff'un ortaya koyduğu model, sadece ekonomik değil, aynı zamanda siyasal güvenliğe dair yeni tehditlerin de

habercisidir. Dijital platformların bireyleri sistematik biçimde izleme kapasitesi, mahremiyetin ötesinde bireysel özerklik ve demokratik denetim mekanizmaları üzerinde ciddi riskler oluşturmaktadır. Böylece güvenlik, yalnızca fiziksel tehditler değil, dijital manipülasyon, veri tekelleşmesi ve algoritmik yönlendirme gibi yapısal tehditleri de kapsayan bir boyuta taşınmaktadır.

Dijital teknolojilerin güvenlik algısını nasıl dönüştürdüğünü anlamak için Ronald Deibert'in *Black Code* adlı çalışması da önemli bir referans kaynağıdır. Deibert (2013), dijital alanın yalnızca iletişim veya ticaret mecrası olmadığını, aynı zamanda küresel gözetim ağlarının ve siber istihbarat faaliyetlerinin merkezi haline geldiğini ortaya koymaktadır. Özellikle devlet destekli dijital gözetim programlarının yaygınlaşmasının, bireysel mahremiyetin ötesinde siyasal muhalefeti bastırma ve vatandaş davranışlarını şekillendirme araçları haline geldiğini ifade etmektedir. YZ destekli gözetim mekanizmaları, yalnızca teknolojik değil, aynı zamanda politik güç ilişkilerinin dijitalleştirilmiş uzantıları olarak değerlendirilmelidir.

C.A.S.E. Collective (2006), güvenliğin yalnızca maddi tehditlerle değil, aynı zamanda toplumsal, söylemsel ve normatif süreçlerle şekillendiğini ileri sürerek, güvenlik çalışmalarına disiplinlerarası ve eleştirel bir yön kazandırmaktadır. Özellikle teknolojik tehditlerin "doğal" değil, söylemler aracılığıyla "inşa edilmiş" olduğu varsayımı, dijital teknolojilerin güvenlik politikalarıyla nasıl bütünleştirildiğini analiz etmede önemli bir çerçeve sağlamaktadır.

Lucas Kello (2013) da siber devrimin geleneksel uluslararası ilişkiler kuramlarının öngörmediği "ara formlar" yarattığını savunarak, bu alandaki teorik açığı vurgulamaktadır. Ona göre ne tamamen savaş ne de barış olarak tanımlanabilen siber eylemler, devlet dışı aktörlere stratejik dengeyi etkileyebilecek ölçekte güç kazandırmaktadır.

Siber güvenlik, geleneksel güvenlik anlayışının ötesine geçerek devlet, birey ve özel sektör üçgeninde yeniden tanımlanmakta; bu durum, teknolojinin güvenlik üzerindeki dönüştürücü etkisini açıkça ortaya koymaktadır. Singer ve Friedman (2014), siber güvenliğin artık yalnızca teknik uzmanların değil; siyaset yapıcıların, şirket yöneticilerinin ve bireylerin sorumluluk alanına girdiğini vurgulamaktadır. Myriam Dunn Cavelty (2008) ise siber güvenliğin bir güvenlik sorunu olarak nasıl "inşa edildiğini" detaylı biçimde ele almakta ve sürecin yalnızca teknolojik değil, siyasi ve ideolojik tercihlerle şekillendiğini göstermektedir.

Sonuç olarak, güvenlik kavramı, tarihsel olarak askeri tehditler ve devlet merkezli risk algıları çerçevesinde şekillenmiş olsa da, günümüzde siber güvenlik ve YZ gibi gelişmelerle birlikte çok boyutlu, öznelerarası ve teknolojik bir niteliğe bürünmüştür. Geleneksel güvenlik yaklaşımı bu yeni tehdit türlerini anlamakta ve yönetmekte yetersiz kalırken, eleştirel güvenlik kuramları, bu karmaşık ve çoğul güvenlik alanlarını açıklamada daha kapsayıcı bir perspektif sunmaktadır. Güvenliğe dair analizlerin sadece güç dengesi ve askeri kapasite üzerinden değil, aynı zamanda teknolojinin politik etkileri, etik sınırları ve toplumsal sonuçları üzerinden yapılması gerekliliği açıktır. Güvenlik artık sadece korunmak değil, aynı zamanda kimin, neye karşı ve ne pahasına korunacağı sorularını da kapsayan derinlemesine bir siyasal meseleye dönüşmüştür.

YAPAY ZEKÂ VE GÜVENLİK

YZ, günümüz dijital çağının şekillenmesinde merkezi bir konuma sahip olup, modern teknolojik gelişmelerin kritik unsurlarından biri olarak öne çıkmaktadır. İnsan zekâsını taklit edebilen ve karmaşık görevleri özerk biçimde yerine getirebilen bu sistemler, yalnızca bilimsel araştırmaların ilerlemesine katkı sağlamakla kalmamakta, aynı zamanda toplumsal yaşamın işleyişinde de dönüştürücü bir rol oynamaktadır. YZ'nin temelinde yatan varsayım, basit ve rutin işlemleri aşarak insan benzeri muhakeme gücü ve bilişsel yetenek gerektiren karmaşık görevlerin de makineler aracılığıyla gerçekleştirilebileceği fikridir. Bu niteliği sayesinde YZ, günümüzde sosyoekonomik dönüşümün başlıca itici güçlerinden biri olarak kabul edilmektedir (Jiang ve diğerleri, 2022).

Literatürde YZ farklı açılardan tanımlanmaktadır. Zhang ve Dafoe (2019, s. 5), insan zekâsı gerektiren işlevleri gerçekleştirebilen ve bağımsız kararlar alabilen bilgisayar sistemleri olarak tanımlarken; Galloway ve Swiatek (2018, s. 734), YZ'yi duyma ve öğrenme gibi becerileri makinelere kazandıran gelişmiş teknolojilerin bütünü

şeklinde tanımlamaktadır. Russell ve Norvig (2010, s. 4), YZ'yi "belirsizlik koşullarında en iyi sonucu elde etmeye çalışan mantıklı ajanlar" üzerinden kavramsallaştırırken; Scherer (2016, s. 359), insan tarafından yapıldığında zekâ gerektirdiği kabul edilen görevleri yerine getirebilen makineler olarak ifade etmektedir. Bu farklı yaklaşımlar ışığında YZ, insan zekâsının bilişsel işlevlerini taklit eden; öğrenme, akıl yürütme ve karar verme süreçlerini özerk biçimde gerçekleştirebilen teknolojik bir sistem olarak değerlendirilebilir.

Bu kavramsal çerçeve, YZ'nin güvenlik alanındaki etkilerini anlamak açısından da önemlidir. Çünkü YZ'yi mümkün kılan temel teknolojiler, güvenlik uygulamalarının dönüşümünde belirleyici bir rol oynamaktadır. Örneğin makine öğrenimi, büyük veri kümelerinden öğrenerek sınıflandırma, tahmin ve analiz yapabilen algoritmalar bütünü olup; ses tanıma, görüntü tanıma ve tavsiye sistemleri gibi geniş kullanım alanlarına sahiptir (Russell & Norvig, 2010). Diğer bir teknoloji olan yapay sinir ağları, biyolojik sinir sisteminden esinlenerek geliştirilmiş yapılardır. Bunların çok katmanlı versiyonu olan derin öğrenme, doğruluk ve verimliliği artırarak günlük yaşamı kolaylaştıran teknolojilerin temelini oluşturmaktadır (Mondal, 2020). Robotik ise; algılama, hareket etme ve karar verme yeteneklerini bir araya getirerek farklı sektörlerde uygulanmakta, YZ'nin fiziksel dünyadaki etkisini pekiştirmektedir. Bu teknolojilerin bütüncül işlevi yalnızca teknik alanlarla sınırlı kalmamaktadır. Sosyal bilimlerdeki araştırmalara da yeni açılımlar sunarak YZ'nin güvenlik bağlamındaki çok yönlü karakterini ortaya koymaktadır.

YZ, güvenlik paradigmalarını köklü bir şekilde dönüştürerek iç güvenlikten siber savunmaya, askeri uygulamalardan ulusal güvenlik politikalarına kadar geniş bir yelpazede yenilikçi çözümler sunmaktadır. Büyük veri analitiği, makine öğrenimi ve otonom sistemler gibi YZ teknolojileri, tehdit algılama, kriz yönetimi ve stratejik karar alma süreçlerinde hız, hassasiyet ve verimlilik artışı sağlarken, aynı zamanda etik, hukuki ve mahremiyetle ilgili ciddi tartışmaları gündeme getirmektedir. YZ'nin çift kullanımlı doğası, bu teknolojinin hem sivil hem de askeri alanlarda yaygınlaşmasını hızlandırarak uluslararası rekabet yoluyla yeni bir güvenlik çağını şekillendirmektedir. Ancak bu dönüşüm, teknolojik fırsatlar kadar mahremiyet ihlalleri, algoritmik önyargılar ve etik hesap verebilirlik gibi sorunları da beraberinde getirmektedir.

