

Jandarma ve Sahil Güvenlik Akademisi

Güvenlik Bilimleri Enstitüsü

Güvenlik Bilimleri Dergisi, Mayıs 2025, Cilt:14, Sayı:1, 87-110

doi: 10.28956/gbd.1569382

Gendarmerie and Coast Guard Academy

Institute of Security Sciences

Journal of Security Sciences, May 2025, Volume:14, Issue:1, 87-110

doi: 10.28956/gbd.1569382

Makale Türü ve Başlığı / Article Type and Title

Araştırma / Research Article

Sınır Güvenliğinde Yapay Zekâ Entegrasyonu

Integration of Artificial Intelligence Into Border Security

Yazar(lar) / Writer(s)

İbrahim İRDEM, Doç.Dr., Polis Akademisi Başkanlığı, Güvenlik Bilimleri Enstitüsü,

Türkiye, ibrahimirdem33@gmail.com, ORCID: 0000-0003-0559-3418

Murat UZUNPARMAK, Dr., İçişleri Bakanlığı, Türkiye, muzunparmak@gmail.com,

ORCID: 0000-0002-3027-4016

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:

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

-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.

This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 17.10.2024

Makale Kabul Tarihi / Accepted : 30.05.2025

Atıf Bilgisi / Citation:

İrdem İ. ve Uzunparmak M., (2024). Sınır Güvenliğinde Yapay Zekâ Entegrasyonu,

Güvenlik Bilimleri Dergisi, 14(1), ss 87-110. doi: 10.28956/gbd.1569382



SINIR GÜVENLİĞİNDE YAPAY ZEKÂ ENTEGRASYONU

Öz

Artan küresel tehditlere, demografik hareketlere ve sınır aşan suçlara bağlı olarak yapay zekâ destekli uygulamalar sınır güvenliğinin idamesinde gerek dünyada gerekse Türkiye’de güvenlik yönetiminin vazgeçilmez bir unsuru hâline gelmiştir. Geleneksel yöntemlerin yetersiz kaldığı yeni güvenlik sorunlarına karşı önleyici, etkin, veri odaklı, hızlı ve verimli yaklaşımlar geliştirme ihtiyacı yapay zekâ kullanımına yönelik çabaların artmasına neden olmuştur. Ancak yapay zekâ sınır gözetiminde ve yönetiminde önemli fırsatlar sunmakla birlikte uygulamada etik, hukuki ve teknik boyutlarda birtakım sorunları beraberinde getirmektedir. İçerik analizi ve betimleyici nitel analiz yöntemine dayanan çalışmada yapay zekânın sınır güvenliği konusunda beraberinde getirdiği teknolojik ilerlemeler ele alınmakta, sınır güvenliğinin tatbikinde yapay zekânın rolü tartışılmaktadır. Çalışmada dünyadan ve Türkiye’den uygulamalarla sınır güvenliğinde yapay zekâ entegrasyonuna yönelik çabalara yer verilmektedir. Çalışmanın varsayımı; yapay zekâ ile entegre bir sınır güvenliği anlayışının insana duyulan ihtiyacı azalttığı, hataları olabildiğince en aza indirerek daha proaktif bir yaklaşım sergilediği, tehdit ve riskler karşısında hızlı ve etkili müdahalede bulunma imkânı tanıdığı, karar alma sürecini desteklediği ve sınır güvenliğini daha etkin bir şekilde yönetmeye imkân tanıdığıdır. Bununla birlikte yapay zekâyâ dair çeşitli teknik, hukuki ve etik, sorunların uygulamalar sırasında mutlaka kapsamlı bir şekilde göz önünde bulundurulması ve sınır güvenliğinin tahkiminde teknolojinin sunduğu fırsatların riskler gözötilerek optimum düzeyde kullanılması temel bir zorunluluk teşkil etmektedir.

Anahtar Kelimeler: Sınır, Sınır Güvenliği, Türkiye, Yapay Zekâ.

INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO BORDER SECURITY

Abstract

Due to increasing global threats, demographic movements and cross-border crimes, artificial intelligence-supported applications have become an indispensable element of security management in the maintenance of border security both in the world and in Türkiye. The need to develop preventive, effective, data-oriented, fast and efficient approaches to new security problems, where traditional methods are insufficient, has led to an increase in efforts to use artificial intelligence. However, while artificial intelligence offers significant opportunities in border surveillance and management, it also brings with it some technical, legal and ethical problems in practice. The study, based on content analysis and descriptive qualitative analysis methods, addresses the technological advances brought by AI in border security, and discusses the role of AI in the implementation of border security. The study includes efforts to integrate AI in border security with applications from the world and Turkey. The assumption of the study is that an integrated border security approach with artificial intelligence reduces the need for humans, exhibits a more proactive approach by minimizing errors as much as possible, supports the rapid and effective intervention and decision-making process in the face of threats and risks, and enables more effective management of border security. However, it is a fundamental requirement that various ethical, legal and technical issues related to artificial intelligence be taken into consideration comprehensively during applications and that the opportunities offered by technology in the strengthening of border security are used at an optimum level by considering the risks.

Keywords: Border, Border Security, Türkiye, Artificial Intelligence.

GİRİŞ

Sınır güvenliğinin etkin bir şekilde tesisi hem iç güvenlik açısından hem de dış güvenlik açısından büyük önem taşımaktadır. İç güvenlik bağlamında sınır güvenliği; düzensiz göçün engellenmesi, uyuşturucu, göçmen ve silah kaçakçılığının önlenmesi, insan ticareti faaliyetlerinin durdurulması ve organize suç örgütlerinin faaliyetlerinin kesintiye uğratılması sebebiyle stratejik öneme haizken dış güvenlik perspektifinden ise küresel terörizmle mücadele, aşırıcılığın önüne geçilmesi, bölgesel ya da uluslararası güvenlik tehditlerini bertaraf etme açısından kritik bir rol ifa etmektedir (Hashmat, 2017, s.264).

Küreselleşme ile birlikte güvenlik tehditlerinin içeriğinin genişlemesi, demografik hareketlerin yoğunlaşması ve sınır aşan suçların küresel olarak dolaşıma girmesi sınır güvenliğinin önemini pekiştirmiştir (İrdem vd., 2021, s.6). Değişen ve giderek karmaşıklaşan günümüz güvenlik dinamiği içerisinde sınır güvenliği yalnızca geleneksel kontrol mekanizmalarıyla sağlanamayacak bir yapıya doğru evrilmiştir. Sınır güvenliğinin idamesi sürecinde karşılaşılan tehditlerin çeşitliliği sınır güvenliğinin sağlanmasında yapay zekâ kullanımını zorunlu hâle getirmiştir.

Jeopolitik konumları nedeniyle bir takım tehdit ve risklerle karşı karşıya kalan ülkeler sınır güvenliği meselesine stratejik bir bakış açısıyla yaklaşarak, sınır güvenliği politikalarına yapay zekâyı giderek daha fazla entegre etmeye başlamıştır. Özellikle ABD, Çin, Hindistan ve İsrail gibi ülkeler küresel güç rekabeti ve bölgesel tehditler nedeniyle sınır güvenliğini stratejik bir öncelik haline getirmiştir. Hindistan; bilhassa Pakistan ve Bangladeş ile olan kara sınırlarında yapay zekâ teknolojilerini kullanarak sınır güvenliğini optimize etme amacı güderken, Avustralya ve Birleşik Krallık deniz hudutlarını korumak için yapay zekâ destekli uygulamalardan olabildiğince yararlanmaktadır. Türkiye ise komşu ülkelerde yaşanan istikrarsızlıklar, düzensiz göç, terörizm ve sınır ötesi suçlar gibi güvenlik tehditleri karşısında sınır güvenliğini güçlendirmek amacıyla yapay zekâ teknolojilerini sınır güvenliği politikasına etkin bir şekilde entegre etmeye çalışmakta, belirtilen ülkelerde olduğu gibi bu alana ciddi kaynak ayırmaktadır.

Yapay zekâ; sınır ekipmanları, gözetleme cihazları ve personel gibi sınır güvenliğine ilişkin geleneksel yöntemleri etkili ve kapsamlı bir şekilde dönüştürmüştür (Güven, 2024, s.67). Yapay zekâ; sınır kontrol ve gözetim sürecine insansız hava araçları, termal kameralar, otonom gözetleme kuleleri, görüntü işleme teknikleri, dronlar, zırhlı araçlar ve biyometrik güvenlik sistemleri

gibi ileri teknolojileri entegre ederek sınır güvenliğini daha etkin, hızlı ve yenilikçi yapıya kavuşturmaktadır. Ayrıca veri temelli analizlerle desteklenen karar destek sistemleri sayesinde daha isabetli ve proaktif koruma mekanizmasının oluşturulmasını mümkün kılmaktadır. Bununla birlikte yapay zekâ, sistemsel problemler, veri güvenliği zafiyetleri, mahremiyet ihlalleri, kötü niyetli aktörler tarafından gerçekleştirilecek etik dışı uygulamalar gibi çok katmanlı sorun alanlarını da içermektedir. Bu nedenle sınır güvenliği uygulamalarında yapay zekâ kullanımında etik standartlara riayet edilip teknik alt yapısı sürekli gözden geçirilecek ve optimize edilecek şekilde tatbik edilmelidir. Hukuki açıdan ise özgürlük ve güvenlik arasındaki hassas dengeyi gözeten standartlarla şekillenmesi gerekmektedir.

