

Artificial Intelligence-Based Border Technologies and Digital Migration Security in Türkiye

Yapay Zekâ Destekli Sınır Teknolojileri: Türkiye'nin Dijital Göç Güvenliği

Kübra Betül Biçen Gören*

Abstract: In recent years, mass migration movements have led to significant transformations in national and international security policies. During this period, the integration of new technologies has become inevitable across various domains, such as border security, identity verification, risk analysis, and humanitarian aid coordination. Artificial intelligence (AI) technologies have consequently emerged as vital tools in the field of migration security. This study examines AI-supported migration security practices within the context of migration crises, focusing specifically on biometric identification, risk analysis, and real-time monitoring systems. Through a holistic approach, the research evaluates their implementation methods, operational advantages, and the accompanying ethical, legal, and societal challenges. Conducted within a qualitative research framework, the study analyzes official documents published by institutions under the Ministry of Interior of the Republic of Türkiye, alongside reports from international organizations such as UNHCR, IOM, and FRONTEX, utilizing document analysis. The findings indicate that while AI-supported applications may increase the vulnerability of migrants, security-oriented approaches also play a decisive role in social integration processes. In this context, the study aims to rethink the relationship between technology and society from a social science perspective, emphasizing the critical importance of human rights, transparency, and accountability in migration management.

Keywords: Artificial Intelligence, Migration Security, Syrian Crisis, Biometric Identification, Border Management

Öz: Son yıllarda yaşanan kitlesel göç hareketleri, ulusal ve uluslararası güvenlik politikalarında köklü değişimlere yol açmıştır. Bu süreçte sınır güvenliğinden kimlik doğrulamaya, risk analizinden insani yardım koordinasyonuna kadar pek çok alanda yeni teknolojilerin devreye alınması kaçınılmaz hâle gelmiştir. Yapay zekâ (YZ) teknolojileri, büyük veri analizi, gerçek zamanlı izleme ve otomatik karar destek sistemleri gibi yetenekleri sayesinde göç güvenliği alanında önemli bir araç hâline gelmiştir. Bu çalışmada, YZ destekli göç güvenliği uygulamaları göç krizi bağlamında ele alınmaktadır. Söz konusu teknolojilerin uygulama biçimleri, operasyonel avantajları ve beraberinde getirdiği etik, hukuki ve toplumsal sorunlar bütüncül bir yaklaşımla değerlendirilmektedir. Nitel araştırma yöntemi çerçevesinde yürütülen çalışmada, Türkiye Cumhuriyeti İçişleri

* Asst. Prof. Dr., Police Academy, Institute of Security Sciences, Department of International Security
Dr. Öğr. Üyesi, Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Uluslararası Güvenlik Ana Bilim Dalı
ORCID <https://orcid.org/0000-0002-1145-7642>
betulbicen@hotmail.com

Cite as/ Atıf: Biçen Gören, K. B. (2026). Artificial intelligence-based border technologies and digital migration security in Türkiye / Yapay zekâ destekli sınır teknolojileri: Türkiye'nin dijital göç güvenliği. *Turkish Studies-Economics, Finance, Politics*, 21(3), 4335-4385. Ankara Bilim University Publications.
<https://dx.doi.org/10.7827/TurkishStudies.88226>

Received/Geliş: 07 November/Kasım 2025

Accepted/Kabul: 15 September/Eylül 2026

Published/Yayın: 25 September/Eylül 2026

Checked by plagiarism software



Bakanlığı'na bağlı kurumların yayımladığı resmi belgeler ile UNHCR, IOM ve FRONTEX gibi kuruluşların raporları doküman analizi yöntemiyle incelenmiştir. Araştırma bulguları, yapay zekâ destekli uygulamaların göçmenlerin kırılganlığını artırabileceği gibi, güvenlik temelli yaklaşımların sosyal bütünleşme süreçleri üzerinde de belirleyici rol oynadığını ortaya koymaktadır. Bu bağlamda çalışma, teknoloji toplum ilişkisini sosyal bilimsel bir perspektifle yeniden düşünmeyi amaçlamaktadır. Ayrıca göç yönetiminde insan hakları, şeffaflık ve hesap verebilirlik ilkelerinin önemine vurgu yapmaktadır.

Anahtar Kelimeler: Yapay Zekâ, Göç Güvenliği, Suriye Krizi, Biyometrik Kimlik Doğrulama, Sınır Yönetimi.

Structured Abstract

Over the past decade, the escalating complexity and volumetric scale of irregular migration flows have fundamentally reconfigured national and international security priorities. Traditional paradigms of border management have proved inadequate in addressing contemporary migratory mobilities characterized by transnational illicit networks, high-velocity movement, and systemic humanitarian emergencies. Consequently, the integration of artificial intelligence (AI) technologies into border security and migration governance has emerged as a critical structural innovation. AI-enabled systems allow sovereign states to optimize operational efficacy through advanced big data analytics, real-time surveillance, biometric verification, and automated administrative decision-making.

This study investigates how Türkiye has institutionalized AI-supported technologies within its broader migration and border security apparatus, specifically in the post-Syrian crisis landscape. It addresses three core research inquiries: How do AI-driven systems transform the structural governance of migration and security in Türkiye? What are the ensuing ethical, legal, and socio-political implications of these technologies? Why has algorithmic automation become central to Türkiye's digital migration security architecture? By doing so, the study posits Türkiye's empirical trajectory as a critical case study reflecting both the operational utility and the structural tensions of AI integration in contemporary migration governance.

The theoretical framework synthesizes securitization theory and surveillance studies. Drawing upon the Copenhagen School (Buzan, Wæver, & de Wilde, 1998), the research underscores that security threats are constructed not merely through objective metrics of danger, but through the discursive practices of political actors. Consequently, framing migration as an existential security threat legitimizes exceptional governance mechanisms, including pervasive digital surveillance and automated risk profiling.

Furthermore, the study engages the biopolitical analytics of surveillance conceptualized by Foucault (1977) and Lyon (2001). In AI-governed border spaces, the systemic collection, extraction, and categorization of biometric data transform migrants into digitized subjects, thereby reinforcing state sovereignty and asymmetrical power dynamics. Complementing this, Gonzalez's (2019) conceptualization of "digital borders" demonstrates how technological infrastructures project state power far beyond physical territorial demarcations. Thus, AI technologies operate dually as technical instruments and political mechanisms that continuously redefine the juridical and social boundaries of citizenship, identity, and belonging.

By bridging these theoretical lenses, this research conceptualizes AI not as a neutral administrative tool, but as a socio-technical assemblage that embeds specific ideological and normative presuppositions within its algorithmic architecture. The study contributes to the burgeoning literature on the dual-use nature of digital governance in migration management—acting simultaneously as an instrument of administrative efficiency and an apparatus of social control.

Methodologically, the study adopts a qualitative design underpinned by systematic document analysis. Primary empirical data are drawn from official legislative publications, policy declarations, and strategic frameworks promulgated by agencies under the Ministry of Interior of the Republic of Türkiye, most notably the Directorate General of Migration Management (DGMM). Secondary data encompass evaluative reports published by international bodies, including the UNHCR, IOM, FRONTEX, Europol, and the European Commission.

The gathered texts were subjected to thematic coding to isolate patterns in the operationalization of AI technologies across three principal dimensions: (1) biometric identification and digital profiling, (2) algorithmic risk assessment and automated decision support systems, and (3) real-time surveillance protocols and cross-border intelligence interoperability. Analytical reliability was reinforced through cross-source triangulation between national institutional outputs and international reporting, while theoretical sensitivity ensured the interpretation of data remained anchored within securitization and biopolitical frameworks.

The empirical findings demonstrate that Türkiye's digital migration security framework functions as a multi-layered, technologically mediated apparatus. AI-supported instruments are leveraged to augment the precision, velocity, and predictability of border enforcement, thereby fusing disparate administrative databases into an interconnected governance matrix.

Specifically, Türkiye's national *GöçNet* infrastructure consolidates comprehensive biometric records—encompassing fingerprints, facial morphology, and iris scans—of populations under temporary

protection. These datasets facilitate real-time identity authentication, spatial mobility tracking, and administrative risk assessment. Similarly, *Mobile Migration Points*, deployed as AI-enhanced verification units across metropolitan zones, enable decentralized biometric screening and immediate database synchronization. While these innovations consolidate state bureaucratic oversight, they simultaneously generate acute concerns regarding data consent, informational privacy, and inherent algorithmic bias.

Machine learning algorithms scrutinize biographical indicators, transit itineraries, and digital footprints to forecast latent security vulnerabilities. Paralleling the European Union's experimental *iBorderCtrl* framework, emerging technological protocols in Türkiye classify individuals through algorithmic risk metrics that directly inform border clearance or detention protocols. Although such systems maximize administrative efficiency, they carry a high risk of reproducing systemic biases embedded within training datasets, rendering transparency and explainability indispensable prerequisites for protecting procedural due process.

At the infrastructural level, ASELSAN's electro-optic surveillance networks, reinforced by uncrewed aerial vehicles (UAVs) and ground-penetrating radar arrays, provide continuous perimeter oversight.. Moreover, institutionalized data-sharing agreements with Europol, Interpol, and the UNHCR optimize transnational cooperation against human trafficking and smuggling, albeit raising critical questions concerning jurisdictional accountability, data privacy, and state sovereignty.

The broader theoretical discussion reveals that AI-driven infrastructures do more than merely enhance administrative performance; they fundamentally reconstruct state–society relations by expanding the architecture of digital panopticism. The migration-security nexus in Türkiye illustrates how algorithmic governance accelerates the securitization of human mobility, giving rise to novel modalities of inclusion and exclusion across physical and virtual domains.

The study concludes that AI-supported border technologies constitute a profoundly transformative yet structurally ambivalent development in contemporary migration governance. While they afford unprecedented optimization in managing high-volume population movements, they concurrently risk normalizing pervasive digital surveillance and eroding human agency in consequential administrative determinations.

Consequently, the institutionalization of AI within migration security must be governed by strict human rights compliance, emphasizing transparency, proportionality, and institutional accountability. Legal frameworks, including Türkiye's Personal Data Protection Law (KVKK) and the EU's General Data Protection Regulation (GDPR), require harmonization to mitigate the unauthorized exploitation of sensitive biometric information. Ethical algorithmic governance remains a vital prerequisite for preserving the legitimacy of modern digital border regimes.

Ultimately, Türkiye's institutional experience offers valuable empirical insights for states striving to balance national security imperatives with human dignity in the digital era. Future scholarly inquiry must investigate mechanisms for auditing and contesting algorithmic determinations to ensure that artificial intelligence serves as an instrument of equitable facilitation rather than systemic exclusion. Sustainable migration governance necessitates not only advanced technological proficiency, but an uncompromising normative commitment to justice, transparency, and human-centric policymaking.