Dolayısıyla YZ, güvenlik uygulamalarında yalnızca teknik kapasitesiyle değil, toplumsal, hukuki ve siyasal boyutlarıyla da bütüncül biçimde ele alınmalıdır. Yüksek işlem gücü, eksik verilerden genelleme yapabilme yeteneği ve değişken koşullara uyum sağlayarak esnek kararlar alma kapasitesi, YZ'yi güvenlik alanında aktif bir aktör konumuna taşımaktadır. Veri temelli karar alma mekanizmaları ve insan davranışlarını modelleme kabiliyeti, bireylerin günlük yaşamlarını şekillendirmenin ötesine geçerek devlet-toplum ilişkilerinde köklü dönüşümlere yol açabilmektedir. Bu bağlamda yüz tanıma sistemleri gibi uygulamaların, güvenlik süreçlerini optimize ederken aynı zamanda mahremiyet ve adalet konularında yeni tartışmalar doğurduğu ifade edilebilir. Böylece YZ, yalnızca teknolojik bir yenilik olmanın ötesinde, gücün merkezileşmesi, karar alma süreçlerinin otomatikleşmesi ve bireysel özerkliğin yeniden tanımlanması gibi boyutlarıyla paradigmatik bir değişimi temsil etmektedir.

Bu genel çerçeve doğrultusunda, YZ'nin güvenlik üzerindeki etkileri farklı düzlemlerde ele alınabilir. YZ destekli güvenlik sistemleri, suç önleme, gözetim ve kriz yönetimi alanlarında yeni imkânlar sunmaktadır. YZ destekli askeri ve ulusal güvenlik uygulamaları, otonom silah sistemlerinden istihbarat analizine kadar stratejik avantajlar sağlamaktadır. YZ destekli siber güvenlik, tehdit algılama ve savunma mekanizmalarında kritik bir rol üstlenmektedir. Son olarak, YZ'nin güvenlik kapasitesi ve sınırlamaları, etik, hukuki ve teknik sorunların merkezinde yer almakta ve kapsamlı bir değerlendirme gerektirmektedir.

Yapay Zekâ Destekli Güvenlik Sistemleri

YZ destekli güvenlik sistemleri, geleneksel yöntemleri aşarak daha hızlı, verimli ve proaktif bir güvenlik anlayışı geliştirmektedir. Bu sistemler, yüz tanıma teknolojilerinden tahmine dayalı polisliğe, kriz yönetiminden uluslararası işbirliklerine kadar çok çeşitli alanlarda uygulanmaktadır. YZ destekli güvenlik sistemlerinin en yaygın uygulamalarından biri, kamusal alanlarda kullanılan yüz tanıma teknolojileridir. Bu sistemler, biyometrik verilerden

yararlanarak havaalanları, tren istasyonları ve büyük etkinlik alanları gibi yoğun bölgelerde gerçek zamanlı birey tanımlama görevini üstlenmektedir. Çin, ABD ve birçok Avrupa ülkesi, kamuya açık alanlarda yüksek çözünürlüklü kameralarla entegre çalışan yüz tanıma teknolojilerini geniş çapta kullanmaktadır. Örneğin, Çin'de 176 milyon kameradan oluşan bir ağ, yüz tanıma teknolojileriyle entegre edilerek vatandaşların hareketlerini izlemekte ve sosyal puanlama sistemiyle toplumsal kontrolü güçlendirmektedir (Ay & Sezer, 2019, s. 127).

Yüz tanıma teknolojilerinin ötesinde, YZ'nin büyük veri analitiği ve makine öğrenimi algoritmalarıyla desteklediği tahmine dayalı polislik modelleri, suç önleme stratejilerini dönüştürmektedir. Kolluk kuvvetleri, geçmiş suç verilerini analiz ederek suçun meydana gelme olasılığı olan bölgeleri belirlemekte, kaynak planlamasını buna göre şekillendirmektedir (Lyon, 2019; Radulov, 2019). Bu uygulamalarda kullanılan algoritmalar, büyük veri kümeleri üzerinden örüntü tespiti yapmakta ve bu yolla potansiyel suçlu profillerini ortaya çıkarmaktadır. ABD'de kullanılan "PredPol" uygulaması, suç türü, yeri ve zamanı hakkındaki verileri analiz ederek tahmine dayalı algoritmalarla çalışmakta ve kolluk kuvvetlerinin kaynaklarını daha etkin kullanmasını sağlamaktadır (Çiçek, 2025, s. 57). Türkiye'de ise ASENA yazılımı, milyonlarca veriyi birleştirerek uyuşturucu ve diğer suç unsurlarını tespit etmekte, kolluk kuvvetlerinin suç önleme kapasitesini artırmaktadır (Yalçın, 2024, s. 194). Bu tür tahmine dayalı analizler, veri kaynaklarının çeşitliliği ve kalitesi kadar, algoritmaların nasıl eğitildiği ve hangi kriterlerle çalıştığı da güvenliğin etkinliğini ve etik sınırlarını belirleyen önemli unsurlardır (Crawford, 2021).

Tahmine dayalı polislik, YZ'nin suç önlemedeki rolünün yalnızca bir yönünü oluştururken, terörle mücadele ve kriz yönetiminde gerçek zamanlı tehdit analizi, bu teknolojilerin daha geniş bir güvenlik bağlamında nasıl işlediğini göstermektedir. Doğal dil işleme algoritmaları, sosyal medya platformlarındaki verileri analiz ederek nefret söylemi veya çocuk istismarı gibi suç içeriklerini otomatik olarak kategorize etmekte ve kolluk kuvvetlerinin hızlı müdahalesini sağlamaktadır (Hälterlein, 2023). YZ tabanlı video gözetim sistemleri ise, şüpheli davranışları veya tehlikeli nesneleri tespit ederek, kamusal alanlarda güvenliği güçlendirmektedir. Örneğin, CCTV (Closed-Circuit Television) görüntüleriyle entegre YZ sistemleri, silahları tanımlayabilir ve duruşları analiz ederek şüpheli etkinlikleri tespit edebilmektedir (Kanat & Akoğuz, 2024).

YZ'nin güvenlik alanındaki etkisi, yalnızca yerel ve ulusal düzeyle sınırlı kalmayıp küresel güvenlik politikalarını da derinden dönüştürmektedir. YZ teknolojileri, sınır güvenliği, uluslararası işbirlikleri ve diplomatik stratejilerin yeniden şekillendirilmesinde önemli bir rol oynamaktadır. Avrupa Birliği'nin Frontex kurumu, YZ destekli analitik ve operasyonel yetenekleri kullanarak, sınır güvenliğini güçlendirmekte ve göçmen takibi süreçlerini daha etkin bir şekilde yönetmektedir. Bu teknolojiler, büyük veri analitiği ve gerçek zamanlı izleme sistemleri sayesinde sınır bölgelerindeki hareketliliği izlemek, potansiyel tehditleri tespit etmek ve göçmen akımlarını koordine etmek için kullanılmaktadır (Fischer & Wenger, 2021). Uydu görüntüleri ve biyometrik pasaport sistemleri gibi teknolojiler de, sınır yönetimi ve uluslararası güvenlik işbirliklerinde vazgeçilmez araçlar hâline gelmiştir (Hälterlein, 2023).

YZ destekli güvenlik sistemleri, yüz tanıma teknolojilerinden tahmine dayalı polisliğe, kriz yönetiminden küresel güvenlik politikalarına kadar geniş bir uygulama yelpazesinde güvenlik kapasitesini artırmaktadır. Gerçek zamanlı tehdit analizi ve veri odaklı karar alma mekanizmaları, proaktif bir güvenlik paradigmasını desteklemektedir.-

Yapay Zekâ Destekli Askeri-Ulusal Güvenlik Uygulamaları

YZ, askeri ve ulusal güvenlik alanlarında dönüştürücü bir rol oynayarak, stratejik üstünlük arayışındaki devletlerin savaş, istihbarat ve gözetim pratiklerini yeniden şekillendirmektedir. Otonom silah sistemlerinden büyük veri analitiğine, YZ destekli teknolojiler, operasyonel hız, hassasiyet ve karar alma süreçlerinde önemli avantajlar sunmaktadır.

Otonom silahlar, insan müdahalesi olmadan hedef seçme ve angajman yeteneğine sahip sistemlerdir. Hedef tanıma özellikli dronlar ve robotik tanklar gibi otonom silahlar askeri güvenlikte önemli avantajlar getirmektedir (Bilgin,

2024). Türkiye'nin Bayraktar İHA ve SİHA'ları gibi YZ destekli sistemler, daha küçük devletlerin bile hassas vuruş kabiliyetlerini artırarak asimetrik avantajlar göstermelerini sağlamaktadır (Kanat & Akoğuz, 2024). Bu sistemler, insan operatörlerin risklerini azaltırken, hızlı karar alma ve yüksek isabet oranıyla stratejik üstünlük sunmaktadır (Darici, 2020).