Bu çalışmada dünyadan ve Türkiye’den uygulamalarla yapay zekânın sınır güvenliğine entegrasyonu incelenmekte, yapay zekânın sunduğu fırsatların teknik, hukuki ve etik boyuttaki risklerle dengelenerek sınır güvenliğinin sağlanmasında yapay zekâdan nasıl daha etkin bir şekilde yararlanılabileceği tartışılmaktadır. Çalışmada öncelikle yapay zekâdan ve beraberinde getirdiği fırsatlarla birlikte teknik, hukuki ve etik risklerden bahsedilmekte, akabinde ise sınır güvenliğinin öneminden hareketle sınır güvenliğinin idamesinde yapay zekâ kullanımına yönelik küresel eğilimlere ve Türkiye’deki gelişmelere yer verilmektedir. Çalışma politika yapıcılara ve uygulayıcılara yönelik önerilerle sonuçlandırılmaktadır.

1. YAPAY ZEKÂ

1950’lerden beri tartışılmaya başlayan yapay zekâ konusunda evrensel olarak üzerinde mutabık kalınmış bir tanım bulunmamaktadır (Gbadegeshin vd, 2021, s.468). Bunun sebebi; yapay zekânın birden fazla araştırma alanının odağında yer alması ile, her bir disiplinin kavramı kendi yöntemi, uzmanlık alanı ve çalışma amacına göre tanımlamasından kaynaklanmaktadır (Wang, 2019, s.28).

İnsan hayatının neredeyse her yönünü dönüştürme yeteneğine sahip olan yapay zekâ, insan zekâsı gerektiren görevleri yerine getirebilen akıllı makinelerin geliştirilmesiyle ilgilenen bir alandır (Dogget, 2023, s. 22). Yapay zekâyı insan tarafından tanımlanan belirli hedeflere yönelik içerik, tahminler, tavsiyeler veya kararlar gibi çıktılar üreten mühendislik sistemine ayrılmış teknik ve bilimsel bir alan olarak nitelendirmek mümkündür (International Organization for Standardization, 2022).

Yapay zekâ geleneksel teknolojilerden farklı bir biçimde insan özelliklerinden hareketle modellenerek bireylerin bilişsel ve davranışsal

özelliklerini taklit etme kabiliyetine sahiptir (Adaş ve Erbay, 2022, s.328). Yapay zekâ esasında evrendeki kullanılabilir aklın ya da zekânın işlenmesi ve bilgi türlerinin toplanması sürecinde mekanik bir simülasyon sistemidir. Bu süreç bilginin toplanması ve yorumlanmasını içeren ve hatta eyleme geçerek onu zekâyâ dönüştüren bir aşamayı kapsamaktadır (İrdem ve Çobanoğlu, 2021, s.177). Makine öğrenimi, yapay sinir ağları ve derin öğrenme gibi farklı bileşenleri bünyesinde birleştiren yapay zekâ; veri odaklı öngörüler ve karmaşık modellemeler gerçekleştirebilen, insan beyninin nöral işleyişinden esinlenerek uyarlanabilir ve gelişmiş çözümlemeler sunabilen bir teknolojidir (İşcan ve Kaygısız, 2024, s.203). Rasyonel ve insani düşünme, karar verme ve çıktı üretme gibi işlevleri özerk bir şekilde gerçekleştirebilen bir sistem, program, yazılım ya da algoritma olarak da ifade edilebilir (Martinez, 2019, s.1038).

Avrupa Birliği (AB) Yapay Zekâ Yasası'na göre yapay zekâ sistemi; farklı özerklik düzeyleriyle çalışmak üzere tasarlanmış, konuşlandıktan sonra uyarlanabilirlik gösterebilen, açık ya da dolaylı hedefler doğrultusunda aldığı girdilerden hareketle fiziksel veya sanal ortamları etkileyebilecek içerikler, öneriler ya da kararlar gibi çıkarımlar yapan makine temelli bir sistemdir (EU Artificial Intelligence Act, Article 3).

Yapay zekânın bilimsel bir kavram olarak kökeni, 1956'da ABD'de eğitim kurumu olan Dartmouth Koleji'ndeki bir araştırma programına kadar geriye götürülebilmektedir. Her ne kadar yapay zekâ niteliğindeki tartışmalar daha önce gündeme gelse de bu program sayesinde yapay zekâ sistematik laboratuvarlar çerçevesinde ele alınmaya başlamıştır (Skeikh, Prins ve Schrijvers, 2023, s.4). Programda John McCarthy tarafından düzenlenen çalışmaya Marvin Minsky, Nathaniel Rochester ve Claude Shannon gibi alanın öncü isimleri de katılım sağlamış, bu etkinliğin ardından yapay zekâ çalışmaları hızla gelişmeye başlamıştır (Coşkun ve Gülleroğlu, 2021, s.949). 1956'da yapay zekâyâ ilişkin ilk bilimsel toplantıyı düzenleyen McCharthy; yapay zekâyı zeki makineler üretme bilimi ve mühendisliği olarak tanımlamış, zekâyı ise dünya üzerindeki hedeflere ulaşmayı sağlayan hesaplanabilir bir beceri olarak ifade etmiştir (Smith ve Seward, 2023, s.42). Sonraki yıllarda çok sayıda bilim insanı otomatik akıl yürütmeye odaklanmış, yapay zekâ matematik teoremlerini kanıtlamak ve cebirsel problemleri çözmek amacıyla uygulanır hâle gelmiştir. Hatta bu konuda Allen Newell, Herbert A. Simon ve Cliff Shaw tarafından yazılan 'Logic Theorist' (Akıl /Mantık Teorisyeni) adlı bilgisayar programı 20. yüzyılın önemli matematik kitaplarından biri olan, matematiğin felsefesi ve mantığını ele almayı amaçlayan 'Principia Mathematica' daki ilk 52 teoremin

38'ini ispatlamış ve diğer teoriler için de kısmen kanıtlayıcı veriler sunmuştur (Gugerty, 2006, s. 880).

Türkiye’de yapay zekânın geleceğine yönelik farkındalık konusunda ilk önemli çalışmayı ise Cahit Arf’ın 1958 yılında Erzurum’da verdiği “*Makineler Düşünebilir Mi?*” başlıklı konferans oluşturmaktadır. Arf; kendisinden yaklaşık sekiz yıl önce, 1950’de Alan M. Turing tarafından kaleme alınan, “*Computing Machinery and Intelligence*” -Hesaplama Makineleri ve Zekâ- başlıklı makalesinde sorguladığı, makinelerin bir düşünme yetisine sahip olup olmayacağı sorusunu, Erzurum’da halka açık olarak düzenlenen konferansta yeniden gündeme taşımıştır (Sarı, 2021, s.815). Düşünme sisteminin makinelerle entegrasyonunu tavuk ve tavşan sayısını bulmaya yönelecek makine ile Bay Ahmed’in oğulları olan Ali ile Veli arasındaki miras meselesini çözmeye yönelecek makine üzerinden ele almıştır. Arf’a göre mantıksal ve analitik görevleri yerine getirecek şekilde tasarlanabilecek makinelerin işleyiş tarzı ile insan zihninin çalışma biçimi arasında ortak yönler mevcuttur. Ancak Arf; elektronik beyin olarak da nitelendirilebilecek makinelerin insan beynine kıyasla bazı görevleri hızlıca yerine getirebildiğini, kendi kendisini geliştirebilen makine icat etmenin mümkün olabileceğini fakat insan beyninin kendi kendini geliştirebilirken makinelerin sabit kaldığını belirtmektedir (Arf, 1958, s.103). Arf’a göre makine ile insan beyni arasındaki asıl fark; insan beyni estetik değerleri işleyip özgür iradesiyle karar verebilirken makinelerin ise bu yetilerden yoksun olmasıdır. Ayrıca Arf, bu özelliklerin belirsizlik içerdiğini ve insan dışı tabiât hadiselerinin mevcut olduğunu dile getirerek nispeten küçük sayıda atom içeren olayların makinelerin işleyişinde etkili kılınması durumunda makinelerin estetik yargılarının bile geliştirilebileceğini, hatta bir müzik parçasını beğenmediğini söyleyecek şekilde insan beynine benzer hâle gelebileceğini vurgulamaktadır. Arf bu öngörüsünü ise yüzyıllar sonrasına dayandırmakta, belki de hiçbir zaman gerçekleşemeyebileceğini belirtmektedir (Arf, 1958, s.103). Arf’ın kaleme aldığı zaman diliminde ortaya attığı bu öngörüler son derece dikkat çekici ve heyecan vericidir. Lakin Büyük Dil Modellerinin dil işleme ve yaratıcı çıktı üretme kabiliyeti ile kuantum bilgisayarın üstün işlem kapasitesinin hâlihazırda beraberinde getirdiği çığır aşan gelişmeler karşısında bu öngörüler üzerinde yeniden düşünülmesi kaçınılmazdır.