Keywords: Artificial Intelligence, Migration Security, Syrian Crisis, Biometric Identification, Border Management

الملخص المنظم

على مدى العقد الماضي، أدى التصاعد المستمر في تعقيد تدفقات الهجرة غير النظامية وحجمها إلى إعادة تشكيل جذرية لأولويات الأمن على المستويين الوطني والدولي. وقد أثبتت النماذج التقليدية لإدارة الحدود محدوديتها في التعامل مع أنماط التنقل الهجري المعاصرة التي تتسم بوجود شبكات غير مشروعة عابرة للحدود الوطنية، وسرعة عالية في الحركة، وحالات طوارئ إنسانية ذات طابع بنوي. وبناءً على ذلك، برز إدماج تقنيات الذكاء الاصطناعي المدعومة بالذكاء الاصطناعي للدول ذات السيادة تحسين الكفاءة التشغيلية من خلال التحليلات المتقدمة للبيانات الضخمة، والمراقبة الآنية والتحقق البيومتري، واتخاذ القرارات الإدارية المؤتمتة.

تبحث هذه الدراسة في الكيفية التي قامت بها تركيا بمأسسة التقنيات المدعومة بالذكاء الاصطناعي ضمن منظومتها الأوسع لإدارة الهجرة وأمن الحدود، ولا سيما في السياق الذي تشكل في أعقاب الأزمة السورية. وتنتقل الدراسة من ثلاثة تساؤلات بحثية رئيسة: كيف تعيد الأنظمة القائمة على الذكاء الاصطناعي تشكيل البنية الحوكمية للهجرة والأمن في تركيا؟ وما التداعيات الأخلاقية والقانونية والاجتماعية.

السياسية المترتبة على استخدام هذه التقنيات؟ ولماذا أصبحت الأتمتة الخوارزمية عنصرًا محوريًا في البنية الرقمية لأمن الهجرة في تركيا؟ ومن خلال معالجة هذه التساؤلات، تطرح الدراسة التجربة التركية بوصفها دراسة حالة نقدية تعكس في آن واحد المنفعة التشغيلية والتوترات البنيوية الناجمة عن إدماج الذكاء الاصطناعي في حوكمة الهجرة المعاصرة.

يجمع الإطار النظري للدراسة بين نظرية الأمانة ودراسات المراقبة. واستنادًا إلى مدرسة كوبنهاغن تؤكد الدراسة أن التهديدات الأمنية لا تتشكل استنادًا إلى المؤشرات الموضوعية للخطر فحسب، بل كذلك من خلال (Wilde, 1998) الممارسات الخطابية للفاعلين السياسيين. وبناءً عليه، فإن تأطير الهجرة باعتبارها تهديدًا أمنيًا وجوديًا يضيفي الشرعية على آليات حوكمة استثنائية، بما في ذلك المراقبة الرقمية واسعة النطاق والتميط الآلي للمخاطر.

ففي (Lyon, 2001) ولبون (Foucault, 1977) كما تستند الدراسة إلى التحليلات البيوسياسية للمراقبة كما صاغها فوكو الفضاءات الحدودية الخاضعة لحوكمة الذكاء الاصطناعي، تؤدي عمليات الجمع المنهجي للبيانات البيومترية واستخراجها وتصنيفها إلى تحويل المهاجرين إلى ذوات رقمية، بما يعزز سيادة الدولة ويكرّس علاقات القوة غير المتكافئة. واستكمالًا لهذا المنظور، يوضح مفهوم الكيفية التي تتيج بها البنى التحتية التكنولوجية للدولة إسقاط سلطتها إلى ما وراء (Gonzalez, 2019) الحدود الرقمية «لدى غونزاليس» التخوم الإقليمية المادية. ومن ثم، تمثل تقنيات الذكاء الاصطناعي في آن واحد بوصفها أدوات تقنية وآليات سياسية تعيد باستمرار تعريف الحدود القانونية والاجتماعية للمواطنة والهوية والانتماء.

ومن خلال الربط بين هذه المنظورات النظرية، تتعامل الدراسة مع الذكاء الاصطناعي لا بوصفه أداة إدارية محايدة، بل باعتباره تجميعًا سوسيو-تقنيًا تتضمن بنيته الخوارزمية افتراضات أيديولوجية ومعيارية محددة. وتسهم الدراسة بذلك في الأدبيات المتنامية المتعلقة بالطبيعة مزدوجة الاستخدام للحوكمة الرقمية في إدارة الهجرة، إذ تعمل في الوقت ذاته بوصفها أداة لتعزيز الكفاءة الإدارية وجهازًا للضبط الاجتماعي.

من الناحية المنهجية، تعتمد الدراسة تصميمًا نوعيًا قائمًا على التحليل المنهجي للوثائق. وقد استُمدت البيانات التجريبية الأولية من المنشورات التشريعية الرسمية، وإعلانات السياسات، والأطر الاستراتيجية الصادرة عن المؤسسات التابعة لوزارة الداخلية في جمهورية أما البيانات الثانوية، فتشمل التقارير التقييمية الصادرة عن الهيئات (DGMM) تركيا، وفي مقدمتها المديرية العامة لإدارة الهجرة والوكالة (IOM)، والمنظمة الدولية للهجرة (UNHCR)، والمنظمات الدولية، بما في ذلك المفوضية السامية للأمم المتحدة لشؤون اللاجئين والمفوضية الأوروبية (Europol)، واليوروبول (FRONTEX) الأوروبية لحرس الحدود والسواحل.

وقد خضعت النصوص المجمعة لترميز موضوعاتي بهدف استخلاص الأنماط المتعلقة بالتشغيل الفعلي لتقنيات الذكاء الاصطناعي عبر ثلاثة أبعاد رئيسية: 1: (تحديد الهوية البيومتري والتميط الرقمي، و) 2: (التقييم الخوارزمي للمخاطر وأنظمة دعم القرار المؤتمتة، و) 3: بروتوكولات المراقبة الآتية وقابلية التشغيل البيئي للمعلومات الاستخباراتية العابرة للحدود. وعُززت الوثائق التحليلية من خلال التثليث بين المصادر، وذلك بالمقارنة بين المخرجات المؤسسية الوطنية والتقارير الدولية، في حين ضمنت الحساسية النظرية بقاء تفسير البيانات مؤطرًا ضمن منظوري الأمانة والسياسة الحيوية.

وتُظهر النتائج التجريبية أن إطار أمن الهجرة الرقمي في تركيا يعمل بوصفه منظومة متعددة الطبقات تتوسطها التكنولوجيا وتوظف الأصوات المدعومة بالذكاء الاصطناعي لتعزيز دقة إنفاذ الحدود وسرعته وقابليته للتنبؤ، بما يؤدي إلى دمج قواعد البيانات الإدارية المتباينة ضمن مصفوفة حوكمية مترابطة.

على توحيد سجلات بيومترية شاملة للسكان الخاضعين «GöçNet» وعلى وجه التحديد، تعمل البنية التحتية الوطنية التركية للحماية المؤقتة، بما يشمل بصمات الأصابع، وخصائص مورفولوجيا الوجه، ومسح قزحية العين. وتتيح مجموعات البيانات هذه التحقق الآني التي (Mobile Migration Points) «من الهوية، وتتبع الحركة المكانية، والتقييم الإداري للمخاطر. وبالمثل، تتيح «نقاط الهجرة المتنقلة تُستخدم بوصفها وحدات تحقق معززة بالذكاء الاصطناعي في المناطق الحضرية الكبرى، إجراء الفحص البيومتري اللامركزي والمزامنة الفورية مع قواعد البيانات. وعلى الرغم من أن هذه الابتكارات تعزز قدرة الجهاز البيروقراطي للدولة على الإشراف والمراقبة، فإنها تثير في الوقت نفسه إشكاليات حادة تتعلق بالموافقة على معالجة البيانات، وخصوصية المعلومات، والتحيز الخوارزمي المتأصل.

وتقوم خوارزميات التعلم الآلي بتحليل المؤشرات البيوغرافية، ومسارات العبور، والبصمات الرقمية بغرض التنبؤ بمواطن تعمل البروتوكولات التكنولوجية الناشئة في «iBorderCtrl» الضعف الأمنية الكامنة. وعلى نحو مواز للإطار التجريبي للاتحاد الأوروبي تركيا على تصنيف الأفراد وفق مقاييس خوارزمية للمخاطر تؤثر بصورة مباشرة في إجراءات السماح بالعبور عبر الحدود أو الاحتجاز وعلى الرغم من أن هذه الأنظمة تزيد الكفاءة الإدارية إلى أقصى حد، فإنها تنطوي على مخاطر مرتفعة لإعادة إنتاج التحيزات البنيوية الكامنة في مجموعات بيانات التدريب، الأمر الذي يجعل الشفافية وقابلية التفسير شرطين لا غنى عنهما لحماية ضمانات الإجراءات القانونية الواجبة.

والمندوعة بالمركبات الجوية غير ASELSAN، وعلى مستوى البنية التحتية، توفر شبكات المراقبة الكهرو بصرية التابعة لشركة ومنظومات الرادار المخترق للأرض، مراقبة مستمرة للمناطق الحدودية. ومن خلال دمج هذه المنظومات مباشرة مع (UAVs) المأهولة تتجسد منظومة أمنية تنبؤية قائمة على البيانات. وإضافة إلى ذلك، تسهم اتفاقيات GöçNet وشبكة (JABS) نظام المعلومات المتكامل للدرك تبادل البيانات المؤسسية مع اليوروبول والإنتربول والمفوضية السامية للأمم المتحدة لشؤون اللاجئين في تعزيز التعاون العابر للحدود في مكافحة الاتجار بالبشر وتهريب المهاجرين، وإن كانت تثير في الوقت ذاته تساؤلات جوهرية بشأن المساءلة القضائية، وخصوصية البيانات وسيادة الدولة.

ويكشف النقاش النظري الأوسع أن البنى التحتية القائمة على الذكاء الاصطناعي لا تقتصر على تحسين الأداء الإداري، بل تعيد بصورة جوهرية تشكيل العلاقات بين الدولة والمجتمع من خلال توسيع بنية «البانوبتيكية الرقمية» أو المراقبة الرقمية الشاملة. وتوضح العلاقة

الترابطية بين الهجرة والأمن في تركيا كيف تعمل الحوكمة الخوارزمية على تسريع أمنة التنقل البشري، بما يفرض إلى ظهور أنماط جديدة من الإدماج والإقصاء عبر المجالين المادي والافتراضي.

وتخلص الدراسة إلى أن تقنيات الحدود المدعومة بالذكاء الاصطناعي تمثل تحولاً عميقاً، وإن كان ملتبساً من الناحية البيئية، في حوكمة الهجرة المعاصرة. فبينما توفر هذه التقنيات إمكانيات غير مسبقة لتحسين إدارة التحركات السكانية واسعة النطاق، فإنها تتطوّر، في الوقت ذاته، على مخاطر تطبيع المراقبة الرقمية الشاملة وتقليص الفاعلية البشرية في القرارات الإدارية ذات الآثار المصيرية.

وبناءً على ذلك، ينبغي أن تخضع مؤسسة الذكاء الاصطناعي في مجال أمن الهجرة لامتحان صارم لمعايير حقوق الإنسان، مع التأكيد على مبادئ الشفافية والتناسب والمساءلة المؤسسية. كما تستلزم الأطر القانونية، بما في ذلك قانون حماية البيانات الشخصية التركي قدرًا من المواءمة بما يحد من الاستغلال غير المصرح به، (GDPR) واللائحة العامة لحماية البيانات في الاتحاد الأوروبي (Kvkk) للمعلومات البيومترية الحساسة. وتظل الحوكمة الأخلاقية للخوارزميات شرطاً جوهرياً للحفاظ على مشروعية أنظمة الحدود الرقمية الحديثة.