İstihbarat toplama ve analizinde de YZ, büyük veri analitiği ve sinyal istihbaratı gibi alanlarda benzersiz avantajlar sunmaktadır. YZ algoritmaları, farklı formatlardaki verileri (uydu görüntüleri, iletişim kayıtları) birleştirerek anormallikleri tespit edebilmekte ve operasyonel karar alma süreçlerini hızlandırabilmektedir (Bilgin, 2024). Örneğin, ABD'nin Maven Projesi, Irak ve Suriye'deki hedefleri belirlemek için YZ tabanlı görüntü analizi kullanmakta, analistlerin saatler süren manuel incelemelerini dakikalara indirmektedir (Hoadley & Lucas, 2018). Çin'in "Yeni Nesil YZ Gelişim Planı" ise, YZ'yi istihbarat, ortak harekât resmi oluşturma ve hızlı karar alma süreçlerine entegre ederek askeri modernizasyonu desteklemektedir (Zeng, 2021). Sosyal medya platformları, YZ ile analiz edilerek dezenformasyon kampanyalarını ve potansiyel tehditleri tespit etmekte kullanılmaktadır; çeşitli YZ uygulamaları, çevrimiçi faaliyetleri izleyerek suç senaryolarını önlemeyi amaçlamaktadır (Radulov, 2019).

YZ, askeri ve ulusal güvenlikte otonom silah sistemlerinden istihbarat analizine kadar geniş bir yelpazede dönüştürücü bir rol oynamaktadır. Operasyonel verimlilik ve stratejik üstünlük sağlama potansiyeli, devletlerin güvenlik politikalarını güçlendirmekte ve güvenli toplum hedeflerine katkı sunmaktadır. YZ'nin doğru yönetişim ve etik çerçevelerle kullanılması, güvenlik süreçlerinin daha hızlı, hassas ve etkin bir biçimde yürütülmesini mümkün kılmakta, böylece hem vatandaşların korunması hem de devletlerin krizlere daha hazırlıklı olması sağlanmaktadır.

Yapay Zekâ Destekli Siber Güvenlik

YZ, siber güvenlik alanında önemli bir dönüşüm sağlayarak, hem savunma hem de saldırı stratejilerini yeniden şekillendirmektedir. Büyük veri analitiği, makine öğrenimi ve derin öğrenme algoritmaları, siber tehditlerin tespitinde, önlenmesinde ve yanıt süreçlerinde kritik bir rol oynamaktadır (Brundage ve diğerleri, 2018, s. 9). YZ tabanlı erken uyarı, saldırı tespit ve önleme sistemleri, siber güvenliğin temel taşlarından biri haline gelmiştir. Makine öğrenimi algoritmaları, ağ trafiğindeki anormallikleri ve potansiyel tehditleri gerçek zamanlı olarak tespit ederek, insan analizlerinin yetersiz kaldığı büyük veri kümelerini hızlı bir şekilde işleyebilmektedir. Örneğin, davranışsal analiz yöntemleri, ağ trafiği, uygulama aktiviteleri ve kullanıcı davranışlarındaki sapmaları belirleyerek iç tehditleri tespit etmekte kullanılmaktadır (Jahankhani ve diğerleri, 2020, s. 436). Türkiye'de geliştirilen AVCI, AZAD, KASIRGA, ATMACA ve KULE gibi YZ tabanlı yazılımlar, zararlı yazılımların tespiti ve tehdit istihbaratı gibi işlemleri otomatikleştirerek siber savunma kapasitesini artırmaktadır (Çiçek, 2025, s. 1001). Bu sistemler, siber saldırıların hızına ve ölçeğine yanıt verebilmek için 7/24 çalışacak şekilde tasarlanmış olup, insan tabanlı gözetimin sınırlamalarını aşarak tehditlere saniyeler içinde tepki verebilmektedir (Das & Sandhane, 2021).

YZ sistemleri, inandırıcı kimlik avı (phishing) e-postaları ve mesajları üreterek geleneksel filtreleme sistemlerini aşabilmekte ve hedefli saldırıları daha etkili hâle getirebilmektedir. Bu tür sistemler, dil modelleme ve kişiselleştirilmiş içerik üretimi sayesinde kullanıcıları kandırmada daha yüksek başarı oranına sahiptir (Das & Sandhane, 2021). Ayrıca, makine öğrenimi algoritmaları, yazılım zafiyetlerini keşfetmek için kullanılan otomatik araçlar ile birleştirildiğinde, insan denetimini aşan hız ve kapsamda güvenlik açıkları tespit edilebilmektedir (Oseni ve diğerleri, 2020; Marwala, 2023).

YZ destekli savunma sistemleri, siber saldırılar, fidye yazılımları ve deepfake gibi tehditlere karşı etkili çözümler sunmaktadır. YZ, bu tür tehditlere karşı davranışsal anormallikleri tespit ederek ve otomatik yanıt mekanizmalarıyla saldırıları engelleyerek savunma kapasitesini güçlendirmektedir (Das & Sandhane, 2021). Çin'in "Cyberspace Administration of China" birimi, YZ destekli sistemlerle siber tehditlere karşı ulusal güvenliği korumak amacıyla oluşturulmuştur (Zeng, 2021). Yine benzer şekilde, ABD'deki istihbarat kurumlarının kullandığı sistemler, potansiyel güvenlik açıklarını önceden tespit edebilen YZ temelli antivirüs yazılımlarıyla donatılmıştır (Darici, 2020). Ayrıca, YZ,

deepfake gibi aldatıcı içeriklerin tespitinde, doğal dil işleme ve görüntü analizi tekniklerini kullanarak yanlış bilgilendirme kampanyalarına karşı mücadele etmektedir (Azgin & Kiralp, 2024). YZ'nin savunma sistemlerindeki bu etkinliği, eğitim verilerinin kalitesine ve algoritmaların manipülasyona karşı dayanıklılığı ile ilgilidir (Abanoz & Acar, 2023).

Kritik altyapıların korunmasında YZ uygulamaları, özellikle enerji, sağlık, finans ve ulaşım gibi sektörlerde de hayati önem taşımaktadır. YZ, ağ saldırılarını tespit etmek, sızma testleri yapmak ve güvenlik açıklarını analiz etmek için kullanılarak, altyapıların siber saldırılara karşı direncini artırmaktadır (Bilgin, 2024). Akıllı binaların bulut hizmet altyapısını korumak için kullanılan YZ tabanlı sistemler, tehditleri gerçek zamanlı olarak tespit ederek hızlı yanıt mekanizmaları sunmaktadır (Jahankhani ve diğerleri, 2020). Türkiye gibi orta ölçekli güçler, YZ'nin büyük veri işleme ve desen tanıma yeteneklerini kullanarak nükleer tesisler, barajlar ve finans sistemleri gibi altyapılara yönelik siber tehditlere karşı savunma kapasitesini güçlendirmektedir (Çiçek, 2025).

Sonuç olarak, YZ sistemleri siber güvenlikte hem savunma kapasitesini artırmakta hem de operasyonel süreçleri hızlandırmaktadır. Büyük veri analitiği, makine öğrenimi ve davranışsal analiz yöntemleri sayesinde ağ trafiği ve kullanıcı aktivitelerindeki anormallikler hızlı ve etkili biçimde tespit edilebilmektedir. Ulusal ve kritik altyapı düzeyinde uygulanan YZ tabanlı sistemler, tehdit istihbaratını otomatikleştirerek siber saldırılara karşı proaktif önlemler alınmasına imkân tanımakta; fidye yazılımları, deepfake içerikler ve diğer dijital tehditlere karşı savunma mekanizmalarını güçlendirmektedir. Bu bağlamda, YZ teknolojileri yalnızca siber güvenlik süreçlerini desteklemekle kalmayıp, devletlerin ve kurumların siber tehditlere karşı hazırlıklı olmasını sağlayan stratejik bir araç olarak öne çıkmaktadır.

Yapay Zekânın Güvenlik Kapasitesi ve Sınırlamaları

YZ, güvenlik alanında önemli fırsatlar sunarken, ciddi sınırlamalar ve riskler de barındırmaktadır. Teknolojik doğruluk, YZ sistemlerinin güvenlik uygulamalarındaki temel sorunlarından biridir. İçerik denetimi, tehdit analizi ve yüz tanıma gibi uygulamalarda YZ sistemleri, bağlamı anlamakta güçlük çekmekte, bu durum yanlış pozitif veya negatif tespitlere yol açabilmektedir. Siber güvenlikte yanlış pozitifler kritik altyapılarda gereksiz kesintilere neden olurken, yanlış negatifler gerçek tehditlerin gözden kaçmasına yol açabilmektedir (Çiçek, 2025).

Crawford (2021, s. 4), YZ sistemlerinin yeni verilerle karşılaştığında öngörülemez sonuçlar üretebileceğine dikkat çekmiş ve bu durumun güvenlik uygulamalarında risk oluşturduğunu vurgulamıştır. Benzer şekilde, yüz tanıma sistemlerinde kontrolsüz ortamlar ve kalabalık kamusal alanlar, doğruluk oranlarını düşürmekte ve güvenilirliği azaltmaktadır (Hälterlein, 2023).