Günümüzde yapay zekâ sadece matematik alanında değil, hemen hemen hayatın her alanında devrim yaratan teknolojik gelişmeleri içeren, insan zekâsı gerektiren iş ve işlemleri yerine getirmeyi amaçlayan bilgisayar sistemlerinin

gelişimi olarak telakki edilebilir. Yapay zekânın özellikle son on yılda ivme kazanması bilgisayarın hesaplama gücündeki büyük ilerlemeler ve çok sayıda veriye erişim imkânı sayesinde gerçekleşmiştir. Özellikle gelişmiş algoritmaların oluşturulması, düşük maliyetli grafik işlemcilerinin yaygınlaştırılması ve akıllı sistemlerin daha etkili şekilde öğrenmesini sağlayan, büyük ve doğru şekilde işlenmiş veri kümesinin kullanılabilir hâle gelmesi yapay zekâ araştırmalarını canlandırmıştır (Collins, Dennehy, Conboy ve Mikalef, 2021, s.2). Yapay zekâ birçok alanda ve geniş bir yelpazede yenilikçi uygulamalara kapı aralamıştır.

2. YAPAY ZEKÂNIN TEKNİK, HUKUKİ VE ETİK BOYUTU: FIRSATLAR VE RİSKLER

Yapay zekâya ilişkin teknolojik ilerlemeler makinelerle veri toplama, bilgiyi analiz etme, desenleri tanımlama ve bu verilere dayanarak rasyonel kararlar verme yeteneği kazandırmıştır. Yapay zekâ; algoritmalar, bilgisayar programları ve istatistiksel modellerden istifade ederek karar verme sürecini köklü bir şekilde etkilemektedir. Sabit tekrarlanan uygulamalar sayesinde iş ve işlemlerde hız sağlamaktadır. Bununla birlikte yapay zekâ potansiyel gelişmelere karşı duyarlı tepkiler geliştirerek gelecek tahmini ve risk değerlendirmesi yapma kabiliyetine sahiptir. Böylece öğrenen ve sürekli gelişmeye açık olan algoritmalar sayesinde olası risk, tehlike ya da hata senaryolarını belirleyerek insan hatasını en aza indirmeyi amaçlanmaktadır. Erken uyarı sistemi ve tehdit analizleri sayesinde olası riskleri proaktif bir yaklaşımla kontrol altına almaktadır. Çoğu zaman insan emeğini daha yüksek beceri gerektiren alanlara yönlendirerek işler olan otomasyon mekanizması sayesinde verimliliği olumlu yönde etkilemektedir. İnsan hatalarından mümkün olduğunca arınmış şekilde yönetsel süreci daha kolay ve hızlı hâle getiren yapay zekâ maliyeti azaltarak değer inşa etmektedir (İrdem ve Çobanoğlu, 2022, s.195).

Çok sayıda alanda tatbik edilen yapay zekâ uygulamaları ortaya çıkardığı olumlu yönler yanında birtakım karmaşık sorun alanlarını da bünyesinde barındırmaktadır. Bu sebeple yapay zekâdan istifade ederken, beraberinde getirdiği riskler de göz ardı edilmemeli, fırsat ne kadar çoksa riskin de o kadar fazla olabileceği asla gözden kaçırılmamalıdır.

Yapay zekâ araçlarının teknik açıdan karşı karşıya kaldığı en önemli sorun alanlarından biri “önyargı” riskidir. Algoritmaların veriler üzerinden öğrenmesini sağlayarak modelleri eğiten bireylerin bilinçli ya da bilinçsiz bir şekilde kendi bakış açılarını yansıtmaları durumunda yapay zekâ karar alma

sürecinde ayrımcılık yapabilmekte ve yanlış kararların ortaya çıkmasına neden olabilmektedir. Önyargılı kararlar ise adaletsizlikleri tetikleyebilmekte, mevcut eşitsizlikleri derinleştirebilmektedir (Ferrara, 2024, s.1). Örneğin yapay zekâ X ülkesinden gelen göçmenlere karşı önyargı ile eğitilirse, sınır kontrolleri sırasında X ülkesi vatandaşlarını haksız yere yüksek riskli veya şüpheli olarak kategorize edebilecektir. Böyle bir durum ise herhangi bir suç geçmişi olmayan masum insanlara yönelik ayrımcılığın artmasına, toplumsal güven kaybına ve sosyal dışlanmaya neden olacaktır.

Büyük veri ve karmaşık problemler için makine öğrenmesini ve derin öğrenmeyi kullanan yapay zekâ derin sinir ağlarının algoritmik yapısıyla çalışmaktadır. Ancak yapay zekâ algoritmasının karar alma süreci insan kavrayışına kapalı ve çoğunlukla belirsiz olduğu için bu durum karşımıza yapay zekânın “kara kutu” sorunu olarak çıkmaktadır (Eschenbach, 2021, s.1607). Karar alma mekanizmasının “şeffaf” olmaması yapay zekâ ile elde edilen çıktıların ya da tahminlerin güvenilirliğinin sorgulanmasına neden olmaktadır. Sınır bölgelerinde yapay zekâ destekli uygulamalar sayesinde bireylerin jest ve mimikler üzerinden davranışlarının şüpheli olarak kabul edilip edilmeyeceği ayrımı bu duruma örnek gösterilebilir. Kullanılan sistemin hangi kriterleri esas alarak bireylerin davranışlarını anormal kabul ettiği ve sınır geçişine neden müsaade etmediği konusundaki belirsizlik önemli soru işaretlerini beraberinde getirmektedir.

Yapay zekâ uygulamalarının geliştirilmesi oldukça maliyetli bir çabayı gerektirmektedir. Yapay zekâ teknolojileri her geçen gün gelişmekte, bu teknolojilerin geliştirilme sürecinde ciddi uzmanlık bilgisine ve insan kaynağına ihtiyaç duyulmaktadır. Bununla birlikte teknolojik altyapı harcamaları, verilerin elde edilmesi ve işlenmesi sürecinde karşı karşıya kalınan masraflar yapay zekânın maliyetli bir uygulama alanı olduğunu göstermektedir.

Yapay zekâ teknik açıdan taşıdığı riskler yanında teknik boyutuyla bağlantılı şekilde hukuki ve etik problemlere de yol açabilmektedir. Verilerin kötü niyetli kişilerin eline geçmesi, veri gizliliğine yönelik riskler ve bireylerin mahremiyetine yönelik saldırılar hem birey güvenliğini tehdit etmekte hem de hukuki sorun doğurmaktadır. Bu nedenle, yapay zekâdaki gelişmelere paralel şekilde etkili siber güvenlik önlemlerinin geliştirilmesi kaçınılmazdır. Bununla birlikte yapay zekâ tarafından alınan kararlar makine öğrenimi algoritmalarına ve temel verilere dayandığı için yanlı ya da eksik veri girişi veya algoritmik ve teknolojik belirsizlikler etik sorunlara yol açabilmektedir (Guan, Dong ve Zhao,

2022, s.3). Yapay zekânın ön yargıya dayanarak karar alması veya yanıltıcı bir değerlendirme yapması hukuki açıdan ise sorumluluk ve hesap verebilirlik riski barındırmaktadır. Çünkü hatalı sonuçların hukuki yaptırımının kime yükleneceği belirsizdir. Bu nedenle yapay zekâyâ bir sorumluluk isnat edilmesi açısından ‘hukuki kişilik’ tanınıp tanınmaması gerektiğine ilişkin tartışmalar hukuk literatüründe gündeme gelmektedir (Kılıçarslan, 2019, s.379). Ancak yapay zekâyâ ilişkin düzenlemelerin dünya genelinde nispeten geriden geldiği belirtilebilir. Bunun temel sebebi ise yapay zekâ teknolojisinin hızla hayatımıza etki etmesi ve pek çok ülkede kanun koyucuların yapay zekânın kullanım alanları, faydaları ve ortaya çıkabilecek sorunlara yönelik çözüm geliştirmede yavaş hareket etmesidir (Küçük, 2024, s.36).

Yapay zekâ kimi zaman özgürlük ve güvenlik arasındaki hassas dengeyi aşındırabilmektedir. Güvenlik adına gerçekleştirilen pratiklerin orantısız ve amacından sapacak bir şekilde bireysel özgürlükleri baskılaması hak ihlali yarattığı gibi etik soruna da sebebiyet vermektedir. Güvenliği sağlamak adına kullanılan ileri düzey teknolojik aygıtların veya güvenlik adına yoğunlaşan veri odaklı denetim mekanizmalarının bireysel mahremiyeti ve özerkliği zedelemesi özgürlük ve güvenlik arasında bir gerilim yaratmaktadır.