وفي المحصلة، تقدم التجربة المؤسسية التركية معطيات تجريبية قيّمة للدول الساعية إلى تحقيق التوازن بين مقتضيات الأمن القومي ووصون الكرامة الإنسانية في العصر الرقمي. وينبغي للبحوث المستقبلية أن تستقصي الآليات الكفيلة بتدقيق القرارات الخوارزمية والظعن فيها، بما يضمن أن يؤدي الذكاء الاصطناعي دور أداة للتيسير العادل والمنصف، لا أن يتحول إلى آلية للإقصاء البيئي. ومن ثم، فإن حوكمة الهجرة المستدامة لا تستلزم كفاءة تكنولوجية متقدمة فحسب، بل تقتضي كذلك التزاماً معيارياً راسخاً لا يقبل المساومة بمبادئ العدالة والشفافية وصنع السياسات المتمحورة حول الإنسان.

الكلمات المفتاحية: الذكاء الاصطناعي، أمن الهجرة، الأزمة السورية، تحديد الهوية البيوميترية، إدارة الحدود.

Résumé Structuré

Au cours de la dernière décennie, la complexité croissante et l'ampleur quantitative des flux migratoires irréguliers ont profondément reconfiguré les priorités nationales et internationales en matière de sécurité. Les paradigmes traditionnels de gestion des frontières se sont révélés insuffisants pour répondre aux formes contemporaines de mobilité migratoire, caractérisées par des réseaux illicites transnationaux, une forte vélocité des déplacements et des situations d'urgence humanitaire systémiques. Dans ce contexte, l'intégration des technologies d'intelligence artificielle (IA) dans la sécurité des frontières et la gouvernance migratoire s'est imposée comme une innovation structurelle majeure. Les systèmes fondés sur l'IA permettent aux États souverains d'optimiser leur efficacité opérationnelle grâce à l'analyse avancée des mégadonnées, à la surveillance en temps réel, à la vérification biométrique et à l'automatisation de la prise de décision administrative.

La présente étude examine la manière dont la Türkiye a institutionnalisé les technologies assistées par l'IA au sein de son dispositif global de gestion des migrations et de sécurité frontalière, notamment dans le contexte consécutif à la crise syrienne. Elle s'articule autour de trois questions de recherche principales : comment les systèmes pilotés par l'IA transforment-ils la structure de gouvernance des migrations et de la sécurité en Türkiye ? Quelles sont les implications éthiques, juridiques et sociopolitiques qui découlent de l'utilisation de ces technologies ? Pourquoi l'automatisation algorithmique est-elle devenue un élément central de l'architecture numérique turque de sécurisation des migrations ? À travers ces interrogations, l'étude appréhende la trajectoire empirique de la Türkiye comme une étude de cas critique permettant de mettre en évidence à la fois l'utilité opérationnelle et les tensions structurelles inhérentes à l'intégration de l'IA dans la gouvernance migratoire contemporaine.

Le cadre théorique articule la théorie de la sécurisation et les études sur la surveillance. S'appuyant sur l'École de Copenhague (Buzan, Wæver, & de Wilde, 1998), la recherche souligne que les menaces sécuritaires ne sont pas construites uniquement à partir de mesures objectives du danger, mais également à travers les pratiques discursives des acteurs politiques. Dès lors, la construction de la migration en tant que menace existentielle pour la sécurité légitime le recours à des mécanismes exceptionnels de gouvernance, notamment à une surveillance numérique généralisée et au profilage automatisé des risques.

L'étude mobilise également les analyses biopolitiques de la surveillance conceptualisées par Foucault (1977) et Lyon (2001). Dans les espaces frontaliers gouvernés par l'IA, la collecte, l'extraction et la catégorisation systématiques des données biométriques transforment les migrants en sujets numérisés, renforçant ainsi la souveraineté étatique et les rapports de pouvoir asymétriques. En complément, la conceptualisation des « frontières numériques » proposée par Gonzalez (2019) montre comment les infrastructures technologiques permettent de projeter le pouvoir étatique bien au-delà des délimitations territoriales physiques. Les technologies d'IA fonctionnent ainsi simultanément comme des instruments

techniques et des mécanismes politiques qui redéfinissent en permanence les frontières juridiques et sociales de la citoyenneté, de l'identité et de l'appartenance.

En articulant ces différentes perspectives théoriques, cette recherche conceptualise l'IA non pas comme un outil administratif neutre, mais comme un assemblage sociotechnique incorporant des présupposés idéologiques et normatifs spécifiques dans son architecture algorithmique. L'étude contribue ainsi à la littérature émergente consacrée au caractère dual de la gouvernance numérique dans la gestion migratoire, celle-ci fonctionnant simultanément comme un instrument d'efficacité administrative et comme un dispositif de contrôle social.

Sur le plan méthodologique, l'étude adopte une approche qualitative fondée sur une analyse documentaire systématique. Les données empiriques primaires sont issues de publications législatives officielles, de déclarations de politique publique et de cadres stratégiques émanant des organismes relevant du ministère de l'Intérieur de la République de Türkiye, au premier rang desquels la Direction générale de la gestion des migrations (DGMM). Les données secondaires comprennent des rapports d'évaluation publiés par des organismes internationaux, notamment le Haut-Commissariat des Nations Unies pour les réfugiés (HCR/UNHCR), l'Organisation internationale pour les migrations (OIM/IOM), FRONTEX, Europol et la Commission européenne.

Les textes recueillis ont fait l'objet d'un codage thématique visant à identifier les régularités dans l'opérationnalisation des technologies d'IA selon trois dimensions principales : (1) l'identification biométrique et le profilage numérique ; (2) l'évaluation algorithmique des risques et les systèmes automatisés d'aide à la décision ; et (3) les protocoles de surveillance en temps réel et l'interopérabilité transfrontalière des renseignements. La fiabilité analytique a été renforcée par une triangulation intersources entre les productions institutionnelles nationales et les rapports internationaux, tandis qu'une sensibilité théorique constante a permis de maintenir l'interprétation des données dans les cadres analytiques de la sécurisation et de la biopolitique.

Les résultats empiriques montrent que le dispositif numérique turc de sécurisation des migrations fonctionne comme un appareil multicouche à forte médiation technologique. Les instruments assistés par l'IA sont mobilisés afin d'accroître la précision, la rapidité et la prédictibilité du contrôle frontalier, tout en intégrant des bases de données administratives hétérogènes au sein d'une matrice de gouvernance interconnectée.

Plus précisément, l'infrastructure nationale turque GöçNet centralise des dossiers biométriques exhaustifs — comprenant les empreintes digitales, la morphologie faciale et les scans de l'iris — relatifs aux populations placées sous protection temporaire. Ces ensembles de données permettent l'authentification de l'identité en temps réel, le suivi de la mobilité spatiale et l'évaluation administrative des risques. De même, les Points mobiles de migration (*Mobile Migration Points*), déployés dans les zones métropolitaines en tant qu'unités de vérification renforcées par l'IA, permettent un contrôle biométrique décentralisé ainsi qu'une synchronisation immédiate avec les bases de données. Si ces innovations renforcent la capacité de supervision bureaucratique de l'État, elles suscitent simultanément de sérieuses préoccupations relatives au consentement au traitement des données, à la confidentialité informationnelle et aux biais algorithmiques intrinsèques.

Les algorithmes d'apprentissage automatique analysent les indicateurs biographiques, les itinéraires de transit et les empreintes numériques afin d'anticiper des vulnérabilités sécuritaires latentes. À l'instar du dispositif expérimental européen iBorderCtrl, les protocoles technologiques émergents en Türkiye classifient les individus au moyen d'indicateurs algorithmiques de risque qui influencent directement les procédures d'autorisation de franchissement des frontières ou de placement en rétention. Bien que de tels systèmes maximisent l'efficacité administrative, ils présentent un risque élevé de reproduction des biais systémiques incorporés dans les jeux de données d'entraînement, faisant ainsi de la transparence et de l'explicabilité des conditions indispensables à la protection des garanties procédurales et du droit à une procédure régulière.

Au niveau infrastructurel, les réseaux de surveillance électro-optiques d'ASELSAN, renforcés par des véhicules aériens sans équipage (UAV) et des réseaux de radars à pénétration de sol, assurent une surveillance continue du périmètre frontalier. Directement intégrés au Système intégré d'information de la Gendarmerie (JABS) et à GöçNet, ces dispositifs matérialisent un paradigme sécuritaire prédictif fondé sur les données. En outre, les accords institutionnalisés de partage de données avec Europol, Interpol et le HCR optimisent la coopération transnationale en matière de lutte contre la traite des êtres humains et le trafic illicite de migrants, tout en soulevant des interrogations majeures concernant la responsabilité juridictionnelle, la protection des données et la souveraineté étatique.

La discussion théorique élargie révèle que les infrastructures pilotées par l'IA ne se limitent pas à améliorer les performances administratives ; elles restructurent fondamentalement les relations entre l'État et la société en élargissant l'architecture du panoptisme numérique. Le nexus migration-sécurité en Türkiye illustre la manière dont la gouvernance algorithmique accélère la sécurisation de la mobilité humaine, donnant naissance à de nouvelles modalités d'inclusion et d'exclusion dans les espaces tant physiques que virtuels.

L'étude conclut que les technologies frontalières assistées par l'IA constituent une évolution profondément transformatrice, mais structurellement ambivalente, de la gouvernance migratoire contemporaine. Si elles offrent des possibilités sans précédent d'optimisation de la gestion des mouvements de population à grande échelle, elles risquent simultanément de normaliser une surveillance numérique généralisée et d'éroder la capacité d'action humaine dans les processus de décision administrative produisant des conséquences substantielles pour les individus.

En conséquence, l'institutionnalisation de l'IA dans le domaine de la sécurité migratoire doit être encadrée par un strict respect des droits humains, fondé notamment sur les principes de transparence, de proportionnalité et de responsabilité institutionnelle. Les cadres juridiques, notamment la loi turque sur la protection des données à caractère personnel (KVKK) et le Règlement général sur la protection des données de l'Union européenne (RGPD/GDPR), doivent faire l'objet d'une harmonisation afin de prévenir l'exploitation non autorisée d'informations biométriques sensibles. Une gouvernance algorithmique éthique demeure, à cet égard, une condition essentielle au maintien de la légitimité des régimes contemporains de frontières numériques.

En définitive, l'expérience institutionnelle de la Türkiye fournit des enseignements empiriques précieux aux États qui cherchent à concilier les impératifs de sécurité nationale et le respect de la dignité humaine à l'ère numérique. Les recherches futures devront examiner les mécanismes permettant d'auditer et de contester les décisions algorithmiques afin de garantir que l'intelligence artificielle fonctionne comme un instrument de facilitation équitable plutôt que comme un mécanisme d'exclusion systémique. Une gouvernance durable des migrations requiert ainsi non seulement une maîtrise technologique avancée, mais également un engagement normatif sans compromis en faveur de la justice, de la transparence et de l'élaboration de politiques publiques centrées sur l'humain.