Otonom silah sistemleri ise karmaşık savaş ortamlarında ayrımcılık ve orantılılık ilkelerine uygun hareket edememekte, sivil kayıplar gibi istenmeyen sonuçlar doğurabilmektedir (Carnevali, 2022). Bu tür öngörülemez hatalar, YZ'nin güvenilirliğini sorgulatmakta ve insan denetiminin gerekliliğini ön plana çıkarmaktadır.

Algoritmik önyargı ve ayrımcılık potansiyeli ise, YZ'nin güvenlik uygulamalarındaki bir diğer önemli sınırlamasıdır. YZ sistemleri, eğitim veri setlerindeki önyargıları yansıtarak, özellikle yüz tanıma teknolojilerinde etnik ve cinsiyet temelli ayrımcılığa yol açabilmektedir. ProPublica'nın COMPAS yazılımı analizi, renkli bireylerin tekrar suç işleme olasılığının beyaz bireylere göre sistematik olarak yüksek tahmin edildiğini ortaya koymuş ve bu durumun adalet sistemine önyargıların entegre olma riskini gösterdiğini vurgulamıştır (Cole ve diğerleri, 2022). Buolamwini ve Gebru (2018; akt. Hälterlein, 2023, s. 769) ise, yüz tanıma sistemlerinin koyu ten rengine sahip bireyler ve kadınlar üzerinde daha düşük doğruluk sağladığını tespit ederek, teknolojinin etnik ve cinsiyet önyargılarını pekiştirdiğini göstermiştir. Bu önyargılar, yalnızca bireysel hak ihlallerine yol açmakla kalmayıp, güvenlik politikalarının meşruiyetini de zedelemektedir.

Veri güvenliği ve mahremiyet ihlalleri de YZ'nin güvenlik kapasitesini sınırlayan önemli bir faktördür. Büyük veri analitiğine dayalı YZ uygulamaları, kullanıcıların dijital izlerini detaylı biçimde takip edebilmekte ve kamusal ya da özel verileri izinsiz analiz edebilmektedir. Çin'in sosyal kredi sistemi örneğinde görüldüğü gibi, bu tür uygulamalar gözetim toplumuna geçişi hızlandırmakta ve bireylerin

davranışlarının sürekli kontrol edilmesine yol açmaktadır (Şahin, 2024; Kaygısız, 2020). Düzenlemeler bu sorunları sınırlamayı amaçlasa da, kullanıcıların veri haklarını tam anlamıyla koruyabildiğini söylemek zordur.

YZ'nin teknik güvenilirliği de tartışma konusudur. Sistemlerin yanlış eğitilmesi, aşırı genelleştirme yapmaları ve beklenmeyen veriler karşısında hatalı tahminler, güvenlik açısından ciddi riskler doğurmaktadır (Jahankhani ve diğerleri, 2020). Algoritmalar, küçük veri manipülasyonlarıyla kolaylıkla yanıltılabilmekte ve bu da sistemlerin saldırılara açık hale gelmesine neden olmaktadır (Oseni ve diğerleri, 2020). Özellikle siber güvenlikte, veri zehirleme saldırıları YZ tabanlı sistemlerin yanlış sınıflandırmalar yapmasına yol açmakta, bu durum güvenilirlik kaybını ve siber suçların karmaşıklığını arttırmaktadır (Hoadley & Lucas, 2018).

Tüm bu sınırlamalar, YZ'nin güvenlik kapasitesinin yalnızca teknolojik yeterlilikle değerlendirilemeyeceğini, aynı zamanda etik, hukuki ve toplumsal boyutların da göz önünde bulundurulması gerektiğini göstermektedir. YZ sistemleri, güvenlik alanında önemli faydalar sunarken, öngörülemezlik, algoritmik önyargı ve veri güvenliği gibi kritik riskler de barındırmaktadır. Yanlış pozitif veya negatif tespitler, otonom silah sistemlerindeki ayrımcılık riski ve yüz tanıma uygulamalarındaki etnik veya cinsiyet temelli önyargılar, teknolojinin güvenilirliğini ve güvenlik politikalarının meşruiyetini doğrudan etkilemektedir. Ayrıca, büyük veri analitiğine dayalı YZ sistemlerinin mahremiyet üzerindeki etkileri, bireylerin davranışlarının sürekli gözetim altında tutulmasına yol açmakta ve güvenlik uygulamalarının etik sınırlarını zorlamaktadır. Bu bağlamda, YZ'nin güvenlik alanındaki etkinliğinin ancak insan denetimi, etik çerçeveler ve güçlü veri yönetimi mekanizmalarıyla desteklendiğinde güvenli ve meşru biçimde artırılabileceği ifade edilebilir. Böylece YZ, güvenlik uygulamalarında hem fırsatlar hem de sorumluluklar yaratan karmaşık bir araç olarak öne çıkmaktadır.

YAPAY ZEKÂ ÇAĞINDA GÜVENLİK PARADOKSU: GÜVENLİ TOPLUM MU, GÖZETİM TOPLUMU MU?

Modern toplumun, yeni bilgi ve iletişim teknolojilerinin hızla yayılmasıyla bir "gözetim toplumu" haline geldiği ifade edilebilir (Lyon, 2007). Zuboff, gözetimin sadece belirli bir ortamdaki davranışları gözlemlemekle sınırlı olmadığını, toptan bir kapsama sahip olarak gelecekteki davranışları manipüle etmeye kaydığını savunmaktadır (Zuboff, 2019). Lyon ise gözetimin her zaman güç ve onun dağılımıyla ilgili olduğunu belirtirken, mevcut teorik yaklaşımların dijital teknolojiler çağında güç ilişkilerini yeterince ele almadığını vurgulamaktadır (Lyon, 2007, s. 20).

Bu bağlamda YZ çağında, güvenlik sağlama kapasitesindeki artış ile gözetim ve kontrol mekanizmalarının güçlenmesi arasındaki gerilimin, "güvenli toplum mu, gözetim toplumu mu?" sorusunu gündeme getiren bir paradoksu ortaya çıkardığı ifade edilebilir. YZ, ulusal güvenlik, istihbarat ve şehir yönetiminde gözetleme yeteneklerini artırırken; sınır güvenliğinde "akıllı sınırlar" oluşturarak ve Palantir gibi şirketlerin veri analitiğiyle suç tespitini kolaylaştırarak güvenlik potansiyelini yükseltmektedir (Crawford, 2021). Ancak bu teknolojilerin otoriter kontrol mekanizmalarını güçlendirme riski, bireysel özgürlükleri ve demokratik değerleri tehdit ederek güvenlik-gözetim paradoksunu derinleştirmektedir.

Güvenlik-gözetim paradoksu, YZ'nin toplumsal güvenliği artırma potansiyeli ile bireyleri sürekli izleyen bir gözetim toplumuna dönüşme riski arasındaki gerilimi ifade etmektedir. Bu paradoksun, YZ'nin devletler ve özel sektör tarafından nasıl kullanıldığına bağlı olarak, güvenli bir toplum yaratma vaadi ile otoriter kontrol mekanizmalarını güçlendirme tehlikesi arasında bir denge arayışını zorunlu kıldığı ifade edilebilir. YZ'nin güvenlik alanındaki katkıları, otoriterleşmeyi teşvik etme riski ve bireysel özgürlüklerden vazgeçme sorunsalı, bu paradoksun temel boyutlarını oluşturmaktadır.

YZ, güvenlik paradigmalarını dönüştürerek terörle mücadele, suç önleme ve kriz yönetiminde önemli yenilikler sunmaktadır. Ancak, YZ'nin güvenlik alanındaki bu faydaları, otoriter rejimlerde toplumsal kontrol ve kitle gözetimi için kullanılma riskiyle gölgelenmektedir. Çin'in Sosyal Kredi Sistemi, bu tehdidin en çarpıcı örneğidir. Yüz tanıma, büyük veri analitiği ve algoritmalar yardımıyla

bireylerin ekonomik, sosyal ve dijital davranışları değerlendirilmekte; olumlu davranışlar ödüllendirilirken, istenmeyen davranışlar ulaşım, finansman veya eğitim gibi alanlarda kısıtlamalarla sonuçlanmaktadır (Crawford, 2021; Jahankhani ve diğerleri, 2020). Çin'in "Sharp Eyes" (Keskin Gözler) programı, kent merkezlerinden kırsal alanlara kadar uzanan geniş kapsamlı bir gözetim altyapısıdır. Bu program, yüz tanıma sistemleri ve davranışsal analiz algoritmaları ile donatılmış milyonlarca kamerayı birleştirerek, kamu alanlarının %100'e yakın bir oranda gözetlenmesini hedeflemektedir (Shahbaz, 2018). Demokratik toplumlarda da benzer endişeler söz konusudur. ABD'de öngörücü polislik uygulamaları, özellikle marjinalleştirilmiş grupları orantısız hedef alarak algoritmik önyargılara yol açabilmektedir (Crawford, 2021). Rusya'da ise YZ destekli yüz tanıma teknolojileri, rejim karşıtlarını bastırmak için kullanılmaktadır (Azgin & Kiralp, 2024, s. 510). Bu sistemlerin ortak özelliği, güvenlik gerekçesiyle gözetimin norm haline gelmesi ve bu süreçte bireylerin "şüpheli" olarak konumlandırılmasıdır (Doyran, 2021, s. 3).