Askerî karar alma sürecinde bireylerin yerini alması sebebiyle savaş alanının doğasını tamamen değiştirme potansiyeline sahip otonom silah sistemleri güçlü devletler lehine bir ‘güç asimetrisi’ yarattığı gibi insan hakları ihlaline neden olabilmektedir. Nitekim düşmanı tespit etmede içsel bir öngörüsü bulunmadığı için otonom silahların devreye girmesiyle birlikte kimin yaşamının sona ereceğini makinelerin eline bırakmak etik olmadığı gibi aynı zamanda insan yaşamına ve insan onuruna saygının ihlalidir (Güneysu, 2024, s.145). Otonom sistemlerin insan müdahalesi olmadan bağımsız karar alabilmesi ve sensor füzyonu, makine öğrenimi, gerçek zamanlı karar alma ve hareket planlaması gibi birçok gelişmiş teknolojiyi bünyesinde barındırması sebebiyle doğası gereği karmaşık bir yapı arz etmesi mahremiyet ihlalinden yaşam hakkının tehlikeye girmesine kadar geniş bir yelpazede risk teşkil etmektedir. Sınır güvenliğini sağlamak için kullanılan otonom dronların yanlış hedefleme yapması durumunda karşı karşıya kalınacak telafisi güç zararlar otonom sistemlerin insan hakları üzerinde doğurduğu potansiyel tehdidi açıkça göstermektedir.

3. SINIR GÜVENLİĞİ

Sınırlar ulusal ve uluslararası politikanın gittikçe önem kazandığı önemli bir bileşenidir (Simmons ve Kenwick, 2022, s.854). Bir devletin egemen olduğu coğrafi alanı temsil eden sınır kavramı aynı zamanda bir devletin gücünü de ifade etmektedir. Sınır her devlet için özel bir değere sahip olup; temel olarak üç işlevi yerine getirir (Świerczyńska, 2023, s.154): Bunlardan ilki, devlet toprağına yönelik silahlı bir saldırıyı önlemeye yönelik askerî işlev; ikinci olarak malların ve hizmetlerin kontrolsüz hareketini engelleyen bir bariyer olarak ekonomik işlev; üçüncüsü ise düzensiz göçü, insan- organ ticaretini vb. engelleyen ya da insanların serbest hareketini kontrol altına alan sosyal işlevdir. Askerî işlevi ülke savunması ile açıklamak mümkündür. Askerî işlev ülkenin ulusal güvenliğinin dış saldırılara ya da tehditlere karşı korunması, egemenliğin muhafazasıdır. Bununla birlikte sınırlar ülkeler arasında mal, hizmet, sermaye ve insan akışını gözetim altına alan yerlerdir. Geçirgen ve kontrolsüz sınırlar ulus ötesi organize suç örgütlerinin mensupları, terör örgütü üyeleri ya da yabancı terörist savaşçılar tarafından hedef alınmaktadır. Bu durum ise devletlerin suçla ve terörle mücadele çabalarına gölge düşürmek yanında ülke nüfusunun savunmasızlığını artırmakta, uluslararası barışı ve güvenliği olumsuz yönde etkilemektedir (Global Counterterrorism Forum, 2016). Bu nedenle sınırların terör eylemlerinden, düzensiz göç hareketlerinden, mal, uyuşturucu vb. gibi kaçakçılık faaliyetlerinden korunması, düzenli ve yasal olan insan hareketliliğinin ve sınırlar arası etkileşimin teşvik edilmesi amacıyla sınır güvenliği devletler için kritik bir rol oynamaktadır.

Devletler sınır güvenliğine yönelik tedbirlerle kontrolsüz bir sınırın yarattığı kırılganlığı ortadan kaldırmayı, ülke topraklarında bulunan tüm bireylerin yaşam kalitesini iyileştirmeyi, ülkenin ekonomik canlılığına yönelik riskleri azaltmayı amaçlamaktadır (Manjarrez, 2015, s.795). Hükümetler son yıllarda gelişen teknolojiyle birlikte sınır güvenliğine ciddi kaynak ayırmaya başlamışlardır (IOM, 2017, s. 2).

Sınır güvenliğinin ulus devletler tarafından etkili bir şekilde korunması ulus ötesi insan hareketliliğini kontrollü bir şekilde yönetmeye imkân tanımaktadır. Ayrıca yasa dışı ticareti engellemekte, kaçakçılık, uyuşturucu ve terör faaliyetlerinin önlenmesini sağlamaktadır. Bununla birlikte biyolojik, kimyasal ya da sağlıkla ilgili tehditlerin ülke içine yayılımı sınır güvenliğinin etkin bir şekilde tesisi sayesinde bastırılmaktadır.

Sınırlar salt coğrafi bir elek, araç, bariyer, çit ya da fiziksel bir duvar görevi görmekle kalmayıp aynı zamanda sosyal olarak inşa edilen ayrımlardır. Bu nedenle sınırları sosyal ve politik bir yapı olarak tanımlamak da mümkündür (Storey, 2007, s.1). Sınırlar bir yandan ulus devletin neyi koruyacağını, yargı yetkisinin alanını, egemenliğinin nerede başlayıp bittiğini belirlerken diğer yandan da ‘bizi’, ‘diğerlerinden’ ayıran şeyin ve ‘kim olduğumuzun’ fiziksel ve kavramsal tezahürüdür (Spiro, 2010, s.16).

Sınırlar; toplumsal gruplar arasında ayrımlar üreten sosyal ve sembolik bağları ya da etkileşimleri içeren, bu bağların görece konumlarını ve yerlerle olan bağlantısını yapılandıran hatlardır (Faist, 2009, s. 81). Bir devlete ait semboller, işaretler, anlatılar sınır belirlemede son derece önemli olup; sınırlar dünyanın pek çok bölgesinde hafızanın yani ortak tarihin jeopolitiği tarafından belirlenmektedir (Kolossoff ve Scott, 2013). Dolayısıyla sınır güvenliği sınırların sosyal olarak da inşa edildiği gerçeğinden hareketle sınırların salt fiziksel olarak korunmasını değil aynı zamanda toplumsal hassasiyetler, değerler, kimlikler, semboller gibi unsurların da muhafazasını içermektedir.

4. SINIR GÜVENLİĞİNDE YAPAY ZEKÂ TATBİKİ

İçinde bulunduğumuz dijital çağda sınırlar giderek güvenlikleştirilmekte, devletler yeni teknolojilerden yararlanılarak sınır güvenliği yönetimi sürecinde geniş alt yapılar inşa etmektedir. Sınır yönetim sürecinde parmak izi uygulamasından yüz tanıma, iris tarayıcılarından biyometrik teknolojiye, coğrafi etiketlemeden dronlara ve yalan dedektörlerine kadar pek çok yeni sistemler geliştirilmektedir (OHCHR, 2023, s.4). Sınırların dijitalleşmesi sınır gözetiminden veri toplama ve analizine kadar sınır yönetiminin tüm boyutlarını içermektedir. Bu çerçevede sınırların dijitalleşmesi ile anlaşılması gereken şey, sınırların gözetimi ve yönetiminde teknolojiden mümkün mertebe yararlanılmasıdır.

Sınırların dijitalleşmesi ile birlikte sınır geçişleri hızlı ve zaman tasarrufu sağlayacak şekilde sağlanmakta, yasa dışı geçiş ihlallerine yönelik tespit becerisi artmaktadır. Özellikle yapay zekâ ve veri analitiği sayesinde sınır gözetim sürecinin daha dinamik bir yapıya kavuşması güvenlik açıklarını bertaraf etmede proaktif bir yaklaşım ortaya koyarak tehdit ve risklere karşı erken tespit ve müdahale imkânı sunmaktadır. Dijitalleşme; sınır yönetiminde bir standardizasyon tahkim ederek otomasyonu sağlamakta, sınır güvenliğinden sorumlu aktörlere veri elde etme, elde edilen veriyi değerlendirme ve sınır geçişini kontrol etmede kolaylıklar sağlamaktadır. Ülke içinde sınır