Mots-clés: Intelligence artificielle, Sécurité migratoire, Crise syrienne, Identification biométrique, Gestion des frontières.

Resumen Estructurado

Durante la última década, la creciente complejidad y la magnitud cuantitativa de los flujos migratorios irregulares han reconfigurado de manera fundamental las prioridades de seguridad tanto nacionales como internacionales. Los paradigmas tradicionales de gestión fronteriza han demostrado ser insuficientes para afrontar las formas contemporáneas de movilidad migratoria, caracterizadas por redes ilícitas transnacionales, desplazamientos de alta velocidad y emergencias humanitarias de carácter sistémico. En consecuencia, la integración de tecnologías de inteligencia artificial (IA) en la seguridad fronteriza y la gobernanza migratoria se ha consolidado como una innovación estructural de importancia crítica. Los sistemas habilitados por IA permiten a los Estados soberanos optimizar su eficacia operativa mediante el análisis avanzado de macrodatos (*big data*), la vigilancia en tiempo real, la verificación biométrica y la toma automatizada de decisiones administrativas.

El presente estudio examina la manera en que Türkiye ha institucionalizado las tecnologías respaldadas por IA dentro de su aparato más amplio de gestión migratoria y seguridad fronteriza, particularmente en el escenario configurado tras la crisis siria. La investigación aborda tres interrogantes fundamentales: ¿cómo transforman los sistemas impulsados por IA la estructura de gobernanza de la migración y la seguridad en Türkiye? ¿Cuáles son las implicaciones éticas, jurídicas y sociopolíticas derivadas de estas tecnologías? ¿Por qué la automatización algorítmica se ha convertido en un componente central de la arquitectura digital de seguridad migratoria de Türkiye? A partir de estas cuestiones, el estudio plantea la trayectoria empírica de Türkiye como un estudio de caso crítico que refleja simultáneamente la utilidad operativa y las tensiones estructurales inherentes a la integración de la IA en la gobernanza migratoria contemporánea.

El marco teórico articula la teoría de la securitización con los estudios sobre vigilancia. Sobre la base de la Escuela de Copenhague (Buzan, Wæver, & de Wilde, 1998), la investigación subraya que las amenazas a la seguridad no se construyen exclusivamente mediante indicadores objetivos de peligro, sino también a través de las prácticas discursivas de los actores políticos. En consecuencia, la construcción discursiva de la migración como una amenaza existencial para la seguridad legítima mecanismos excepcionales de gobernanza, entre ellos la vigilancia digital generalizada y la elaboración automatizada de perfiles de riesgo.

Asimismo, el estudio incorpora los análisis biopolíticos de la vigilancia conceptualizados por Foucault (1977) y Lyon (2001). En los espacios fronterizos gobernados mediante IA, la recopilación, extracción y categorización sistemáticas de datos biométricos transforman a los migrantes en sujetos digitalizados, reforzando de este modo la soberanía estatal y las relaciones asimétricas de poder. Complementariamente, la conceptualización de las «fronteras digitales» propuesta por Gonzalez (2019) demuestra cómo las infraestructuras tecnológicas proyectan el poder estatal mucho más allá de las delimitaciones territoriales físicas. De este modo, las tecnologías de IA operan simultáneamente como instrumentos técnicos y mecanismos políticos que redefinen de manera continua las fronteras jurídicas y sociales de la ciudadanía, la identidad y la pertenencia.

Mediante la articulación de estas perspectivas teóricas, la presente investigación conceptualiza la IA no como una herramienta administrativa neutral, sino como un ensamblaje sociotécnico que incorpora presupuestos ideológicos y normativos específicos en su arquitectura algorítmica. De este modo, el estudio contribuye a la creciente literatura sobre la naturaleza de doble uso de la gobernanza digital en la gestión migratoria, que actúa simultáneamente como instrumento de eficiencia administrativa y como dispositivo de control social.

Desde el punto de vista metodológico, el estudio adopta un diseño cualitativo sustentado en un análisis documental sistemático. Los datos empíricos primarios proceden de publicaciones legislativas oficiales, declaraciones de política pública y marcos estratégicos promulgados por organismos dependientes del Ministerio del Interior de la República de Türkiye, en particular por la Dirección General de Gestión de la Migración (DGMM). Los datos secundarios comprenden informes de evaluación publicados por organismos internacionales, entre ellos el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR/UNHCR), la Organización Internacional para las Migraciones (OIM/IOM), FRONTEX, Europol y la Comisión Europea.

Los textos recopilados fueron sometidos a codificación temática con el propósito de identificar patrones relativos a la operacionalización de las tecnologías de IA en tres dimensiones principales: (1) identificación biométrica y elaboración de perfiles digitales; (2) evaluación algorítmica de riesgos y sistemas automatizados de apoyo a la toma de decisiones; y (3) protocolos de vigilancia en tiempo real e interoperabilidad transfronteriza de inteligencia. La fiabilidad analítica se reforzó mediante la triangulación entre fuentes, contrastando los productos institucionales nacionales con los informes internacionales, mientras que la sensibilidad teórica permitió mantener la interpretación de los datos anclada en los marcos de la securitización y la biopolítica.

Los hallazgos empíricos demuestran que el marco digital de seguridad migratoria de Türkiye funciona como un aparato multicapa mediado tecnológicamente. Los instrumentos respaldados por IA se emplean para incrementar la precisión, la rapidez y la capacidad predictiva de la vigilancia y el control fronterizos, integrando bases de datos administrativas heterogéneas en una matriz de gobernanza interconectada.

En particular, la infraestructura nacional turca GöçNet consolida registros biométricos exhaustivos — que comprenden huellas dactilares, morfología facial y escaneos del iris — de las poblaciones acogidas al régimen de protección temporal. Estos conjuntos de datos facilitan la autenticación de identidad en tiempo real, el seguimiento de la movilidad espacial y la evaluación administrativa de riesgos. De manera análoga, los Puntos Móviles de Migración (*Mobile Migration Points*), desplegados como unidades de verificación reforzadas mediante IA en áreas metropolitanas, permiten realizar controles biométricos descentralizados y sincronizar de manera inmediata la información con las bases de datos correspondientes. Si bien estas innovaciones consolidan la capacidad de supervisión burocrática del Estado, generan simultáneamente importantes preocupaciones relacionadas con el consentimiento para el tratamiento de datos, la privacidad de la información y los sesgos algorítmicos inherentes.

Los algoritmos de aprendizaje automático analizan indicadores biográficos, itinerarios de tránsito y huellas digitales con el propósito de predecir vulnerabilidades latentes en materia de seguridad. De forma paralela al marco experimental iBorderCtrl de la Unión Europea, los protocolos tecnológicos emergentes en Türkiye clasifican a los individuos mediante métricas algorítmicas de riesgo que inciden directamente en los procedimientos de autorización de cruce fronterizo o de detención. Aunque estos sistemas maximizan la eficiencia administrativa, presentan un elevado riesgo de reproducir sesgos sistémicos incorporados en los conjuntos de datos de entrenamiento, lo que convierte la transparencia y la explicabilidad algorítmica en requisitos indispensables para garantizar el debido proceso y las garantías procedimentales.

En el plano infraestructural, las redes de vigilancia electroóptica de ASELSAN, reforzadas mediante vehículos aéreos no tripulados (UAV) y sistemas de radar de penetración terrestre, proporcionan una supervisión continua del perímetro fronterizo. Integrados directamente con el Sistema Integrado de Información de la Gendarmería (JABS) y GöçNet, estos recursos materializan un paradigma de seguridad predictivo y basado en datos. Asimismo, los acuerdos institucionalizados de intercambio de datos con Europol, Interpol y el ACNUR optimizan la cooperación transnacional contra la trata de personas y el tráfico ilícito de migrantes, aunque plantean cuestiones críticas relativas a la responsabilidad jurisdiccional, la privacidad de los datos y la soberanía estatal.

La discusión teórica más amplia pone de manifiesto que las infraestructuras impulsadas por IA no se limitan a mejorar el rendimiento administrativo, sino que reconstruyen de manera fundamental las relaciones entre el Estado y la sociedad mediante la expansión de la arquitectura del panoptismo digital. El nexo entre migración y seguridad en Türkiye ilustra cómo la gobernanza algorítmica acelera la securitización de la movilidad humana y da lugar a nuevas modalidades de inclusión y exclusión tanto en los espacios físicos como en los virtuales.

El estudio concluye que las tecnologías fronterizas respaldadas por IA constituyen un desarrollo profundamente transformador, aunque estructuralmente ambivalente, en la gobernanza migratoria contemporánea. Si bien ofrecen posibilidades sin precedentes para optimizar la gestión de movimientos poblacionales de gran volumen, simultáneamente entrañan el riesgo de normalizar una vigilancia digital generalizada y de erosionar la agencia humana en decisiones administrativas con consecuencias sustanciales para los individuos.

En consecuencia, la institucionalización de la IA en el ámbito de la seguridad migratoria debe regirse por un estricto cumplimiento de los derechos humanos, con especial énfasis en los principios de transparencia, proporcionalidad y rendición de cuentas institucional. Los marcos jurídicos, incluida la Ley de Protección de Datos Personales de Türkiye (KVKK) y el Reglamento General de Protección de Datos de la Unión Europea (RGPD/GDPR), requieren una adecuada armonización con el fin de mitigar la explotación no autorizada de información biométrica sensible. La gobernanza algorítmica ética constituye, por tanto, un requisito esencial para preservar la legitimidad de los regímenes contemporáneos de fronteras digitales.

En última instancia, la experiencia institucional de Türkiye ofrece valiosas aportaciones empíricas para los Estados que aspiran a conciliar los imperativos de seguridad nacional con la protección de la dignidad humana en la era digital. Las investigaciones futuras deberán examinar los mecanismos destinados a auditar e impugnar las determinaciones algorítmicas, a fin de garantizar que la inteligencia artificial funcione como un instrumento de facilitación equitativa y no como un mecanismo de exclusión sistémica. Una gobernanza migratoria sostenible exige no solo un elevado nivel de competencia tecnológica, sino también un compromiso normativo irrenunciable con la justicia, la transparencia y la formulación de políticas públicas centradas en el ser humano.

Palabras clave: Inteligencia artificial, Seguridad migratoria, Crisis siria, Identificación biométrica, Gestión fronteriza.