Güvenlik-gözetim arasındaki bu gerilim, güvenlik adına bireysel özgürlüklerden vazgeçme sorunsalını öne çıkarmaktadır. YZ'nin sürekli gözetim kapasitesi, bireylerin mahremiyet alanlarını daraltmakta ve ifade özgürlüğü üzerinde olumsuz bir etki yaratmaktadır. Gözetim altında olduğunu hisseden bireylerin oto-sansür uygulama ve kamusal alandan çekilme eğiliminde oldukları belirtilmektedir (Coeckelbergh, 2022). Özel sektörün gözetim kapitalizmi de bu paradoksu derinleştirmektedir. Google ve Facebook gibi teknoloji devleri, kullanıcı verilerini toplayarak bireylerin davranışlarını tahmin eden ve manipüle eden algoritmalar geliştirmiştir. Zuboff, bu sistemlerin bireyleri ticari ve siyasi manipülasyon nesnelerine dönüştürdüğünü ifade etmek amacıyla "enstrümantal güç" kavramını kullanmaktadır (Zuboff, 2019, s. 19). Sonuç olarak, güvenlik - gözetim paradoksu, YZ çağında güvenli bir toplum yaratma çabalarının, bireysel özgürlükleri tehdit eden bir gözetim toplumuna dönüşme riskini barındırdığını göstermektedir.

Bununla birlikte YZ sistemleri, güvenlik politikalarını desteklemek için tasarlanırken, önyargılı veri setleri ve algoritmalar nedeniyle ayrımcı sonuçlar üretebilmekte, bu da mahremiyet, eşitlik ve ifade özgürlüğü gibi temel hakları tehdit etmektedir. Gözetim kapitalizmi, büyük veri analitiği ve algoritmik denetim mekanizmaları aracılığıyla bireylerin mahremiyetini ihlal ederken, özellikle savunmasız gruplar üzerinde orantısız etkiler yaratmaktadır.

YZ sistemlerinin önyargı üretme riski, özellikle yüz tanıma ve tahmine dayalı polislik gibi güvenlik uygulamalarında belirgindir. Algoritmalar, genellikle insan tarafından üretilen veri setlerinden öğrenildiğinden, bu veriler toplumsal önyargıları yansıtabilmektedir (Akyılmaz, 2020). Tahmine dayalı polislik algoritmaları, geçmiş suç verilerine dayanarak belirli mahalleleri veya etnik grupları hedef almakta; bu da eşitsizlikleri derinleştiren bir döngü yaratmaktadır (Sönmez, 2019). Örneğin, Afro-Amerikan bireylerin beyaz bireylere göre daha tehlikeli olarak sınıflandırılması, toplumsal güveni zedeleyen ve aidiyet duygusunu zayıflatan ayrımcı sonuçlara yol açmaktadır (Abanoz & Acar, 2023, s. 40). Bu önyargılar, algoritmaların tarafsız olmadığını, mevcut güç dengesizliklerini ve ayrımcılık kültürlerini yansıttığını ve hatta güçlendirdiğini göstermektedir (Sloane, 2022, s. 4). Bu bağlamda algoritmik önyargıların, mahremiyet hakkı, ayrımcılık yasağı ve ifade özgürlüğü gibi insan haklarını doğrudan tehdit ettiği ifade edilebilir.

Bununla birlikte, YZ sistemlerinin veri toplama ve profilleme süreçleri, bireylerin mahremiyetini ihlal ederek demokratik toplumlarda özel alanın sınırlarını zorlamaktadır. Sosyal medya platformları ve diğer dijital ara yüzler, kullanıcı verilerini toplayarak bireylerin davranışlarını izlemekte ve tahmin etmekte; bu, bireylerin rızası olmadan ayrıntılı profiller oluşturulmasına yol açmaktadır (Masco, 2020). Ayrıca, YZ destekli içerik denetimi, dilbilimsel ve kültürel bağlamları yeterince yorumlayamadığı için yanlışlıkla insan hakları yanlısı içerikleri silebilmekte, bu da ifade özgürlüğünü kısıtlayan başka bir hak ihlaline yol açmaktadır (Azgin & Kiralp, 2024). Gözetim sistemlerinin, belirli etnik veya dini grupları hedef alarak sınıflandırması, eşitlik ilkesine aykırı uygulamaları körükleyerek masumiyet karinesinin zedelenmesine yol açmaktadır (Eşitti, 2015).

Gözetim kapitalizminin ise, bireysel hak ve özgürlükleri hedef alan tehditleri daha da karmaşık hale getirdiği

ifade edilebilir. Zuboff'un tanımladığı üzere, gözetim kapitalizmi, bireylerin davranışlarını veri toplama yoluyla tahmin ederek ve ticarileştirerek özerkliği ve mahremiyeti tehdit eden bir sistemdir (Zuboff, 2019). Örneğin Facebook ve Google, kullanıcı verilerini reklamcılık ve pazarlama için toplarken; bu veriler devletlerle iş birliği içinde gözetim amaçlı da kullanılabilir. Çin'in Sosyal Kredi Sistemi örneğinde ise, bireylerin günlük davranışlarını izleyerek oluşturulan cezalandırma ve ödüllendirme mekanizmaları, toplumsal ve bireysel hareket özgürlüğünün kısıtlanmasına yol açmaktadır (Şahin, 2024). Bu sistemler, bireyleri bir "sürü zihniyeti"ne yönlendirerek bağımsız düşünme kabiliyetlerinin ortadan kaldırılmasına yol açmaktadır (Risse, 2023, s. 170).

Uluslararası insan hakları belgeleri, YZ sistemlerinin ayrımcılık yapmaması ve temel haklara saygı göstermesi gerektiğini vurgulamaktadır. Özellikle "Toronto Deklarasyonu", algoritmaların şeffaf, adil ve hesap verebilir şekilde tasarlanması ve uygulanmasını önermektedir. Bu belge, YZ'nin eşitlik ilkesine uygun biçimde geliştirilmesi gerektiğini ve ayrımcılığı önlemek için açık standartlara ihtiyaç olduğunu belirtmektedir (Sloane, 2022). Ancak uygulamada, özellikle azınlık gruplara yönelik sınıflandırmalarda ve güvenlik politikalarında bu ilkelere yeterince riayet edilmemektedir. Sonuçta gözetim teknolojilerinin artan kullanımının, kişisel veri ve davranışsal izlerin sürekli olarak kaydedildiği bir "dijital panoptikon" (Lyon, 2019) yarattığı ifade edilebilir. Bu durumun, bireylerin ifade özgürlüğünü sınırlayarak, otosansürü arttırması ve demokratik katılımı zayıflatması kaçınılmaz görünmektedir.

Güvenlik gerekçeleriyle meşrulaştırılan YZ teknolojileri kitle gözetimi, davranış manipülasyonu ve muhaliflerin bastırılması gibi mekanizmalar aracılığıyla otoriter yönetimlerin iktidarlarını pekiştirmesine olanak tanımaktadır. Çin'in Sosyal Kredi Sistemi ve Sincan bölgesindeki yoğun gözetim ağları ile Rusya'nın yüz tanıma sistemleri, YZ'nin toplumsal kontrol amacıyla nasıl araçsallaştırıldığını güçlü bir şekilde ortaya koymaktadır. Bu uygulamalar, bireysel özerkliği tehdit ederken, otoriter modellerin küresel yayılımı ve teknoloji transferi yoluyla demokratik toplumlar üzerinde de ciddi riskler oluşturmaktadır.

Otoriter devletlerde YZ tabanlı kitle gözetim sistemleri, toplumsal düzeni sağlama kisvesi altında bireylerin her hareketini izleyen ve değerlendiren kapsamlı ağlar oluşturmaktadır. Çin'in sosyal kredi sistemi, yüz tanıma teknolojisi, büyük veri analitiği ve WeChat gibi platformlardan toplanan verilerle bireylerin ekonomik, sosyal ve siyasi davranışları puanlanmakta; düşük puan alanlar uçak bileti alamama, yüksek hızlı internete erişememe veya çocuklarının iyi okullara kabul edilmemesi gibi yaptırımlarla karşılaşmaktadır (Kaygısız, 2020). Sistemin, vatandaşların davranışlarını "kamusal ve mahrem verilerle desteklenen araçsal gücün yüceltilmesi" şeklinde işlev görerek dijital totalitarizmi güçlendirdiği ifade edilebilir (Şahin, 2024, s. 77).