güvenliğinden sorumlu çeşitli birimler arasında yönetim esaslı veri paylaşımı ve dijitalleşme yoluyla sağlanan veri entegrasyonu ülkeler arasında sınır yönetimine ilişkin iş birliğini güçlendirmektedir. Ancak sınır yönetimi ve güvenliği sürecinde tatbik edilen dijital araçlar ve pratikler kişisel verilerin tehdit altına girmesinden veri güvenliği problemlerine, algoritmaların önyargı ile işlenmesine bağlı olarak ayrımcı ve eşitsiz uygulamalara, kötü niyetli kişiler eliyle gerçekleştirilecek siber saldırılara sebep olabilmektedir. Sınır güvenliğinin idamesinde kullanılan yapay zekâ uygulamaları insan faktörünün önemini geri plana attığından karar alma sürecinde de bazı zorlukları beraberinde getirmektedir. Kişisel tecrübe ve içgörüden soyutlanmış olan ve kimi zaman teknik sorunlarla karşı karşıya kalma potansiyeli yüksek olan yapay zekâ eksik veya hatalı kararların alınmasına, karar alma sürecinde gecikmelere yol açabilmektedir. Verilerin kötüye kullanımı ya da sızdırılması mahremiyet bağlamında ciddi sorunlar ortaya çıkarabilmekte, etik sorunlar doğurabilmektedir. Bu sebeple politika yapıcılar ve uygulayıcılar yapay zekânın beraberinde getirdiği olumlu özellikler yanında karşılaşılabilecek olumsuzlukları da değerlendirmelidir. Gerek belirli bir ülke içerisinde uygulanması sırasında, gerekse de ülkeler arasında iş birliği sürecinde yapay zekâ tarafından üretilen verilerin ve kararların sürekli gözden geçirilmesi, iyileştirmeler yapılması elzemdir. Yapay zekânın kullanımına ilişkin genel-özel standartların oluşturulması, şeffaflık, hesap verebilirlik ve mahremiyete yönelik etik kaygıların giderilmesi gerekmektedir. Ayrıca sınır geçişleri ile kontrolleri sırasında önyargıdan beslenen, ayrımcılığa dayalı haksız uygulamalara yer verme ihtimali olan bilgi ve değerlendirmelerin beşerî denetimi gerçekleşmeli, insani tecrübe ve öngörü yapay zekâ sistemlerine yansıtılmalıdır.

5. YAPAY ZEKÂ DESTEKLİ SINIR GÜVENLİĞİ UYGULAMALARINA KÜRESEL YAKLAŞIMLAR

Sınır güvenliğine yönelik önlemler dünya genelinde ülkeden ülkeye değişiklik göstermektedir. Devletler radar sistemleri, sismik, akustik veya kızılötesi teknolojiye sahip sabit yer sensörleri, insansız hava araçları (İHA), hava gemileri, mobil gözetleme sistemleri, entegre iletişim sistemleri, iletişim istihbaratı ve sinyal analizi gibi uygulamalara yapay zekâ destekli sınır güvenliği uygulamalarında sıkça yer vermektedir (Brzezinski, 2024, s.3).

Amerika Birleşik Devletleri'nde (ABD) Gümrük ve Sınır Koruma Birimi; insansız hava araçları ve sensörlere ek olarak liman girişlerinde kargo taraması yapmak, kimlik doğrulamak ve sınırda karşılaşılabilecek tehditlere karşı

farkındalığı artırmak amacıyla yapay zekâdan istifade etmektedir. Akışlı video ve görüntülerdeki nesneleri otomatik olarak tanımlamak için yapay zekâ modelleri kullanılmakta; bir anormallik tespit edildiğinde operatörlere gerçek zamanlı uyarılar gönderilmektedir. Bu da ABD’de Gümrük ve Sınır Koruma Biriminin uyuşturucu ve diğer yasa dışı malların ülkeye girmesini durdurma yeteneğini artırmaktadır (Homeland Security, 2024).

Otonom sistemler üzerine uzmanlaşan ve ABD Savunma Bakanlığı ile iş birliği faaliyetlerinde bulunan bir savunma teknolojisi şirketi olan Anduril Endüstri; ABD-Meksika sınırına otonom gözetleme kuleleri yerleştirmiş; bu kuleler, sınırı yasa dışı olarak geçmeye çalışan insanları ve araçları tespit etmek ve izlemek için kameralar, sensörler ve yapay zekâ ile donatılmıştır. Kuleler güneş enerjili tasarımları ve uzaktan yönetim sistemleri sayesinde insan müdahalesi olmadan altı aya kadar otonom olarak çalışabilmekte ve yapay zekâ teknolojisi sayesinde hayvanlar ve insanlar arasında rahatlıkla ayırım yapabilmektedir. Bununla birlikte manevra alanını hızlı bir şekilde değiştirebilen ve şüpheli bir aktivite tespit ettiğinde sınır devriye görevlilerini gerçek zamanlı olarak uyarabilen otonom gözetleme kuleleri yasa dışı sınır geçişlerini azaltmada ve sınır güvenliğini artırmada başarılı bir uygulama örneği oluşturmaktadır (Taridial, 2023).

ABD örneğinde olduğu gibi AB de, sınır güvenliğini sağlamakla görevli kolluk birimlerinin sınır gözetim kapasitesini artırmak amacıyla yoğun çaba harcamaktadır. AB’nin sınır kontrolü ve sınır güvenliği bağlamında kullandığı veya kullanmayı düşündüğü başlıca yapay zekâ uygulamaları biyometrik tanımlama (otomatik parmak izi ve yüz tanıma); duygu tespiti, algoritmik risk değerlendirmesi ve göç izleme, analizi ve tahmini için yapay zekâ araçlarının kullanılmasıdır (European Parliament, 2021). Bu dört temel uygulamalar dışında sınır güvenliğini daha işlevsel hâle getirmek için proje çalışmaları yürütülmektedir.

AB; biyometrik verilerle ilgili kapsamlı bir veri tabanı oluşturmak maksadıyla iborderCTRL (Akıllı Taşınabilir Kontrol Sistemi) projesini geliştirmiştir. Macaristan, Yunanistan ve Letonya sınırları arasındaki geçiş noktasında yapay zekâ destekli yalan dedektörünü içeren uygulama sürecinde sınıra giriş yapan şahıslardan önce pasaport ve vize gibi giriş için gerekli olan belgeleri sisteme yüklemeleri istenmekte, çevrim içi başvuru formu doldurtulmakta, akabinde ise sanal sınır koruma memuru üzerinden çantanın içinde ne olduğuna yönelik ya da seyahat amacına ilişkin bazı sorular

yöneltilmektedir. Kamera karşısında sorulan sorulara cevap veren şahısların mimikleri sensörler ve yapay zekâ veri tabanı ile analiz edilerek yüz ifadelerinden söylemleriyle ilgili çelişki var mı diye çıkarımlarda bulunmaktadır (Şahiner, Ayhan ve Önder, 2021, s.89).

AB’de mevcut sınır gözetim kapasitesini güçlendirmek için REBORDER projesi geliştirilmiş; otonom bir sınır gözetim sisteminin tatbik edilmesi amaçlanmıştır. Projenin hedefleri arasında çok modlu sensörlerle donatılmış İHA’lar, suç faaliyetlerinin ve deniz kirliliğine ilişkin eylemlerin erken teşhis edilebilmesi için gelişmiş tespit yeteneğine haiz teknolojilerin kullanılması bulunmaktadır (European Commission, 2022). Sınır boyunca şüpheli eylemler; sensörler, kameralar ya da İHA’lar tarafından gözetilmektedir. Yapay zekâ tabanlı yazımlar sayesinde cihazlar üzerinden toplanan veriler işlenmekte ve sınır güvenliğine hanel getirecek olası tehditler konusunda sınır görevlileri anında uyarılmaktadır (Taridial, 2023).

Çin’de sınırlarda yüz tanıma ve termal kamera sistemlerinin konuşlandırılmasına ek olarak son beş yıllık süre içerisinde veri analizine dayalı karar destek sisteminin sınır ötesi güvenlik yönetiminin sağlanmasında etkili sonuç doğuracağı değerlendirilmektedir. Sanayi ve Bilgi Teknolojileri Bakanlığı tarafından sınır ötesi veri akışının güçlendirilmesi ve 2025 yılına kadar büyük verilerin optimizasyonun sağlanması amaçlanmaktadır (Reuters, 2021).

Avusturalya Sınır Gücü (ABF) gerek operasyonel faaliyetlerde gerekse de sınır güvenliğine ve yönetimine ilişkin analizlerinde yapay zekâdan yararlanmaktadır. Avusturalya Sınır Gücü ülke topraklarına yönelik seyahatlerde ve girişlerde muhtemel güvenlik risklerini tespit etme, uluslararası posta ve kargo alanındaki yasa dışı malların akışını kesme; görüntü işleme tekniklerini kullanarak sahte belgeleri belirleme, doğal dil işleme ile serbest formatta yazılmış metinlerden önemli varlık bilgileri hakkında çıkarımda bulunma ve sınır güvenliğine yönelik tehditleri engelleme bağlamında gelişmiş analizler kullanmaktadır (Australian Government Department of Home Affairs, 2024). Avusturalya Sınır Gücü sınırıyla ilgili her türlü tehdit, risk ve güvenlik açıklarının bertaraf edilmesi, suçların hemen tespiti ve önlenmesi açısından veri paylaşımına ve gelişmiş veri analizine kayda değer önem atfetmektedir (Outram, 2024). Avusturalya’da yapay zekâ ile entegre gözetleme sistemleri, dronlar ve gemilerle düzensiz göç ve kaçakçılık faaliyetlerine ilişkin gözetim gerçekleşmekte, biyometrik tanıma sistemleri aracılığıyla kimlik doğrulaması yapılmaktadır.