结构式摘要

过去十年来，非正规移民流动在复杂性与规模上的持续上升，从根本上重塑了国家及国际层面的安全优先议程。传统的边境管理范式已难以有效应对当代移民流动的新特征，包括跨国非法网

络的扩展、高速且高度动态的人口流动，以及具有系统性特征的人道主义紧急状态。因此，将人工智能（Artificial Intelligence, AI）技术整合至边境安全与移民治理体系，已成为一项具有关键意义的结构性创新。人工智能赋能系统通过先进的大数据分析、实时监控、生物特征核验以及行政决策自动化，使主权国家能够进一步优化其治理与执法的运行效能。

本研究考察土耳其在叙利亚危机之后的特定背景下，如何将人工智能支持技术制度化地纳入其更广泛的移民治理与边境安全体系。研究围绕三个核心问题展开：人工智能驱动系统如何改变土耳其移民与安全治理的结构性机制？此类技术的应用将产生哪些伦理、法律及社会政治影响？算法自动化为何逐渐成为土耳其数字化移民安全架构的核心组成部分？基于上述问题，本研究将土耳其的实践进程作为一个具有批判性分析价值的案例，以揭示人工智能融入当代移民治理过程中所体现的运行效用及其内在的结构性张力。

本研究的理论框架综合运用安全化理论与监控研究。依据哥本哈根学派（Copenhagen School）的理论观点（Buzan, Wæver, & de Wilde, 1998），研究强调，安全威胁并非仅仅依据客观的危险指标而形成，而是在相当程度上通过政治行为体的话语实践被社会性建构。因此，当移民被框定为一种生存性安全威胁时，广泛的数字监控、自动化风险画像等例外性治理机制便由此获得正当性。

此外，本研究引入福柯（Foucault, 1977）与里昂（Lyon, 2001）所阐释的监控生物政治分析框架。在人工智能治理的边境空间中，对生物特征数据进行系统性收集、提取和分类，使移民逐渐转化为“数字化主体”，从而进一步强化国家主权及不对称的权力关系。与此同时，Gonzalez（2019）提出的“数字边境”（digital borders）概念揭示了技术基础设施如何使国家权力突破实体领土边界，并向物理疆界之外延伸。因此，人工智能技术兼具技术工具与政治机制的双重属性，并持续重构公民身份、身份认同与归属关系的法律边界和社会边界。

通过整合上述理论视角，本研究并不将人工智能视为一种价值中立的行政工具，而是将其概念化为一种“社会—技术组合体”（socio-technical assemblage），其算法架构内嵌特定的意识形态与规范性预设。由此，本研究进一步拓展了关于数字治理在移民管理中“双重用途”属性的相关研究：数字治理既是提升行政效率的工具，同时也可能构成实施社会控制的制度性装置。

在研究方法方面，本研究采用以系统性文献分析为基础的质性研究设计。主要实证资料来源于土耳其共和国内政部所属机构发布的官方立法文件、政策声明与战略框架，其中尤以移民管理总局（Directorate General of Migration Management, DGMM）的相关资料为核心。次级资料则包括联合国难民事务高级专员公署（UNHCR）、国际移民组织（IOM）、欧洲边境与海岸警卫局（FRONTEX）、欧洲刑警组织（Europol）以及欧盟委员会等国际机构发布的评估报告。

研究对所收集文本实施主题编码，以识别人工智能技术在三个主要维度上的具体运行模式：（1）生物特征身份识别与数字画像；（2）算法风险评估与自动化决策支持系统；（3）实时监控机制与跨境情报互操作性。通过对国家机构资料与国际组织报告进行跨来源三角验证，进一步提升分析的可靠性；同时，通过保持理论敏感性，确保资料解释始终立足于安全化理论与生物政治分析框架。

实证研究结果表明，土耳其的数字化移民安全框架已经形成一种多层次、技术中介化的治理装置。人工智能支持工具被用于提高边境执法的精准性、速度与可预测性，并将原本相对分散的行政数据库整合为相互联结的治理矩阵。

具体而言，土耳其国家级GöçNet基础设施整合了临时保护人口的综合性生物特征记录，其中包括指纹、面部形态特征及虹膜扫描数据。此类数据集能够支持实时身份认证、空间流动追踪以及行政风险评估。与此同时，在大都市区域部署的“流动移民服务点”（Mobile Migration Points）作为人工智能增强型身份核验单元，可以实施分布式生物特征核验，并与相关数据库进行即时同步。尽管这些技术创新强化了国家官僚体系的监督能力，但与此同时，也引发了有关数据处理同意、信息隐私以及内在算法偏见等方面的重大关切。

机器学习算法通过分析个人履历指标、过境路线以及数字足迹，对潜在的安全脆弱性进行预测。与欧盟实验性的iBorderCtrl框架相类似，土耳其正在形成的技术协议依据算法风险指标对个人进行分类，而这些分类结果能够直接影响边境通行许可或拘留程序。尽管此类系统能够显著提升行政效率，但其同时存在复制训练数据集中既有系统性偏见的高度风险。因此，透明度与算法可解释性构成维护程序性正当权利与正当程序保障不可或缺的前提条件。

在基础设施层面，ASELSAN的光电监控网络在无人驾驶航空器（Uncrewed Aerial Vehicles, UAVs）以及探地雷达阵列的支持下，实现对边境区域的持续性监测。这些技术设施与宪兵综合信息系统（JABS）及GöçNet直接整合，共同构建了一种预测性、数据驱动型安全范式。此外，与Europol、Interpol以及UNHCR建立的制度化数据共享协议，有助于优化打击人口贩运与偷运移民活动的跨国合作，但同时也引发了有关司法管辖责任、数据隐私及国家主权等方面的重要问题。

进一步的理论讨论表明，人工智能驱动的基础设施并不仅仅提升行政管理绩效，更通过扩展“数字全景敞视主义”（digital panopticism）的制度架构，从根本上重构国家与社会之间的关系。土耳其的“移民—安全”关联机制揭示了算法治理如何加速人口流动的安全化进程，并由此在实体空间与虚拟空间中催生新的包容与排斥机制。

本研究认为，人工智能支持的边境技术是当代移民治理领域一项具有深刻变革意义、但在结构上具有明显双重性的制度发展。一方面，此类技术为管理大规模人口流动提供了前所未有的优化能力；另一方面，它们也可能导致广泛数字监控的常态化，并削弱个人在具有重大后果的行政决策过程中的主体能动性。

因此，将人工智能制度化地纳入移民安全治理，必须受到严格的人权规范约束，并将透明度、比例原则及制度问责置于核心位置。包括土耳其《个人数据保护法》（KVKK）以及欧盟《通用数据保护条例》（GDPR）在内的相关法律框架，需要进一步实现协调与衔接，以降低敏感生物特征信息遭受未经授权利用的风险。符合伦理规范的算法治理因而构成维护现代数字边境制度合法性的关键前提。

总体而言，土耳其的制度实践为数字时代寻求在国家安全需求与人的尊严之间实现平衡的国家提供了具有重要价值的实证启示。未来研究应进一步探讨对算法决策进行审计、审查及提出异议

的制度机制，从而确保人工智能成为促进公平治理的工具，而非系统性排斥的机制。可持续的移民治理不仅需要先进的技术能力，更需要对正义、透明度以及以人为本的政策制定原则作出坚定且不可妥协的规范性承诺。

关键词： 人工智能；移民安全；叙利亚危机；生物特征身份识别；边境管理。

Структурированная Аннотация

За последнее десятилетие возрастающая сложность и масштаб нерегулярных миграционных потоков коренным образом изменили приоритеты национальной и международной безопасности. Традиционные парадигмы управления границами продемонстрировали свою недостаточную эффективность в условиях современных миграционных перемещений, характеризующихся деятельностью транснациональных нелегальных сетей, высокой интенсивностью и скоростью мобильности, а также системными гуманитарными чрезвычайными ситуациями. В этих условиях интеграция технологий искусственного интеллекта (ИИ) в системы пограничной безопасности и управления миграцией приобрела значение критически важной структурной инновации. Системы, основанные на технологиях ИИ, позволяют суверенным государствам оптимизировать операционную эффективность посредством расширенной аналитики больших данных, мониторинга в режиме реального времени, биометрической верификации и автоматизированного принятия административных решений.

Настоящее исследование посвящено анализу того, каким образом Türkiye институционализировала технологии, поддерживаемые искусственным интеллектом, в рамках более широкой системы управления миграцией и обеспечения пограничной безопасности, в особенности в контексте, сформировавшемся после сирийского кризиса. В исследовании рассматриваются три ключевых вопроса: каким образом системы, основанные на ИИ, трансформируют структурные механизмы управления миграцией и безопасностью в Türkiye? Каковы обусловленные применением этих технологий этические, правовые и социально-политические последствия? Почему алгоритмическая автоматизация стала центральным элементом цифровой архитектуры миграционной безопасности Türkiye? Исходя из поставленных вопросов, эмпирическая траектория Türkiye рассматривается в качестве критически значимого кейса, отражающего одновременно операционную полезность и структурные противоречия интеграции искусственного интеллекта в современную систему управления миграцией.

Теоретическая основа исследования объединяет теорию секьюритизации и исследования надзора. Опираясь на положения Копенгагенской школы (Buzan, Wæver, & de Wilde, 1998), исследование исходит из того, что угрозы безопасности конструируются не исключительно посредством объективных показателей опасности, но также посредством дискурсивных практик политических акторов. Следовательно, репрезентация миграции в качестве экзистенциальной угрозы безопасности легитимирует применение исключительных механизмов управления, включая всеобъемлющий цифровой надзор и автоматизированное профилирование рисков.

Кроме того, в исследовании используются биополитические подходы к анализу надзора, концептуализированные Фуко (Foucault, 1977) и Лайоном (Lyons, 2001). В пограничных пространствах, управляемых посредством ИИ, систематический сбор, извлечение и категоризация биометрических данных трансформируют мигрантов в цифровизированных субъектов, тем самым укрепляя государственный суверенитет и асимметричные отношения власти. В дополнение к этому концепция «цифровых границ» Гонсалеса (Gonzalez, 2019) демонстрирует, каким образом технологическая инфраструктура позволяет проецировать государственную власть далеко за пределы физических территориальных разграничений. Таким образом, технологии ИИ одновременно функционируют как технические инструменты и политические механизмы, непрерывно переопределяющие юридические и социальные границы гражданства, идентичности и принадлежности.

Интегрируя указанные теоретические перспективы, настоящее исследование концептуализирует искусственный интеллект не как нейтральный административный инструмент, а

как социотехнический ансамбль (*socio-technical assemblage*), в алгоритмическую архитектуру которого встроены определённые идеологические и нормативные предпосылки. Тем самым исследование вносит вклад в развивающуюся научную литературу, посвящённую двойственной природе цифрового управления в сфере миграции, где оно одновременно выступает инструментом повышения административной эффективности и аппаратом социального контроля.

В методологическом отношении исследование основано на качественном дизайне с применением систематического анализа документов. Первичные эмпирические данные получены из официальных законодательных публикаций, программно-политических документов и стратегических рамочных материалов, подготовленных учреждениями, находящимися в ведении Министерства внутренних дел Республики Türkiye, прежде всего Генеральным управлением по вопросам миграции (Directorate General of Migration Management, DGMM). Вторичные данные включают аналитические и оценочные доклады международных организаций и институтов, в том числе Управления Верховного комиссара ООН по делам беженцев (УВКБ ООН/UNHCR), Международной организации по миграции (МОМ/IOM), FRONTEX, Европола (Europol) и Европейской комиссии.

Собранные тексты были подвергнуты тематическому кодированию с целью выявления закономерностей операционализации технологий ИИ по трём основным направлениям: (1) биометрическая идентификация и цифровое профилирование; (2) алгоритмическая оценка рисков и автоматизированные системы поддержки принятия решений; (3) протоколы мониторинга в режиме реального времени и трансграничная интероперабельность разведывательных данных. Аналитическая надёжность была усилена посредством межисточниковой триангуляции национальных институциональных материалов и международной отчётности, тогда как теоретическая чувствительность обеспечила интерпретацию данных в рамках концепций секьюритизации и биополитики.