Çin'in Sincan bölgesinde, özellikle Uygur Türklerine yönelik gözetim sistemleri, etnik özelliklere dayalı yüz tanıma teknolojileriyle bireyleri gerçek zamanlı olarak izlemekte ve sınıflandırmaktadır (Akyılmaz, 2020). 2010 yılında Urumçi'de 47.000 kamerayla başlayan bu ağ, kısa sürede genişleyerek bölgedeki toplumsal kontrolü yoğunlaştırmıştır (Ay & Sezer, 2019, s. 126). Rusya'da ise Moskova'daki yüz tanıma ağları, Putin rejimini eleştiren gazetecilerin ve muhaliflerin tespitinde kullanılmış, rejim karşıtı hareketleri bastırmak için etkili bir araç haline gelmiştir (Azgin & Kiralp, 2024). Bu durum, bireylerin sürekli izlendikleri hissiyle hareket etmelerine, düşüncelerini ifade etmekten çekinmelerine ve rejimin normlarına uymaya zorlanmalarına yol açmaktadır (Eşitti, 2015, s. 18). YZ'nin bu tür uygulamaları ile bireysel özerkliği tehdit eden ve vatandaşların davranışlarını belirli bir politik norm çerçevesine çekmeye çalışan dijital yönetişim sistemleri haline geldiği anlaşılmaktadır (Coeckelbergh, 2022, s. 141).

Çin'de WeChat üzerinden toplanan veriler, rejime muhalif eğilimleri tespit etmek için analiz edilirken, sosyal medyanın sansür ve propaganda aracı olarak kullanımı bireylerin ifade özgürlüğünü kısıtlamaktadır (Azgin & Kiralp, 2024). Rusya'da YZ tabanlı propaganda ve deepfake teknolojileri, muhalif figürleri itibarsızlaştırmak için kullanılırken, bireylerin siyasi katılımı ve eleştirel düşüncesi üzerinde olumsuz bir etki yaratmaktadır (Türk, 2021). Bu uygulamalar, bireylerin özerkliğini aşındırarak otoriter rejimlerin toplumsal kontrolü derinleştirmesine

olanak tanımaktadır.

YZ'nin otoriter rejimlerdeki kullanımının küresel etkilerinin ise, özellikle teknoloji transferi ve otoriter modellerin ihracı yoluyla diğer toplumlar için de ciddi riskler barındırdığı ifade edilebilir. Çin, Suudi Arabistan ve Etiyopya gibi ülkelere YZ tabanlı gözetim teknolojilerini ihraç ederek, bu rejimlerin ulusal yüz tanıma veritabanları oluşturmasına ve muhalif grupları hedeflemesine olanak tanımaktadır. Çin'in 2017 Siber Güvenlik Yasası, çevrimiçi içerik üzerinde hükümet kontrolünü artırırken; bu model diğer otoriter devletler için bir şablon oluşturmaktadır (Azgin & Kiralp, 2024).

Alibaba gibi şirketler devletle iş birliği içinde bireylerin verilerini hükümetle paylaşarak otoriter gözetim altyapısını güçlendirmiştir (Çiftçi, 2024). Bu teknolojilerin demokratik toplumlara ihracı, otoriterliğin ihracatı olarak tanımlanmakta ve demokratik değerleri tehdit etmektedir. Örneğin, Çin'in YZ ekosistemi ve sivil-asker füzyon politikaları, otoriter kontrol mekanizmalarını küresel ölçekte yaygınlaştırma potansiyeline sahiptir (Türk, 2021, s. 137). Ayrıca, YZ teknolojileri, özellikle sosyal medya ve dijital içerik üretiminde, dezenformasyon ve manipülasyon amacıyla kullanılarak seçim süreçlerini ve kamuoyunu etkileyebilmektedir. Bu durum, demokratik yapıları zayıflatırken, popülist ve otoriter eğilimleri güçlendirme potansiyeli taşımaktadır (Tinnirello, 2022).

Otoriter rejimlerin YZ kullanım biçimi, aynı zamanda bilgi kontrolü ve dezenformasyon süreçlerini de kapsamaktadır. Sosyal medyada kullanıcı davranışlarının izlenmesi, dijital sansür uygulamaları, yapay içerik üretimi ve algoritmik manipülasyon gibi yöntemlerle, rejimlerin kamuoyunu yönlendirme ve muhalif sesleri susturma kapasitesi ciddi şekilde artmıştır (Tinnirello, 2022; Crawford, 2021).
Bu stratejiler, otoriter rejimlerin yalnızca fiziksel değil, bilişsel alanı da kontrol etme çabasının bir parçasıdır. YZ'nin otoriter rejimlerdeki kullanımı, teknolojinin sadece bir güvenlik aracı değil, aynı zamanda siyasal iktidarın yeniden üretildiği bir tahakküm aracına dönüştüğünü göstermektedir. Dijitalleşmenin bu yönü, yalnızca mevcut otoriter rejimleri güçlendirmekle kalmamakta, aynı zamanda demokratik gerilemeyi hızlandırabilecek küresel eğilimleri de tetiklemektedir.

Bu noktada, otoriter bağlamdaki uygulamaların karşısında, demokratik toplumlarda YZ'nin nasıl konumlandırılması gerektiği sorusu öne çıkmaktadır. Demokratik toplumlarda YZ teknolojilerinin kullanımının şeffaflık, hesap verebilirlik ve insan hakları ilkeleriyle uyumlu biçimde denetlenmesi gerekmektedir (Bahtiyar, 2024). YZ'nin demokratik bağlamda güvenlik politikalarına entegrasyonu, yalnızca teknik bir mesele değil; etik, hukuki ve siyasal boyutları olan çok katmanlı bir dönüşüm sürecidir. Crawford'un belirttiği gibi, teknolojinin sürdürülebilirliği, ancak adaletin uygulanması ve gücün sınırlandırılmasıyla mümkündür. YZ sistemlerinin demokratik yönetişimle uyumlu olabilmesi için temel hakların korunması esastır. Veri koruma, ifade özgürlüğü ve ayrımcılık yasağı ilkeleri, yalnızca bireysel hakları değil, aynı zamanda toplumun demokratik yapısını da koruma işlevi görmektedir. Crawford, bu bağlamda, teknolojik sistemlerin sürdürülebilirliğinin, adaletin tesisi ve gücün sınırlandırılması ile mümkün olduğunu vurgulamaktadır (Crawford, 2021, s. 20).

Demokratik denetimin yalnızca mevzuatla değil, aynı zamanda aktif yurttaş katılımı ve sivil toplumun gözetim rolüyle de desteklenmesi gerekmektedir. YZ destekli içerik moderasyonu, şeffaflık eksikliği ve algoritmik önyargılar nedeniyle ifade özgürlüğünü tehdit edebileceği gibi, kamuoyu manipülasyonunu engellemeye de yardımcı olabilir (Tinnirello, 2022).

Bununla birlikte, güvenlik yaklaşımının yalnızca ulusal sınırlar içinde değil, küresel ölçekte de yönetişim ilkelerine bağlanması önemlidir. Birleşmiş Milletler ve Avrupa Konseyi gibi uluslararası örgütlerin, YZ'nin insan haklarıyla uyumlu biçimde kullanılmasına ilişkin normatif çerçeveler geliştirmesi bu alanda önemli bir adımdır (Garcia, 2022).

Alternatif güvenlik yaklaşımları, güvenliği yalnızca "tehditlere karşı korunma" perspektifinden değil, "insan güvenliği" çerçevesinden de ele almayı gerektirmektedir. Bu anlayış, bireyin fiziksel güvenliğinin yanı sıra, mahremiyetinin, ifade özgürlüğünün ve demokratik katılım hakkının korunmasını da kapsamaktadır (Lyon, 2019, s. 2). Aksi halde, güvenlik adına uygulanan teknolojiler, demokrasinin zeminini aşındırma riskini beraberinde getirmektedir.

Sonuç olarak, yapay zekâ destekli güvenlik uygulamaları hem otoriter rejimlerde hem de demokratik toplumlarda geleceğin siyasal ve toplumsal düzenini şekillendirme potansiyeline sahiptir. Ancak bu teknolojilerin güvenliği güçlendirirken özgürlükleri zayıflatma riski, onları yalnızca teknik değil, aynı zamanda derin bir etik ve politik mesele haline getirmektedir. Otoriter rejimlerde YZ, tahakküm ve gözetimi artırarak demokratik değerlerin küresel ölçekte gerilemesine yol açabilirken; demokratik bağlamda ise şeffaflık, hesap verebilirlik ve insan hakları ilkeleriyle desteklenen bir kullanım, teknolojinin özgürlükleri koruyan bir güvenlik aracına dönüşmesini mümkün kılabilir. Güvenlik politikalarının demokratik değerlerle uyumlu bir şekilde şekillendirilmesi, teknolojinin sunduğu fırsatları gözetim toplumuna dönüşme riskinden arındırarak, gerçekten güvenli ve özgür bir toplum idealine hizmet edebilir. Bu nedenle, YZ'nin güvenlik alanındaki rolü, teknolojik ilerlemenin ötesinde, insan hakları, adalet ve toplumsal refah ekseninde yeniden düşünülmelidir. YZ çağında güvenlik-gözetim paradoksunun çözümü, yalnızca teknolojinin kendisinde değil, onu yönlendiren siyasal ve toplumsal tercihlerde aranmalıdır.