Hindistan'da yapay zekâ ile bütünleşmiş aygıtlar sınır gözetiminin sistemli bir yapıya kavuşmasında önemli rol oynamaktadır. Pakistan ve Bangladeş ile olan sınırında Hindistan'ın yapay zekâdan yararlandığı görülmektedir. Sınır ihlallerini tespit etmeye, hedef sınıflandırmasına ve savunma operasyonlarının doğruluğunu artırmaya yardımcı olan sensörler, gözetleme kameraları, veri analizi aygıtları, insansız hava araçları, otonom zırhlı araçlar ve robotlar Hindistan kuvvetleri tarafından kullanılmaktadır (Shankar IAS Parliament, 2023).

Dünya genelinde sınır geçişlerinde yararlanılan ve hızlı bir şekilde yayılma özelliği gösteren teknolojik uygulamalardan biri gözün iris tabakasının taranması şeklinde biyometrik güvenliğin sağlanmasına yönelik 'iris' tanıma sistemidir. Birleşik Arap Emirlikleri, Türkmenistan, Hindistan, İsrail, Birleşik Krallık gibi ülkelerde örnekleri olan iris tanıma uygulaması esasında hem sistemsel açıdan yapay zekâ ile çalışan hem de gözün iris tabakasına dış kaynaklardan yapay zekâ ile müdahale edilmesinin zorluğu sebebi ile yapay zekâdan soyutlanabilen bir özellik arz etmektedir. İris tanıma sisteminde sınır kapılarında kontroller sırasında kişilerin iris desenleri taranarak kimlik doğrulaması yapılmakta ve daha önce sistemde yer alan verilere yönelik eşleşme gerçekleştiğinde sınır geçişlerine müsaade edilmektedir. İris tanıma teknolojisi sınır güvenliğinin muhafaza edilmesinde yüksek güvenli bir sınır geçişi sağlamaktadır. Bireylerin parmak izlerinin dokundukları yerden kötü niyetli kişilerce alınabileceği, sesinin yapay zekâ ya da derin öğrenme teknikleri kullanılarak montaj yardımıyla (deepfake) taklit edilebileceği veya estetik bir operasyonla bir şahsın yüzünün bir diğerine benzetilebileceği düşünüldüğünde; gözün iris desenine yönelik yeniden yapılandırma veya manipüle etme neredeyse hiç mümkün değildir. Çünkü iris deseni 1 yaşından sonra yaşam boyu sabit kalmakta, her iki göz de benzersiz bir yapı arz etmekte, insanlar ikiz bile olsalar DNA'sı aynı olmakla birlikte iris desenleri farklılık içermekte, tek bir insan gözünde 240'tan fazla değişken (serbestlik derecesi) bulunmakta ve aynı iris desenine sahip iki bireyin olasılığı $1:10^{78}$ olmaktadır (Kaya, 2024, s.49). İris tanıma teknolojisi benzersizlik, doğruluk, dış müdahalelere kapalı olma, sahteciliği azaltma, devletin vatandaşın kimliğini doğrulamasını istediği herhangi bir alanda ya da her türlü kamu hizmeti sunumunda yararlanılabilmesi sebebiyle avantaj sağlamaktadır. Kısa sürede tarama ve eşleşme yapma özelliği ile hızlı bir uygulama sürecini beraberinde getirmektedir. Bununla birlikte diğer biyometrik güvenlik sistemleri ile mukayese edildiğinde donanım maliyeti açısından pahalı olsa da veri merkezine

yapılacak yatırım maliyeti, toplam sahip olma ve işlem maliyeti esas alındığında ekonomik açıdan daha da avantaj sağlamaktadır.

6. TÜRKİYE’DE SINIR GÜVENLİĞİNİN SAĞLANMASINDA YAPAY ZEKÂ UYGULAMALARI

Türkiye 2021-2025 yılları arasını kapsayan Ulusal Yapay Zekâ Stratejisi’ni belirleyerek yapay zekâ alanında kapsamlı bir yol haritası oluşturmuştur. Veriye dayalı karar alma, kamu kurum ve kuruluşlarının yeni nesil teknolojileri adapte eder hâle gelmesi, ilgili bakanlıklar tarafından yapay zekâ projelerinin geliştirilmesi, çalışmaların hızlandırılması ve yapay zekâ ekosisteminin olgunluk seviyesinin artırılması ulusal yapay zekâ stratejisinin önemli hedeflerinden olmuştur (Cumhurbaşkanlığı, 2021, s.8).

Teknolojik ilerlemelere ve gelişmelere bağlı olarak dünyada sınır güvenliğini sağlamaya yönelik küresel eğilimlere paralel şekilde, Türkiye de diğer alanlarda olduğu gibi sınır yönetiminde ve sınır güvenliğinin sağlanmasında yapay zekâ ile entegre uygulamalara yoğunlaşmaktadır. Türkiye sınır güvenliğini tahkim ederken çitler, duvarlar, kuleler, tel örgüler gibi geleneksel güvenlik uygulamaları yanında sınırlarında modern ve gelişmiş sınır güvenliği teknolojilerine yer vermektedir. Bu bağlamda; termal kameralar, sensörler, İHA’lar, kızılötesi görüntüleme sistemleri, otonom balon gözetim sistemi uygulamaları ve erken uyarı sistemleri Türkiye’nin sınır güvenliği yönetiminde öne çıkan başlıca araçlar arasındadır.

Türkiye’nin güneydoğu sınırında sınır gözetim kapasitesinin artırılmasına yönelik çabalar kapsamında hedef koordinatların yüksek bir hassasiyetle belirlenmesini sağlayan ‘dragoneye elektro-optik sensör sistemi’ uygulanmaya başlamıştır. Türkiye’nin Hatay, Gaziantep, Kilis, Şanlıurfa, Mardin ve Şırnak illerindeki hudut birimleri tarafından kullanılması amaçlanan elektro-optik sensör sistemi ASELSAN tarafından geliştirilmiştir (ASELSAN, 2021).

HAVELSAN tarafından geliştirilen teknolojiler, Türkiye’de sınır güvenliğinin sağlanmasında önemli bir rol oynamaktadır. Bu teknolojiler arasında; sınır bölgelerinde sensörlerden gelen verilerin haritalar üzerinde izlenmesini sağlayan sistemler, sahil gözetleme ve radar sistemi (SGRS), görüntü ve video teknolojileri ile biyometrik veri teknolojileri yer almaktadır. Ayrıca, otonom manevra yeteneğine sahip sürü algoritmalarıyla görev yapan BARKAN, SANCAR, BAHA ve KAPGAN gibi insansız kara ve deniz araçları da bu kapsamda etkin bir şekilde kullanılmaktadır (savunmasanayist.com, 2023).

Türkiye sınırlarında 5 metre yüksekliğinde engel sistemi, beton duvarlar, tel çitler, devriye yolları, sınır aydınlatma ve kamera sistemleri, Mardin, Urfa gibi illerde solar enerjili aydınlatma sistemi, harekât duyarlı sensörler, asansör kuleler, keşif gözetleme aracı, 10.000 metreden insanı algılayan ve en az 4.000 metreden insan tanıma sistemine sahip elektro optik kuleler bulunmaktadır. Bu elektro optik kuleler bir çatışma ile karşı karşıya kalındığında atış yerini tespit etme kapasitesine sahip olup kablosuz veri akışına haizdir (Haber Türk, 2024).

Türkiye'nin jeopolitik konumu ve çevresindeki ülkeler dikkate alındığında göç rotası açısından kimi zaman göç akınları ile karşılaşabilmektedir. Komşu ülkelerdeki istikrarsızlıklar ve iç çatışmalar sebebiyle kaçakçılık, terör, yasa dışı ticaret gibi faaliyetler açısından kritik bir coğrafyada yer almaktadır. 2.753 km kara sınırı uzunluğuna, adalar dahil 8.333 km sahil uzunluğuna, 783.356 km² kara parçasına ve 9.820 km² su alanlarına sahip Türkiye'de kara ve deniz sınırının kontrolü girift bir hâl alabilmektedir. Ayrıca konvansiyonel tehditlere ek olarak konvansiyonel olmayan düzensiz ve asimetrik tehditlerin devletleri riske atması Türkiye'de sınırların modern teknolojilerle donatılmasını, teknoloji merkezli gözetleme, koruma ve müdahale mekanizmasını zorunlu kılmaktadır (Seren ve Yeşiltaş, 2017).

Yapay zekâ ile entegre modern teknolojilerin Türkiye sınırlarında kullanılması düzensiz göç gibi yasa dışı sınır geçişlerinin önlenmesini, sınır bölgelerinde gerçekleşmesi muhtemel ihlallerin tespitini, izlenmesini ve iyileştirilmesini kolaylaştırmaktadır. Türkiye'nin özellikle Doğu Anadolu bölgesindeki dağlık ve engebeli arazi şartları göz önünde bulundurulduğunda anlık veri paylaşımı ve analiz kapasitesine sahip yapay zekâ destekli teknolojik aygıtlar sınır güvenliğinin daha etkili ve etkin bir yapıya kavuşturulmasına ivme kazandırmaktadır.