Эмпирические результаты свидетельствуют о том, что цифровая система миграционной безопасности Türkiye функционирует как многоуровневый, технологически опосредованный аппарат. Инструменты, поддерживаемые ИИ, используются для повышения точности, оперативности и предсказуемости пограничного контроля, одновременно объединяя разрозненные административные базы данных в единую взаимосвязанную матрицу управления.

В частности, национальная инфраструктура GöçNet в Türkiye консолидирует комплексные биометрические данные лиц, находящихся под временной защитой, включая отпечатки пальцев, параметры морфологии лица и результаты сканирования радужной оболочки глаза. Эти массивы данных обеспечивают аутентификацию личности в режиме реального времени, отслеживание пространственной мобильности и административную оценку рисков. Аналогичным образом мобильные миграционные пункты (*Mobile Migration Points*), развёрнутые в крупных городских зонах в качестве усиленных технологиями ИИ верификационных подразделений, обеспечивают децентрализованную биометрическую проверку и непосредственную синхронизацию с соответствующими базами данных. Несмотря на то что данные инновации укрепляют возможности государственного бюрократического контроля, они одновременно порождают серьёзные вопросы, связанные с согласием на обработку данных, информационной конфиденциальностью и имманентной алгоритмической предвзятостью.

Алгоритмы машинного обучения анализируют биографические показатели, маршруты транзитного перемещения и цифровые следы с целью прогнозирования латентных уязвимостей в сфере безопасности. По аналогии с экспериментальной системой Европейского союза iBorderCtrl формирующиеся в Türkiye технологические протоколы классифицируют лиц на основе алгоритмических показателей риска, непосредственно влияющих на процедуры разрешения пересечения границы либо задержания. Хотя подобные системы максимизируют административную эффективность, они сопряжены с высоким риском воспроизводства системных предубеждений, заложенных в обучающих наборах данных. В связи с этим прозрачность и объяснимость алгоритмов выступают необходимыми предпосылками обеспечения процессуальных гарантий и надлежащей правовой процедуры.

На инфраструктурном уровне электрооптические сети наблюдения ASELSAN, дополненные беспилотными летательными аппаратами (БПЛА/UAV) и комплексами георадаров, обеспечивают

непрерывный мониторинг пограничного периметра. Их непосредственная интеграция с Интегрированной информационной системой жандармерии (JABS) и GöçNet формирует предиктивную, основанную на данных парадигму безопасности. Кроме того, институционализированные соглашения об обмене данными с Европолом, Интерполом и УВКБ ООН способствуют оптимизации транснационального сотрудничества в борьбе с торговлей людьми и незаконным ввозом мигрантов, одновременно порождая принципиально важные вопросы относительно юрисдикционной ответственности, конфиденциальности данных и государственного суверенитета.

Более широкое теоретическое обсуждение показывает, что инфраструктуры, основанные на ИИ, не ограничиваются повышением административной эффективности; они фундаментальным образом реконструируют отношения между государством и обществом посредством расширения архитектуры цифрового паноптицизма. Взаимосвязь миграции и безопасности в Türkiye демонстрирует, каким образом алгоритмическое управление ускоряет секьюритизацию человеческой мобильности, формируя новые механизмы включения и исключения как в физическом, так и в виртуальном пространстве.

Исследование приходит к выводу, что пограничные технологии, основанные на ИИ, представляют собой глубоко трансформирующее, но структурно амбивалентное явление в современной системе управления миграцией. С одной стороны, они обеспечивают беспрецедентные возможности оптимизации управления масштабными перемещениями населения; с другой — создают риск нормализации всеобъемлющего цифрового надзора и ослабления человеческой субъектности при принятии административных решений, имеющих существенные последствия для отдельных лиц.

Следовательно, институционализация искусственного интеллекта в сфере миграционной безопасности должна осуществляться при строгом соблюдении стандартов прав человека с особым акцентом на прозрачность, пропорциональность и институциональную подотчётность. Правовые рамки, включая турецкий Закон о защите персональных данных (KVKK) и Общий регламент Европейского союза по защите данных (GDPR), требуют гармонизации в целях минимизации рисков несанкционированного использования чувствительной биометрической информации. Этическое алгоритмическое управление остаётся важнейшей предпосылкой сохранения легитимности современных режимов цифровых границ.

В конечном счёте институциональный опыт Türkiye предоставляет ценные эмпирические выводы для государств, стремящихся обеспечить баланс между императивами национальной безопасности и защитой человеческого достоинства в цифровую эпоху. Будущие исследования должны быть направлены на изучение механизмов аудита и оспаривания алгоритмических решений, с тем чтобы искусственный интеллект функционировал как инструмент справедливого содействия, а не как механизм системного исключения. Устойчивое управление миграцией требует не только высокого уровня технологической компетентности, но и бескомпромиссной нормативной приверженности принципам справедливости, прозрачности и ориентированного на человека формирования государственной политики.

Ключевые слова: искусственный интеллект, миграционная безопасность, сирийский кризис, биометрическая идентификация, управление границами.

संरचित सारांश

पिछले एक दशक में अनियमित प्रवासन प्रवाहों (*irregular migration flows*) की निरंतर बढ़ती जटिलता और मात्रात्मक व्यापकता ने राष्ट्रीय तथा अंतरराष्ट्रीय सुरक्षा की प्राथमिकताओं को मूलभूत रूप से पुनर्संरचित किया है। सीमा प्रबंधन के पारंपरिक प्रतिमान समकालीन प्रवासी गतिशीलताओं से निपटने में अपर्याप्त सिद्ध हुए हैं, जिनकी प्रमुख विशेषताओं में अंतरराष्ट्रीय अवैध नेटवर्क, तीव्र गति से होने वाला आवागमन तथा प्रणालीगत मानवीय आपातस्थितियाँ शामिल हैं। फलतः, सीमा सुरक्षा और प्रवासन अभिशासन में कृत्रिम बुद्धिमत्ता (Artificial Intelligence—AI) प्रौद्योगिकियों का एकीकरण एक अत्यंत महत्वपूर्ण संरचनात्मक नवाचार के रूप में उभरा है। AI-सक्षम प्रणालियाँ उन्नत विशाल-डेटा (*big data*) विश्लेषण, वास्तविक-समय निगरानी, बायोमेट्रिक सत्यापन तथा स्वचालित प्रशासनिक निर्णय-निर्माण के माध्यम से संप्रभु राज्यों को अपनी परिचालन प्रभावशीलता अनुकूलित करने में सक्षम बनाती हैं।

यह अध्ययन विशेष रूप से सीरियाई संकट के पश्चात् निर्मित परिदृश्य में इस बात का परीक्षण करता है कि Türkiye ने अपनी व्यापक प्रवासन एवं सीमा-सुरक्षा व्यवस्था के भीतर AI-समर्थित प्रौद्योगिकियों को किस प्रकार संस्थागत रूप प्रदान किया है। अध्ययन तीन केंद्रीय अनुसंधान प्रश्नों पर केंद्रित है: AI-संचालित प्रणालियाँ Türkiye में प्रवासन एवं सुरक्षा के संरचनात्मक अभिशासन को किस प्रकार रूपांतरित करती हैं? इन प्रौद्योगिकियों से उत्पन्न नैतिक, विधिक तथा सामाजिक-राजनीतिक निहितार्थ क्या हैं? और एल्गोरिदमिक स्वचालन Türkiye की डिजिटल प्रवासन-सुरक्षा संरचना का केंद्रीय घटक क्यों बन गया है? इन प्रश्नों के माध्यम से अध्ययन Türkiye के अनुभवजन्य प्रक्षेपपथ को एक महत्वपूर्ण केस अध्ययन के रूप में प्रस्तुत करता है, जो समकालीन प्रवासन अभिशासन में AI के एकीकरण की परिचालन उपयोगिता और उससे उत्पन्न संरचनात्मक तनावों—दोनों को प्रतिबिंबित करता है।

अध्ययन का सैद्धांतिक ढाँचा सुरक्षीकरण सिद्धांत (*securitization theory*) और निगरानी अध्ययन (*surveillance studies*) का संश्लेषण करता है। कोपेनहेगन स्कूल (Buzan, Wæver, & de Wilde, 1998) के सैद्धांतिक दृष्टिकोण पर आधारित यह अध्ययन रेखांकित करता है कि सुरक्षा संबंधी खतरों का निर्माण केवल खतरे के वस्तुनिष्ठ मापदंडों के आधार पर नहीं होता, बल्कि राजनीतिक कर्ताओं की विमर्शात्मक प्रथाओं के माध्यम से भी होता है। परिणामस्वरूप, प्रवासन को अस्तित्वगत सुरक्षा-खतरे के रूप में निरूपित करना व्यापक डिजिटल निगरानी और स्वचालित जोखिम-प्रोफाइलिंग सहित असाधारण अभिशासन तंत्रों को वैधता प्रदान करता है।

इसके अतिरिक्त, अध्ययन Foucault (1977) और Lyon (2001) द्वारा प्रतिपादित निगरानी के जैव-राजनीतिक (*biopolitical*) विश्लेषण को भी समाहित करता है। AI द्वारा अभिशासित सीमावर्ती क्षेत्रों में बायोमेट्रिक डेटा का व्यवस्थित संग्रह, निष्कर्षण और वर्गीकरण प्रवासियों को डिजिटलीकृत विषयों (*digitized subjects*) में रूपांतरित करता है, जिससे राज्य की संप्रभुता तथा असममित शक्ति-संबंध और अधिक सुदृढ़ होते हैं। इसके पूरक रूप में Gonzalez (2019) की “डिजिटल सीमाओं” (*digital borders*) की अवधारणा यह प्रदर्शित करती है कि तकनीकी अवसरचनाएँ किस प्रकार राज्य की शक्ति को भौतिक क्षेत्रीय सीमांकन से बहुत आगे तक विस्तारित करती हैं। इस प्रकार, AI प्रौद्योगिकियाँ तकनीकी उपकरणों और राजनीतिक तंत्रों—दोनों के रूप में कार्य करती हैं तथा नागरिकता, पहचान और संबद्धता की विधिक एवं सामाजिक सीमाओं को निरंतर पुनर्परिभाषित करती हैं।

इन सैद्धांतिक दृष्टिकोणों को परस्पर संबद्ध करते हुए यह शोध AI को किसी तटस्थ प्रशासनिक उपकरण के रूप में नहीं, बल्कि एक ऐसे सामाजिक-तकनीकी समुच्चय (*socio-technical assemblage*) के रूप में अवधारित करता है जिसकी एल्गोरिदमिक संरचना में विशिष्ट वैचारिक और मानकीय पूर्वधारणाएँ अंतर्निहित होती हैं। इस प्रकार, अध्ययन प्रवासन प्रबंधन में डिजिटल अभिशासन की द्वि-उपयोगी प्रकृति (*dual-use nature*) से संबंधित उभरते साहित्य में योगदान देता है, जिसमें डिजिटल अभिशासन एक ओर प्रशासनिक दक्षता के साधन के रूप में और दूसरी ओर सामाजिक नियंत्रण के तंत्र के रूप में कार्य करता है।