SONUÇ

YZ teknolojileri, güvenlik paradigmasını köklü bir şekilde dönüştürerek tehdit algılama, kriz yönetimi ve stratejik karar alma süreçlerinde devrim niteliğinde yenilikler sunmaktadır. Geleneksel devlet merkezli ve askeri odaklı güvenlik anlayışı, küreselleşme ve teknolojik ilerlemelerle birlikte dijital, biyolojik ve etik boyutları kapsayan çok katmanlı bir yapıya evrilmiştir. YZ'nin yüz tanıma, tahmine dayalı polislik, otonom silah sistemleri ve siber savunma gibi alanlarda sunduğu fırsatlar, güvenlik kapasitesini artırırken; aynı zamanda mahremiyet, bireysel özgürlükler ve demokratik değerler üzerinde ciddi tehditler oluşturmaktadır. Bu bağlamda çalışma, YZ çağında güvenliğin sağlanması ile gözetim toplumuna dönüşme riski arasındaki paradoksu ele alarak, güvenli bir toplum yaratma çabasının otoriter kontrol mekanizmalarını güçlendirme tehlikesiyle nasıl iç içe geçtiğini ortaya koymaya çalışmaktadır.

YZ'nin güvenlik alanındaki dönüştürücü etkisi, özellikle otoriter rejimlerde kitle gözetimi ve toplumsal kontrol araçları olarak kullanılmasıyla belirginleşmektedir. Demokratik toplumlarda ise algoritmik önyargılar, veri güvenliği ihlalleri ve mahremiyet kayıpları, YZ'nin güvenlik politikalarına entegrasyonunun etik ve hukuki sınırlarını sorgulatmaktadır. Çalışmada, yapay zekâ teknolojilerinin yalnızca güvenlik kapasitesini artıran araçlar olmadığı; aynı zamanda bireysel özgürlükler, mahremiyet ve demokratik değerler üzerinde belirleyici etkiler yarattığı sonucuna varılmıştır. Bulgular, YZ'nin güvenlik politikalarına entegrasyonunun, güvenlik-gözetim paradoksunu derinleştirdiğini ve otoriter kontrol mekanizmalarını güçlendirme riski taşıdığını göstermektedir. Bununla birlikte, şeffaflık, hesap verebilirlik ve insan haklarına dayalı yönetişim çerçeveleri inşa edildiğinde, YZ'nin güvenliği özgürlüklerle uyumlu bir şekilde destekleyebileceği anlaşılmaktadır.

Bu anlamda makalenin katkısı, güvenliği yalnızca teknolojik kapasiteye indirgemeyen; siyasal, etik ve toplumsal boyutlarıyla ele alan bütüncül bir perspektif geliştirmesidir. Literatürde çoğunlukla teknik kapasiteye odaklanan çalışmaların aksine, burada güvenlik kavramının demokratik normlar, insan hakları ve toplumsal refah ile ilişkisi ön plana çıkarılmıştır. Politika düzeyinde ise algoritmik şeffaflık, güçlü veri koruma düzenlemeleri, sivil toplumun aktif katılımı ve uluslararası normatif çerçevelerin güçlendirilmesi kritik görülmektedir.

Güvenli bir toplum inşa etmek, yalnızca teknolojik kapasiteye değil, aynı zamanda demokratik denetim, şeffaflık ve insan haklarına dayalı bir yönetişim modeline bağlıdır. Alternatif güvenlik yaklaşımları, bireylerin fiziksel güvenliğinin yanı sıra mahremiyet, ifade özgürlüğü ve demokratik katılım haklarını merkeze alarak, insan odaklı bir güvenlik anlayışını benimsemelidir. Bu nedenle uluslararası işbirlikleri ve normatif çerçevelerin, YZ'nin küresel ölçekte sorumlu kullanımını desteklemek için vazgeçilmez olduğu ifade edilebilir.

Sonuç olarak, YZ çağında güvenlik, yalnızca tehditlere karşı korunma meselesi olmaktan çıkmış; kimin, neye karşı ve ne pahasına korunacağı sorularını merkeze alan bir siyasal ve etik mesele haline gelmiştir. Bununla birlikte, bu çalışmanın güvenlik-gözetim paradoksuna dair kavramsal ve kuramsal düzeyde önemli bir çerçeve sunduğu; gelecek araştırmalarda farklı rejim tipleri ve vaka analizleriyle desteklenmesi halinde güvenlik-gözetim paradoksunun somut yansımalarını daha net ortaya koyacağı düşünülmektedir. YZ'nin güvenlik alanındaki rolü, teknolojik ilerlemenin ötesinde, insan hakları, adalet ve toplumsal refah ekseninde yeniden düşünülmelidir.

KAYNAKLAR

Abanoz, M. ve Acar, E. (2023). Yapay zekâ ve ontolojik güvensizlik: Bireysel ve toplumsal kaygı dinamikleri üzerine bir değerlendirme. *LAÜ Sosyal Bilimler Dergisi, 14*(1), 22-51.

Adler, E. (1997). Seizing the middle ground: Constructivism in world politics. *European Journal of İnternational Relations*, *3*(3), 319-363.

Akyılmaz, B. (2020). Yapay zekâ temelli gözetim teknolojileri ve pazar ilişkisi. C. Tor-Kadıoğlu (Ed.), *Dijital pazarlamada güncel araştırmalar* içinde (s. 81-101). Artikel Akademi.

Amoore, L. (2013). *The politics of possibility: Risk and security beyond probability*. Duke University Press.

Ay, A. ve Sezer, Ö. (2019). Dijitalleşmenin güvenlikleştirme vaadi: Dijital hapishaneler. *Manas Sosyal Araştırmalar Dergisi, 8*(1), 123-136.

Ayoob, M. (1997). Defining security: A subaltern realist perspective. K. Krause ve M. C. Williams (Eds.), *Critical security studies: Concepts and cases* (pp. 121-146). University of Minnesota Press.

Azgin, B. ve Kiralp, S. (2024). Surveillance, disinformation, and legislative measures in the 21st century: AI, social media, and the future of democracies. *Social Sciences, 13*(10). https://doi.org/10.3390/socsci13100510

Bahtiyar, N. (2024). *Yapay zekâ teknolojilerinin ekonomi ve siyaset bağlamında ortaya çıkardığı yeni toplumsal dinamiklerin ABD, Çin ve Türkiye üzerinden incelenmesi* (Yayımlanmamış Doktora Tezi). Pamukkale Üniversitesi.

Bellany, I. (1981). Towards a theory of international security. *Political Studies*, *29*(1), 100-105.

Bentham, J. (1995). *The panopticon writings*. Verso Books.

Bilgin, K. R. (2024). Geleceğin savaşlarında yapay zekâ. *Güvenlik Stratejileri, 20*(50), 1-33. https://doi.org/10.17752/guvenlikstrtj.1394924

Bodin, J. (2008). *On sovereignty*. Cambridge University Press.

Booth, K. (1997). Security and self: Reflections of a fallen realist. K. Krause ve M. C. Williams (Eds.), *Critical security studies: Concepts and cases* (pp. 35-60). University of Minnesota Press.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S. ve Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford. https://doi.org/10.48550/arXiv.1802.07228

Buzan, B. (2015). *People, states & fear: An agenda for international security studies in the post-Cold War era*. ECPR Press.

Buzan, B., Weaver, O. ve de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

C.A.S.E. Collective. (2006). Critical approaches to security in Europe: A networked manifesto. *Security Dialogue, 37*(4), 443-487. https://doi.org/10.1177/0967010606073085

Carnevali, A. T. (2022). Governing the use of autonomous weapon systems. M. Tinnirello (Ed.), *The global politics of artificial intelligence* (pp. 85-99). CRC Press. https://doi.org/10.1201/9780429446726-4

Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Cicero, M. T. (1999). *De Officiis* (C. D. Yonge, çev.). Harvard University Press.

Coeckelbergh, M. (2022). *The political philosophy of AI: An introduction*. John Wiley & Sons.

Cole, M., Cant, C., Ustek Spilda, F. ve Graham, M. (2022). Politics by automatic means? A critique of artificial intelligence ethics at work. *Frontiers in Artificial Intelligence, 5*, 869114. https://doi.org/10.3389/frai.2022.869114

Crawford, K. (2021). *Atlas of AI*. Yale University Press.

Çiçek, A. E. (2025). Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejisi. *Yönetim Bilimleri Dergisi, 23*(56), 993-1012.

Çiçek, Ç. (2025). Yapay zekâ ile kamu yönetimi ve güvenlikte dönüşümün yeni çağı. *Tarsus Üniversitesi Uygulamalı Bilimler Fakültesi Dergisi, 5*(1), 50-62.

Çiftçi, O. (2024). Yapay zekâ ve silahlanma yarışı: ABD ve Çin arasındaki güç dengesinin değişen dinamikleri. *Marmara Üniversitesi Siyasal Bilimler Dergisi, 12*(2), 175-200. https://doi.org/10.14782/marmarasbd.1436516

Darici, A. B. (2020). Yapay zekânın yönetiminin uluslararası güvenliğe etkileri. *Savunma Bilimleri Dergisi, 19*(1), 49-72.