2024-2028 yıllarını kapsayan 12. Kalkınma Planı'nda Türkiye'de dijital dönüşümün ve yapay zekâ alanındaki gelişmelerin hızlı bir şekilde devam ettiği belirtilmekte; güvenlik hizmetlerinin ifa edilmesinde yapay zekâ, robot teknolojisi, büyük veri analizi, uzay teknolojisi gibi gelişmelerden azami derecede faydalanılacağı ve bu alanda yerli teknoloji ve üretim kapasitesinin artırılacağı ifade edilmektedir (Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023, s. 226). Politika ve tedbirler kapsamında sınır güvenliğine ilişkin olarak Türkiye'de sınır güvenliğinin daha etkin bir yapıya kavuşturulacağı, iş birliğine dayalı analiz ve raporlama faaliyetleri açısından teknolojik ve fiziksel alt yapının güçlendirileceği, kara sınırlarında güvenlik bariyerlerinin, güvenlik

yollarının, sensör sistemlerinin ve izleme kulelerinin güçlendirileceği, sahil güvenlik konusunda ise kontrol noktaları, liman, rıhtım ve ekipman altyapısının optimize edileceği dile getirilmektedir (Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2023, s. 225).

Türkiye'nin sınır yönetimi stratejisinde sınır güvenliğinin etkin bir şekilde tahkim edilmesi için yapay zekâ ile entegre uygulamaların geliştirilmesi ve sürekli iyileştirmeler yapılması oldukça önemlidir. Anlık veri işleme ve analiz etme, tehdit tespiti yapma ve hızlı müdahale bulunma yeteneğini bünyesinde barındıran yapay zekâ teknolojilerinin sınır yönetimi anlayışı için stratejik olarak ön plana çıkarılması yalnızca sınır güvenliğinin sağlanmasına pozitif katkı sunmakla kalmayıp aynı zamanda kaynak tahsisi açısından da olumlu etki yaratmaktadır. İçinde bulunduğumuz dijitalleşme çağında sınır güvenliğinden sorumlu birimlerin yeni teknolojilerle uyumlu bir şekilde mesleki eğitimlerine ağırlık verilmesi ve farkındalıklarının artırılması hiç olmadığı kadar önem kazanmıştır.

SONUÇ

Küresel gelişmeler, tehditler ve riskler dikkate alındığında pek çok gelişmiş ülke sınır güvenliği tedbirlerinde, yapay zekâ ile entegre modern teknolojilerin uygulanmasına hiç olmadığı kadar ağırlık vermeye başlamıştır. Biyometrik doğrulama teknolojilerinden otonom gözetleme kulelerine ve zırhlı araçlara; görüntü işleme tekniklerinden veri analizi aygıtlarına, sensörlerden sınır geçişlerinde sorgulama yapan robotlara ve gözün iris tabakasından kimlik doğrulamaya kadar yapay zekâ ile entegre sınır güvenliği önlemleri artırılmaktadır.

Türkiye; küresel eğilimlere paralel şekilde uluslararası gelişmeleri yakından takip ederek mümkün mertebe yerli ve millî imkânlar doğrultusunda sınır yönetimi stratejisinde yapay zekâ destekli uygulamalara yer vermektedir. Türkiye, sınırlarında geleneksel güvenlik tedbirleri yanında sınır gözetim sistemini güçlü bir şekilde tahkim etmek maksadıyla modern teknolojilerden istifade etmektedir. Dünya genelinde modern teknolojilerden yararlanan diğer devletler gibi Türkiye'nin de kendi jeopolitik konumunu, konvansiyonel ve yeni nesil güvenlik tehditlerinin yapısını, yapay zekânın beraberinde getirdiği olumlu ve olumsuz etkileri birlikte değerlendirerek, bu yöndeki çabalarına aynı hassasiyetle ivme kazandırması gereklidir.

Yapay zekâ sınır güvenliğine yönelik risk ve tehditlerin tasfiye edilmesinde hızlı müdahale etme yeteneğine, sınır yönetiminden sorumlu birimlerin daha rasyonel ve etkili karar almasına, yüksek doğruluk ve güvenilirlik seviyesine haizdir. Bununla birlikte yapay zekâ destekli teknolojiler şeffaflık, hesap verebilirlik, mahremiyet gibi etik kaygılara sebep olmakta; algoritmik ya da teknolojik belirsizlikler veya önyargıya dayalı veri analizi gibi etmenler sebebiyle birtakım olumsuzlukları da beraberinde getirebilmektedir. Bu nedenle pek çok alanda olduğu gibi sınır güvenliğine ilişkin yönetsel süreçte de ortaya çıkması muhtemel sorunların politika yapıcılar ve uygulayıcılar tarafından detaylı olarak değerlendirilmesi gerekmektedir.

Teknik boyuttan kaynaklanan sorunları en aza indirmek için düzenli güncellemeler yapılmalı, algoritmaların mevcut verilerle uyumu sürekli denetlenmelidir. İnsan denetimini merkeze alan bir kontrol mekanizmasından yararlanılarak muhtemel hataları ya da etik sorunları önlemek için hassas davranılmalıdır. Algoritmaların önyargılı hatalı genellemelerde veya çıkarımlarda bulunmasını önlemek adına veri setlerinin çeşitliliği artırılmalıdır. Üretilen çıktıların mantığını ve alınan kararların arkasında yatan etmenleri anlamak için “Nasıl?” ve “Neden?” sorularına cevap vererek etik ve yasal endişeleri gideren ‘açıklanabilir yapay zekâ’ sistemleri geliştirilmelidir. Ülkeler yapay zekâyı pasif bir şekilde ‘kullanan’ tarafta olmaktan ziyade aktif bir şekilde ‘üreten’ tarafta yer almalıdır. Bu nedenle yerli ve millî yatırımlara ağırlık verilerek Ar-Ge sürecinin ulusal kaynaklarla desteklenmesi hayati önem taşımaktadır. Hukuki ve etik açıdan ise yapay zekânın hatalı kararlarından doğabilecek sorumluluğunun kime ait olduğunu belirlemek için yasal düzenlemelere ihtiyaç duyulmaktadır. Üretici ve uygulayıcıların hukuki yükümlülükleri ve sorumluluklarının çerçevesinin net bir şekilde belirlenmesi gerekmektedir. Özellikle veri paylaşımına ilişkin güvenli veri paylaşım platformlarının oluşturulması, etik standartların geliştirilerek yapay zekâ etiğinin yaygınlaştırılması elzemdir. Yapay zekâ araçlarında işlenecek bireylere ait hassas verilerin mahremiyeti titizlikle sağlanmalı, veri sızıntılarının ve kötüye kullanımından doğabilecek risklerin önüne geçilmelidir.

KAYNAKÇA

- Adaş, E. B. ve Erbay, B. (2022). Yapay zekâ sosyolojisi üzerine bir değerlendirme. *Gaziantep Üniversitesi Sosyal Bilimler Dergisi*, 12(1), 326-337.
- Arf, C. (1958). Makine düşünebilir mi? Atatürk Üniversitesi Üniversite Çalışmalarını Muhite Yayma ve Halk Eğitimi Yayınları Konferanslar Serisi 1, 91-103.
- ASELSAN. (2021). Sınır güvenliği. Erişim tarihi: 10 Eylül 2024, <https://www.aselsan.com/tr/haberler/detay/16/sinir-guvenligi->
- Australian Government Department of Home Affairs. (2024). Freedom of information request – FA 24/05/01409. Erişim tarihi: 09 Eylül 2024, <https://www.homeaffairs.gov.au/foi/files/2024/fa-240501409-document-released.pdf>
- Brzezinski, J. (2024). *Augmenting Border Security & Defense*. White Paper, CRFS.
- Collins, C., Dennehy, D., Conboy, K. ve Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, 60, 1-17. doi:10.1016/j.ijinfomgt.2021.102383
- Coşkun F. ve Gülleroğlu, D. H. (2021). Yapay zekânın tarih içindeki gelişimi ve eğitimde kullanılması. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 54(3), 947-966. doi:10.30964/auebfd.916220
- Cumhurbaşkanlığı (2021). *Ulusal Yapay Zekâ Stratejisi 2021-2025*. Ankara.
- Dogget, L. S. (2023). Artificial intelligence AI is ‘buzz’ word of the year, but what exactly is it? *FAOPMA Magazine*. Erişim tarihi: 30 Mayıs 2024, https://faopma.com/JournalDetail/4107/FAOPMA_Magazine_2023_Jul
- EU Artificial Intelligence Act (2024). Article 3: definitions. Erişim tarihi: 4 Mart 2025, <https://artificialintelligenceact.eu/article/3/>
- European Commission. (2022). Autonomous swarm of heterogeneous Robots for BORDER surveillance. Erişim tarihi: 08 Eylül 2024, <https://cordis.europa.eu/project/id/740593/results>