पद्धतिगत रूप से, अध्ययन व्यवस्थित दस्तावेज़ विश्लेषण पर आधारित गुणात्मक अनुसंधान अभिकल्प को अपनाता है। प्राथमिक अनुभवजन्य डेटा Türkiye गणराज्य के आंतरिक मामलों के मंत्रालय के अधीन संस्थाओं, विशेष रूप से प्रवासन प्रबंधन महानिदेशालय (Directorate General of Migration Management—DGMM), द्वारा जारी आधिकारिक विधायी प्रकाशनों, नीतिगत घोषणाओं तथा रणनीतिक रूपरेखाओं से प्राप्त किए गए हैं। द्वितीयक डेटा में संयुक्त राष्ट्र शरणार्थी उच्चायुक्त (UNHCR), अंतरराष्ट्रीय प्रवासन संगठन (IOM), FRONTEX, Europol तथा यूरोपीय आयोग सहित अंतरराष्ट्रीय निकायों द्वारा प्रकाशित मूल्यांकनात्मक रिपोर्टें सम्मिलित हैं।

संकलित पाठों का विषयगत कूटलेखन (*thematic coding*) किया गया, ताकि तीन प्रमुख आयामों में AI प्रौद्योगिकियों के परिचालनात्मक प्रयोग के प्रतिरूपों की पहचान की जा सके: (1) बायोमेट्रिक पहचान और डिजिटल प्रोफाइलिंग; (2) एल्गोरिदमिक जोखिम-मूल्यांकन तथा स्वचालित निर्णय-सहायता प्रणालियाँ; और (3) वास्तविक-समय निगरानी प्रोटोकॉल तथा सीमापार खुफिया सूचनाओं की अंतरसंचालनीयता (*interoperability*)। राष्ट्रीय संस्थागत स्रोतों और अंतरराष्ट्रीय रिपोर्टिंग के बीच अंतर-स्रोत त्रिकोणीकरण (*cross-source triangulation*) के माध्यम से विश्लेषणात्मक विश्वसनीयता को सुदृढ़ किया गया, जबकि सैद्धांतिक संवेदनशीलता ने यह सुनिश्चित किया कि डेटा की व्याख्या सुरक्षीकरण और जैव-राजनीतिक रूपरेखाओं में दृढ़तापूर्वक निहित रहे।

अनुभवजन्य निष्कर्ष प्रदर्शित करते हैं कि Türkiye का डिजिटल प्रवासन-सुरक्षा ढाँचा एक बहुस्तरीय और प्रौद्योगिकी-मध्यस्थित तंत्र के रूप में कार्य करता है। AI-समर्थित उपकरणों का उपयोग सीमा प्रवर्तन की सटीकता, गति और पूर्वानुमेयता बढ़ाने के लिए किया जाता है, जिससे विभिन्न प्रशासनिक डेटाबेसों को एक परस्पर संबद्ध अभिशासन मैट्रिक्स में एकीकृत किया जाता है।

विशेष रूप से, Türkiye की राष्ट्रीय GöçNet अवसंरचना अस्थायी संरक्षण के अंतर्गत आने वाली आबादी के व्यापक बायोमेट्रिक अभिलेखों—जिनमें अंगुलियों के निशान, चेहरे की आकृतिगत विशेषताएँ तथा परितारिका (*iris*) स्कैन सम्मिलित हैं—को समेकित करती है। ये डेटा-समुच्चय वास्तविक समय में पहचान प्रमाणीकरण, स्थानिक गतिशीलता की निगरानी तथा प्रशासनिक जोखिम-मूल्यांकन को संभव बनाते हैं। इसी प्रकार, महानगरीय क्षेत्रों में AI-संवर्धित सत्यापन इकाइयों के रूप में तैनात मोबाइल माइग्रेशन पॉइंट्स (*Mobile Migration Points*) विकेंद्रीकृत बायोमेट्रिक स्क्रीनिंग और डेटाबेस के साथ तत्काल समकालिकीकरण को सक्षम बनाते हैं। यद्यपि ये नवाचार राज्य की नौकरशाही पर्यवेक्षण क्षमता को सुदृढ़ करते हैं, तथापि वे डेटा-सहमति, सूचनात्मक गोपनीयता और अंतर्निहित एल्गोरिदिक पक्षपात से संबंधित गंभीर चिंताएँ भी उत्पन्न करते हैं।

मशीन लर्निंग एल्गोरिदम जीवनी-संबंधी संकेतकों, पारगमन मार्गों तथा डिजिटल पदचिह्नों का विश्लेषण करके अंतर्निहित सुरक्षा-संबंधी संवेदनशीलताओं का पूर्वानुमान लगाते हैं। यूरोपीय संघ की प्रयोगात्मक iBorderCtrl रूपरेखा के समानांतर, Türkiye में उभरते तकनीकी प्रोटोकॉल व्यक्तियों को एल्गोरिदिक जोखिम-मापदंडों के आधार पर वर्गीकृत करते हैं, जो सीमा-पारगमन की अनुमति अथवा निरोध संबंधी प्रक्रियाओं को प्रत्यक्ष रूप से प्रभावित करते हैं। यद्यपि ऐसी प्रणालियाँ प्रशासनिक दक्षता को अधिकतम करती हैं, तथापि इनमें प्रशिक्षण डेटा-समुच्चयों में अंतर्निहित प्रणालीगत पक्षपातों को पुनरुत्पादित करने का उच्च जोखिम विद्यमान है। इस कारण पारदर्शिता और एल्गोरिदिक व्याख्येयता (*explainability*) प्रक्रियात्मक सम्यक् न्याय (*procedural due process*) की सुरक्षा के लिए अपरिहार्य पूर्वशर्तें बन जाती हैं।

अवसंरचनात्मक स्तर पर, ASELSAN के इलेक्ट्रो-ऑप्टिकल निगरानी नेटवर्क, जिन्हें मानवरहित हवाई वाहनों (*Uncrewed Aerial Vehicles—UAVs*) तथा भू-भेदी रडार प्रणालियों द्वारा सुदृढ़ किया गया है, सीमावर्ती परिधि की सतत निगरानी उपलब्ध कराते हैं। इन संसाधनों का जेंडरमेरी इंटीग्रेटेड इन्फॉर्मेशन सिस्टम (*JABS*) और GöçNet के साथ प्रत्यक्ष एकीकरण एक पूर्वानुमानात्मक, डेटा-संचालित सुरक्षा प्रतिमान को मूर्त रूप देता है। इसके अतिरिक्त, Europol, Interpol और UNHCR के साथ संस्थागत डेटा-साझाकरण समझौते मानव तस्करी तथा प्रवासियों की अवैध तस्करी के विरुद्ध अंतरराष्ट्रीय सहयोग को अनुकूलित करते हैं; तथापि ये व्यवस्थाएँ क्षेत्राधिकारगत जवाबदेही, डेटा गोपनीयता तथा राज्य की संप्रभुता से संबंधित महत्वपूर्ण प्रश्न भी उत्पन्न करती हैं।

व्यापक सैद्धांतिक विमर्श से स्पष्ट होता है कि AI-संचालित अवसंरचनाएँ केवल प्रशासनिक प्रदर्शन को उन्नत नहीं करती; वे डिजिटल पैनाप्टिसिज़्म (*digital panopticism*) की संरचना का विस्तार करके राज्य-समाज संबंधों का मूलभूत पुनर्गठन भी करती हैं। Türkiye में प्रवासन-सुरक्षा अंतर्संबंध यह दर्शाता है कि एल्गोरिदिक अभिशासन किस प्रकार मानवीय गतिशीलता के सुरक्षीकरण को तीव्र करता है और भौतिक तथा आभासी—दोनों क्षेत्रों में समावेशन एवं बहिष्करण के नए रूपों को जन्म देता है।

अध्ययन का निष्कर्ष है कि AI-समर्थित सीमा प्रौद्योगिकियाँ समकालीन प्रवासन अभिशासन में अत्यंत परिवर्तनकारी, किंतु संरचनात्मक रूप से द्व्यर्थी विकास का प्रतिनिधित्व करती हैं। एक ओर, वे विशाल पैमाने पर जनसंख्या की आवाजाही के प्रबंधन को अनुकूलित करने की अभूतपूर्व क्षमता प्रदान करती हैं; दूसरी ओर, वे व्यापक डिजिटल निगरानी के सामान्यीकरण तथा दूरगामी परिणामों वाले प्रशासनिक निर्णयों में मानवीय अभिकर्तृत्व (*human agency*) के क्षरण का जोखिम उत्पन्न करती हैं।

अतः प्रवासन सुरक्षा में AI का संस्थानीकरण कठोर मानवाधिकार अनुपालन के अधीन होना चाहिए, जिसमें पारदर्शिता, आनुपातिकता और संस्थागत जवाबदेही को विशेष प्राथमिकता दी जाए। Türkiye के व्यक्तिगत डेटा संरक्षण कानून (*KVKK*) तथा यूरोपीय संघ के सामान्य डेटा संरक्षण विनियमन (*GDPR*) सहित प्रासंगिक विधिक ढाँचों के बीच समुचित सामंजस्य आवश्यक है, ताकि संवेदनशील बायोमेट्रिक सूचनाओं के अनधिकृत उपयोग के जोखिम को न्यूनतम किया जा सके। आधुनिक डिजिटल सीमा व्यवस्थाओं की वैधता बनाए रखने के लिए नैतिक एल्गोरिदिक अभिशासन एक अनिवार्य पूर्वशर्त बना हुआ है।

अंततः, Türkiye का संस्थागत अनुभव डिजिटल युग में राष्ट्रीय सुरक्षा की अनिवार्यताओं और मानवीय गरिमा के संरक्षण के बीच संतुलन स्थापित करने का प्रयास करने वाले राज्यों के लिए महत्वपूर्ण अनुभवजन्य अंतर्दृष्टियाँ प्रदान करता है। भावी अनुसंधान को एल्गोरिदिक निर्णयों के लेखापरीक्षण और उन्हें चुनौती देने के लिए उपलब्ध तंत्रों की जाँच करनी चाहिए, ताकि यह सुनिश्चित किया जा सके कि कृत्रिम बुद्धिमत्ता प्रणालीगत बहिष्करण के तंत्र के बजाय न्यायसंगत सुविधा प्रदान करने वाले साधन के रूप में कार्य करें। सतत प्रवासन अभिशासन के लिए केवल उन्नत तकनीकी दक्षता ही पर्याप्त

नहीं है; इसके लिए न्याय, पारदर्शिता और मानव-केंद्रित नीति-निर्माण के प्रति एक अडिग मानकीय प्रतिबद्धता भी अनिवार्य है।

मुख्य शब्द: कृत्रिम बुद्धिमत्ता, प्रवासन सुरक्षा, सीरियाई संकट, बायोमेट्रिक पहचान, सीमा प्रबंधन।

Yapılandırılmış Özet

Son on yılda düzensiz göç akışlarının giderek artan karmaşıklığı ve hacimsel büyüklüğü, ulusal ve uluslararası güvenlik önceliklerini köklü biçimde yeniden şekillendirmiştir. Geleneksel sınır yönetimi paradigmaları; ulusötesi yasa dışı ağlar, yüksek hızlı hareketlilik ve sistemik insani acil durumlarla karakterize edilen çağdaş göç hareketliliklerini yönetmede yetersiz kalmıştır. Bu bağlamda, yapay zekâ (YZ) teknolojilerinin sınır güvenliği ve göç yönetişimine entegrasyonu, kritik öneme sahip yapısal bir yenilik olarak ortaya çıkmıştır. YZ destekli sistemler; gelişmiş büyük veri analitiği, gerçek zamanlı gözetim, biyometrik doğrulama ve otomatikleştirilmiş idari karar alma mekanizmaları aracılığıyla egemen devletlerin operasyonel etkinliklerini optimize etmelerine imkân sağlamaktadır.