Das, R. ve Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics: Conference Series, 1964*(4), 042072. https://doi.org/10.1088/1742-6596/1964/4/042072

David, M. ve Verbakel, D. (2022). *Critical security studies: A schismatic history. Contemporary security studies*. Oxford University Press.

Deibert, R. J. (2013). *Black code: Surveillance, privacy, and the dark side of the internet*. Signal Books.

Doyran, E. (2021). Dijital dünya, gözetim teknolojileri ve yapay zekâ: Hükümranlık ve özgürlük arasında modern insan. *INSAMER Analiz*. https://insamer.com/tr/dijital-dunya-gozetim-teknolojileri-ve-yapay-zeka-hukumranlik-ve-ozgurluk-arasinda-modern-insan_3989.html

Dupont, B. (2007). Power struggles in the field of security: Implications for democratic transformation. M. Deflem (Ed.), *Sociology of crime, law and deviance: Surveillance and governance: Crime control and beyond* (pp. 259-280). Emerald Group Publishing.

Eşitti, Ş. (2015). *Gözetim toplumunda sinoptikon ve sosyal medya* (Yayımlanmamış Doktora Tezi). Marmara Üniversitesi.

Foucault, M. (1995). *Discipline and punish: The birth of the prison*. Pantheon Books.

Fischer, S.-C. ve Wenger, A. (2021). Artificial intelligence, forward-looking governance and the future of security. *Swiss Political Science Review, 27*(1), 170-179. https://doi.org/10.1111/spsr.12439

Galloway, C. ve Swiatek, L. (2018). Public relations and artificial intelligence: It's not (just) about robots. *Public Relations Review, 44*(5), 734-740. https://doi.org/10.1016/j.pubrev.2018.10.008

Garcia, E. V. (2022). Multilateralism and artificial intelligence: What role for the United Nations? M. Tinnirello (Ed.), *The global politics of artificial intelligence* (pp. 57-75). CRC Press.

Haldun, İ. (2004). *Mukaddime* (A. Işık, çev.). Klasik Yayınları.

Hälterlein, J. (2023). The use of AI in domestic security practices. S. Lindgren (Ed.), *Handbook of critical studies of artificial intelligence* (pp. 763-772). Edward Elgar Publishing.

Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics, 2*(2), 157-180.

Hoadley, D. S. ve Lucas, N. J. (2018). *Artificial intelligence and national security*. Congressional Research Service. https://www.crs.gov

Hobbes, T. (1992). *Leviathan.* Cambridge University Press

Jahankhani, H., Kendzierskyj, S., Chelvachandran, N. ve Ibarra, J. (2020). *Cyber defence in the age of AI, smart societies and augmented humanity*. Springer Nature. https://doi.org/10.1007/978-3-030-35746-7

Jiang, Y., Li, X., Luo, H., Yin, S. ve Kaynak, O. (2022). Quo vadis artificial intelligence? *Discover Artificial Intelligence, 2*(1), 1-19. https://doi.org/10.1007/s44163-022-00022-8

Kanat, S. ve Akoğuz, N. O. (2024). Uluslararası ilişkiler ve yapay zekâ: Uluslararası güvenlik açısından bir değerlendirme. *Sosyal ve Beşeri Bilimler Araştırmaları Dergisi, 25*(54), 60-73.

Kaygısız, Ü. (2020). Gözetim toplumunun siyaset, devlet ve demokraside yansımaları: Algoritmik vatandaşlık odağında bir değerlendirme. *Manas Sosyal Araştırmalar Dergisi, 9*(2), 1288-1299. https://doi.org/10.33206/mjss.537299

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security, 38*(2), 7-40. https://doi.org/10.1162/ISEC_a_00138

Kolodziej, E. A. (2005). *Security and international relations*. Cambridge University Press.

Krause, K. ve Williams, M. C. (1997). *Critical security studies: Concepts and cases*. University of Minnesota Press.

Liddell, H. G. ve Scott, R. (1940). *A Greek-English Lexicon*. Oxford University Press.

Lippmann, W. (1943). *U.S. Foreign policy: Shield of the Republic*. Little Brown and Company.

Locke, J. (2002). *Two treatises of government*. Yale University Press.

Luciani, G. (1989). The security dilemma and the national interest: The case of the Mediterranean. *International Relations, 23*(1), 48-62. https://doi.org/10.1177/004711788902300105

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Lyon, D. (2019). *State and surveillance*. Centre for International Governance Innovation.

Machiavelli, N. (2005). *The prince* (W. K. Marriott, çev.). University of Chicago Press.

Marwala, T. (2023). *Artificial intelligence, game theory and mechanism design in politics*. Springer Nature. https://doi.org/10.1007/978-981-99-5103-1

Masco, J. (2020). Surveillance and the senses. I. Bartoletti (Ed.), *An artificial revolution: Power, politics and AI* (pp. 181-184). The Indigo Press.

Mill, J. S. (2008). *Özgürlük üzerine* (M. Özay, çev.). Türkiye İş Bankası Kültür Yayınları.

Mondal, B. (2020). Artificial Intelligence: State of the Art. Balas, R. K. ve R. Srivastava (Ed.), *Recent Trends and Advances in Artificial Intelligence and Internet of Things (pp. 389-425). Springer.*

Montesquieu, C. (1998). *The spirit of the laws* (A. M. Cohler, B. C. Miller ve H. S. Stone, çev.). Cambridge University Press.

Nişanyan, S. (2009). *Türkçe etimoloji sözlüğü*. Türk Dil Kurumu

Yayınları.

Ogaba, O. (2010). Security, "Globalization and Climate Change": A Conceptual Analysis. E. E. Osita, ve O. Ogaba (Eds.), *Security in Nigeria* (pp. 28-39). NIIA.

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z. ve Vasilakos, A. (2020). Security and privacy for artificial intelligence: Opportunities and challenges. *Journal of the ACM, 37*(4), 111. https://doi.org/10.1145/1122445.1122456

Poku, N. K. ve Graham, D. T. (2000). Introduction. N. K. Poku ve D. T. Graham (Eds.), *Migration, globalization, and human security* (pp. 1-15). Routledge.

Radulov, N. (2019). *Artificial intelligence and security*. New Bulgarian University.

Risse, M. (2023). *Political theory of the digital age: Where artificial intelligence might take us*. Cambridge University Press. https://doi.org/10.1017/9781009255189

Rousseau, J. J. (2004). *Toplum sözleşmesi*. (B. Kaynak, çev.), Betik Yayınları.

Russell, S. J. ve Norvig, P. (2010). *Artificial intelligence: A modern approach*. Pearson Education.

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology, 29*(2), 354-398.

Shahbaz, A. (2018). *Freedom on the net 2018: The rise of digital authoritarianism*. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Singer, P. W. ve Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Sloane, M. (2022). Threading innovation, regulation, and the mitigation of AI harm: Examining ethics in national AI strategies. M. Tinnirello (Ed.), *The global politics of artificial intelligence* (pp. 1-28). CRC Press. https://doi.org/10.1201/9780429446726-1

Sönmez, O. (2019). *Küresel siyaset ve uluslararası ilişkiler yüksek lisans programı kapsamında yapay zekâ ve ulusal güvenlik* (Yayımlanmamış Yüksek Lisans Tezi). Bahçeşehir Üniversitesi.

Şahin, M. (2024). Gözetim toplumu ve Çin sosyal kredi sistemi: Toplumsal kontrolün yeni yüzü. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* (49), 66-84. https://doi.org/10.61904/sbe.1452667

Tinnirello, M. (2022). *The global politics of artificial intelligence*. CRC Press. https://doi.org/10.1201/9780429446726

Türk, O. (2021). *How to govern military AI: On the global governance of artificial intelligence from an international security perspective* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Teknik Üniversitesi.

Ullman, R. (1983). Redefining security. *International Security, 8*(1), 129-153. https://doi.org/10.2307/2538545

Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization, 46*(2), 391-425. https://doi.org/10.1017/S0020818300027764

Wolfers, A. (1962). *Discord and collaboration: Essays on international politics*. The Johns Hopkins Press.

Yalçın, A. (2024). Türkiye'de kamu kurumlarının toplum için geliştirdiği yapay zekâ uygulamaları. *İstanbul Aydın Üniversitesi Sosyal Bilimler Dergisi, 16*(2), 185-215.

Zhang, B. ve Dafoe, A. (2019). *Artificial intelligence: American attitudes and trends*. Center for the Governance of AI, Future of Humanity Institute, University of Oxford. https://ssrn.com/abstract=3312874

Zeng, J. (2021). Securitization of artificial intelligence in China. *The Chinese Journal of International Politics, 14*(3), 385-411. https://doi.org/10.1093/cjip/poab005

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Yazar Katkı Oranları

Yazarlar araştırmaya eşit oranda katkı sağlamıştır.