- European Parliament. (2021). *Artificial intelligence at EU borders: Overview of applications and key issues*. European Parliament, Brussels. Erişim tarihi: 08 Eylül 2024, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf)
- Escenbach, W. J. (2021). Transparency and the black box problem: why we do not trust AI. *Philos. Technol.* 34, 1607–1622.
- Faist, T. (2009). Making and remaking the transnational: of boundaries, social spaces and social mechanisms. *Spectrum: Journal of Global Studies*, 1(2), 67-89.
- Ferrara, E. (2024). Fairness and bias in artificial intelligence: a brief survey of sources, impacts, and mitigation strategies. *Systematic Review*, 6 (3), 1-15.
- Gang, P. (2019). On Defining Artificial Intelligence. *Journal of Artificial General Intelligence*, 10(2), 1-37.
- Gbadegeshin, S.A., Natsheh, A. A, Ghafel, K., Tikkanen, J., Gray, A., Rimpiläinen A., Kuoppala A., Poranen-Kalermo J. ve Hirvonen, N. (2021). What is an artificial intelligence (AI): A simple buzzword or a worthwhile inevitability?. 14th Annual International Conference of Education, Research and Innovation Proceedings of ICERI2021 içinde (ss. 468-479). Online Conference: doi:10.21125/iceri.2021.0171
- Global Counterterrorism Forum (GCTF). (2016). Good practices in the area of border security and management in the context of counterterrorism and stemming the flow of “foreign terrorist fighters”. Erişim tarihi: 23 Ağustos 2024, <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2016%20and%20before/GCTF-Good-Practices%20BSM-ENG.pdf?ver=2016-09-13-124953-540>
- Guan, H., Dong, L. ve Zhao, A. (2022). Ethical risk factors and mechanisms in artificial intelligence decision making. *Behavioral Sciences*, 12(9), 1-17. doi:10.3390/bs12090343
- Gugerty, L. (2006). Newell and Simon’s logic theorist: Historical background and impact on cognitive modeling. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 50(9), 880-884. doi:10.1177/154193120605000904

- Güneysu, G. (2024). Autonomous weapon systems and the humanitarian principle of distinction. *Annales de la Faculté de Droit d'Istanbul*, 74, 133-153.
- Güven, M. (2024). AI-based surveillance system proposal for the second line of defense against irregular migration, smuggling, and terrorism: gendarmerie assessment. *Güvenlik Bilimleri Dergisi*, 13(1), 63-84.
- Haber Türk. (2024). *Sınır güvenliği nasıl sağlanıyor? İçişleri Bakanı Ali Yerlikaya soruları yanıtlıyor – Özel röportaj* [TV Haberi]. Haber Türk TV, 09 Ağustos 2024.
- Hashmat, S. (2017). Border security, T. Sakman, T. (Ed), *Devletin doğasının değişimi: güvenliğin sınırları* (ss.263-268). İstanbul: TASAM Yayınları.
- Homeland Security. (2024). Using AI to secure the homeland. Erişim tarihi: 07 Eylül 2024, <https://www.dhs.gov/ai/using-ai-to-secure-the-homeland>
- International Organization for Migration (IOM). (2017). *Border security, migration governance and sovereignty*. Geneva: IOM Publications.
- International Organization for Standardization (ISO). (2022). ISO/IEC 22989:2022 – Information technology – Artificial intelligence – Artificial intelligence concepts and terminology. Erişim tarihi: 30 Mayıs 2024, <https://www.iso.org/standard/74296.html>
- İrdem, İ., Alkan Ö., Gören, K. B. ve Arslan, Ö. (2021). Güvenlik yönetiminde çağdaş yaklaşımlar. Ankara: Polis Akademisi Yayınları.
- İrdem, İ. ve Çobanoğlu, S. (2021). Yapay zekânın iç güvenlik yönetimi üzerine yansımaları: siber güvenlik. *KAYTEK Dergisi*, 3(2), 175-202.
- İşcan, H. ve Kaygısız A.D. (2024). Yapay zekâ: alt dalları ve uygulama alanları, Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(4), 201-234.
- Kaya, S. A. (2024). Enhancing border security through biometric identification and humanitarian principles. *Border Security Report*. Erişim tarihi: 30 Mayıs 2024, <https://www.border-security-report.com/enhancing-border-security-through-biometric-identification-and-humanitarian-principles/>
- Kılıçarslan, S. K. (2019). Yapay zekânın hukuki statüsü ve hukuki kişiliği üzerine tartışmalar. *Yıldırım Beyazıt Hukuk Dergisi*, 2, 363-389.

- Kolossov V. ve Scott J. (2013). Selected conceptual issues in border studies. *Belgeo*, 1. doi:10.4000/belgeo.10532
- Küçük, Ç. M. (2024). Yapay zekânın hukuk sisteminde kullanılması. *Bilişim Hukuku Dergisi*, 6(1), 24-79.
- Manjarrez, M. V. (2015). Border security: defining it is the real challenge. *Homeland Security & Emergency Management*, 12(4), 793-800.
- Martinez, R. (2019). Artificial intelligence: distinguishing between types & definitions. *Nev Ada Law Journal*, 19(3), 1015-1042.
- Outram, M. (2024). How the Australian Border Force can exploit AI. Erişim tarihi: 09 Eylül 2024, <https://www.aspistrategist.org.au/how-the-australian-border-force-can-exploit-ai>
- Reuters. (2021). China seeks better cross-border control of big data with new plan. Erişim tarihi: 09 Eylül 2024, <https://www.reuters.com/technology/china-urges-stronger-cross-border-security-big-data-2021-11-30>
- Sarı, F. (2021). Cahit Arf'ın "makine düşünebilir mi ve nasıl düşünebilir?" adlı makalesi üzerine bir çalışma. *TRT Akademi*, 6(13), 812-832.
- Savunmasanayist.com. (2023). Sınırlarımızı HAVELSAN'ın geliştirdiği yapay zeka koruyacak. Erişim tarihi: 10 Eylül 2024, <https://www.savunmasanayist.com/sinirlarimizi-havelsanin-gelistirdigi-yapay-zeka-koruyacak>
- Seren, M. ve Yeşiltaş, M. (2017). Türkiye'nin sınır politikası teknoloji ağırlıklı. *SETAV*. Erişim tarihi: 10 Eylül 2024, <https://www.setav.org/yorum/turkiyenin-sinir-politikasi-teknoloji-agirlikli>
- Shankar IAS Parliament. (2023). AI in Defence Sector. Erişim tarihi: 09 Eylül 2024, <https://www.shankariasparliament.com/current-affairs/ai-in-defence-sector>
- Simmons, A. B. ve Kenwick, R. M. (2022). Border orientation in a globalizing world. *American Journal of Political Science*, 66(4), 853-870. doi: 10.1111/ajps.12687
- Skeikh, H., Prins, C. ve Schrijvers, E. (2023). *Mission AI: The new system technology*. Netherlands: Springer.

- Smith L. M. ve Seward, K. R. (2023). Artificial intelligence and development. M. Clarke ve X. A. Zhao (Ed.), *Elgar encyclophedia of development* içinde (ss. 42-47). Northampton, MA: Elgar Publishing.
- Spiro, E. D. (2010). Criminalizing immigration: The Social construction of borders and national security. *SSRN*. Erişim tarihi: 05 Eylül 2024, <https://ssrn.com/abstract=1515466>
- Storey, D. (2007). Europe's shifting borders: Rhetoric and reality. Erişim tarihi: 05 Eylül 2024, http://eprints.worc.ac.uk/458/1/Borders_%282%29.pdf
- Świerczyńska, J. (2023). The importance of border surveillance and border traffic control at the eastern border of the Republic of Poland to the cross-border security of the European Union. *Central European Review of Economics & Finance*, 44(3), 153-174. doi:10.24136/ceref.2023.018
- Şahiner, M. K., Ayhan, E. ve Önder, M. (2021). Yeni sınır güvenliği anlayışında yapay zekâ yönetişi: Fırsatlar ve tehditler. *Uludağ Uluslararası Çalışmalar Dergisi*, 5(2), 83-95.
- T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2023). *On İkinci Kalkınma Planı (2024-2028)*. Erişim tarihi: 12 Eylül 2024, https://www.sbb.gov.tr/wp-content/uploads/2023/12/On-Ikinci-Kalkinma-Plani_2024-2028_11122023.pdf
- Taridial. (2023). How AI is changing border protection. Erişim tarihi: 08 Eylül 2024, <https://tarideal.com/how-ai-is-changing-border-protection/#:~:text=A%20network%20of%20sensors%2C%20cameras,patrol%20agents%20in%20real%2Dtime>
- United Nations Human Rights Office of the High Commissioner (OHCHR). (2023). *Digital border governance: A human rights based approach*. Colchester: University of Essex.