Bu çalışma, özellikle Suriye krizi sonrasında şekillenen konjonktürde, Türkiye'nin YZ destekli teknolojileri daha geniş kapsamlı göç ve sınır güvenliği yapılanması içerisinde nasıl kurumsallaştırdığını incelemektedir. Çalışma üç temel araştırma sorusuna odaklanmaktadır: YZ güdümlü sistemler Türkiye'de göç ve güvenliğin yapısal yönetişini nasıl dönüştürmektedir? Bu teknolojilerin beraberinde getirdiği etik, hukuki ve sosyo-politik sonuçlar nelerdir? Algoritmik otomasyon neden Türkiye'nin dijital göç güvenliği mimarisinin merkezi bir unsuru hâline gelmiştir? Bu sorular çerçevesinde çalışma, Türkiye'nin ampirik deneyimini, çağdaş göç yönetişiminde YZ entegrasyonunun hem operasyonel faydalarını hem de yapısal gerilimlerini yansıtan kritik bir vaka incelemesi olarak ele almaktadır.

Çalışmanın kuramsal çerçevesi, güvenlikleştirme teorisi ile gözetim çalışmalarını bütünleştirmektedir. Kopenhag Okulu'nun yaklaşımından hareketle (Buzan, Wæver, & de Wilde, 1998) araştırma, güvenlik tehditlerinin yalnızca nesnel tehlike ölçütleri üzerinden değil, aynı zamanda siyasal aktörlerin söylemsel pratikleri aracılığıyla inşa edildiğini vurgulamaktadır. Dolayısıyla göçün varoluşsal bir güvenlik tehdidi olarak çerçevelenmesi, yaygın dijital gözetim ve otomatik risk profillemesi de dâhil olmak üzere istisnai yönetim mekanizmalarının meşrulaştırılmasına zemin hazırlamaktadır.

Çalışma ayrıca Foucault (1977) ve Lyon (2001) tarafından kavramsallaştırılan gözetimin biyopolitik analizlerinden yararlanmaktadır. YZ tarafından yönetilen sınır mekânlarında biyometrik verilerin sistematik biçimde toplanması, çıkarılması ve kategorize edilmesi, göçmenleri dijitalleştirilmiş öznelerle dönüştürerek devlet egemenliğini ve asimetrik iktidar ilişkilerini pekiştirmektedir. Buna ek olarak Gonzalez'in (2019) "dijital sınırlar" kavramsallaştırması, teknolojik altyapıların devlet iktidarını fiziksel ve bölgesel sınırların çok ötesine nasıl taşıdığını ortaya koymaktadır. Dolayısıyla YZ teknolojileri, hem teknik araçlar hem de vatandaşlık, kimlik ve aidiyetin hukuki ve toplumsal sınırlarını sürekli olarak yeniden tanımlayan siyasal mekanizmalar şeklinde işlev görmektedir.

Bu kuramsal perspektifleri bir araya getiren araştırma, YZ'yi tarafsız bir idari araç olarak değil, algoritmik mimarisinde belirli ideolojik ve normatif ön kabulleri barındıran sosyo-teknik bir düzenek olarak kavramsallaştırmaktadır. Çalışma bu yönüyle, göç yönetiminde dijital yönetişimin çift kullanımlı doğasına ilişkin gelişmekte olan literatüre katkıda bulunmakta; dijital yönetişimin aynı anda hem idari etkinliği artıran bir araç hem de toplumsal denetim aygıtı olarak işleyebildiğini ortaya koymaktadır.

Metodolojik olarak çalışma, sistematik doküman analizine dayalı nitel bir araştırma deseni benimsemektedir. Birincil ampirik veriler, Türkiye Cumhuriyeti İçişleri Bakanlığına bağlı kurumlar, özellikle Göç İdaresi Genel Müdürlüğü (DGMM) tarafından yayımlanan resmî mevzuat metinleri, politika beyanları ve stratejik çerçevelerden elde edilmiştir. İkincil veriler ise Birleşmiş Milletler Mülteciler Yüksek Komiserliği (UNHCR), Uluslararası Göç Örgütü (IOM), FRONTEX, Europol ve Avrupa Komisyonu dâhil olmak üzere uluslararası kuruluşlar tarafından yayımlanan değerlendirme raporlarından oluşmaktadır.

Toplanan metinler, YZ teknolojilerinin operasyonelleştirilmesine ilişkin örüntüleri üç temel boyutta belirlemek amacıyla tematik kodlamaya tabi tutulmuştur: (1) biyometrik kimliklendirme ve dijital profillemeye, (2) algoritmik risk değerlendirmesi ve otomatik karar destek sistemleri ve (3) gerçek zamanlı gözetim protokolleri ile sınır ötesi istihbaratın birlikte işlerliği. Analitik güvenilirlik, ulusal kurumsal çıktılar ile

uluslararası raporlar arasında gerçekleştirilen kaynaklar arası üçgenleme yoluyla güçlendirilmiş; kuramsal duyarlılık ise verilerin yorumlanmasıyla güvenlikleştirme ve biyopolitik çerçevelere bağlı kalmasını sağlamıştır.

Ampirik bulgular, Türkiye'nin dijital göç güvenliği çerçevesinin çok katmanlı ve teknoloji aracılı bir aygıt olarak işlediğini göstermektedir. YZ destekli araçlar, sınır denetiminin hassasiyetini, hızını ve öngörülebilirliğini artırmak amacıyla kullanılmakta; böylece birbirinden farklı idari veri tabanları birbirine bağlı bir yönetim matrisi içerisinde bütünleştirilmektedir.

Özellikle Türkiye'nin ulusal GöçNet altyapısı, geçici koruma altındaki nüfusa ilişkin parmak izi, yüz morfolojisi ve iris taramalarını kapsayan kapsamlı biyometrik kayıtları konsolide etmektedir. Bu veri kümeleri gerçek zamanlı kimlik doğrulama, mekânsal hareketliliğin izlenmesi ve idari risk değerlendirmesini mümkün kılmaktadır. Benzer şekilde, büyükşehirlerde YZ destekli doğrulama birimleri olarak konuşlandırılan Mobil Göç Noktaları, merkezî olmayan biyometrik tarama ve veri tabanlarıyla anlık senkronizasyon olanağı sağlamaktadır. Bu yenilikler devlet bürokrasisinin denetim kapasitesini güçlendirmekle birlikte veri işleme rızası, bilgi mahremiyeti ve içkin algoritmik önyargılar bakımından ciddi kaygılar doğurmaktadır.

Makine öğrenmesi algoritmaları; biyografik göstergeleri, transit güzergâhlarını ve dijital izleri analiz ederek örtük güvenlik açıklarını öngörmeye çalışmaktadır. Avrupa Birliği'nin deneysel iBorderCtrl çerçevesine paralel olarak Türkiye'de gelişmekte olan teknolojik protokoller, bireyleri sınır geçişine izin verilmesi veya alıkoyma prosedürlerini doğrudan etkileyen algoritmik risk ölçütleri üzerinden sınıflandırmaktadır. Bu sistemler idari etkinliği en üst düzeye çıkarabilmekle birlikte, eğitim veri kümelerinde yerleşik sistemik önyargıları yeniden üretme konusunda yüksek risk taşımaktadır. Bu nedenle şeffaflık ve algoritmik açıklanabilirlik, usule ilişkin güvencelerin ve adil işlem ilkesinin korunması açısından vazgeçilmez ön koşullar hâline gelmektedir.

Altyapısal düzeyde ASELSAN'ın elektro-optik gözetim ağları, insansız hava araçları (İHA/UAV) ve yer altı görüntüleme radar sistemleriyle desteklenerek sınır hattının kesintisiz biçimde izlenmesini sağlamaktadır. Bu unsurların Jandarma Entegre Bilgi Sistemi (JABS) ve GöçNet ile doğrudan bütünleştirilmesi, öngörücü ve veri odaklı bir güvenlik paradigmasını somutlaştırmaktadır. Ayrıca Europol, Interpol ve UNHCR ile kurumsallaştırılmış veri paylaşımı anlaşmaları, insan ticareti ve göçmen kaçakçılığıyla mücadelede ulusötesi iş birliğini optimize etmekte; bununla birlikte yargısal yetki ve hesap verebilirlik, veri mahremiyeti ve devlet egemenliği bakımından kritik sorular ortaya çıkarmaktadır.

Daha geniş kuramsal tartışma, YZ güdümlü altyapıların yalnızca idari performansı artırmakla kalmadığını, aynı zamanda dijital panoptisizmin mimarisini genişleterek devlet-toplum ilişkilerini köklü biçimde yeniden yapılandırıldığını göstermektedir. Türkiye'deki göç-güvenlik ilişkisi, algoritmik yönetimin insan hareketliliğinin güvenlikleştirilmesini nasıl hızlandırdığını ve hem fiziksel hem de sanal alanlarda yeni dâhil etme ve dışlama biçimlerinin ortaya çıkmasına nasıl yol açtığını göstermektedir.

Çalışma, YZ destekli sınır teknolojilerinin çağdaş göç yönetiminde son derece dönüştürücü, ancak yapısal olarak ikircikli bir gelişme oluşturduğu sonucuna ulaşmaktadır. Bu teknolojiler, yüksek hacimli nüfus hareketlerinin yönetiminin optimize edilmesi bakımından daha önce görülmemiş olanaklar sunarken aynı zamanda yaygın dijital gözetimin normalleşmesi ve önemli sonuçlar doğuran idari kararlarda insanın karar verme yetisinin ve failliğinin aşınması riskini beraberinde getirmektedir.

Bu nedenle YZ'nin göç güvenliği alanında kurumsallaştırılması, şeffaflık, ölçülülük ve kurumsal hesap verebilirlik ilkelerini merkeze alan sıkı bir insan hakları uyum rejimine tabi tutulmalıdır. Türkiye'nin Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) dâhil olmak üzere ilgili hukuki çerçevelerin, hassas biyometrik bilgilerin yetkisiz kullanımını sınırlandıracak biçimde uyumlaştırılması gerekmektedir. Etik algoritmik yönetim, modern dijital sınır rejimlerinin meşruiyetinin korunması açısından vazgeçilmez bir ön koşul olmayı sürdürmektedir.

Sonuç olarak Türkiye'nin kurumsal deneyimi, dijital çağda ulusal güvenlik gereklilikleri ile insan onurunun korunması arasında denge kurmaya çalışan devletler açısından değerli ampirik çıkarımlar sunmaktadır. Gelecekteki akademik araştırmalar, yapay zekânın sistemik dışlamanın bir mekanizmasına değil, hakkaniyetli kolaylaştırmanın bir aracına dönüşmesini güvence altına almak amacıyla algoritmik kararların denetlenmesine ve bunlara itiraz edilmesine imkân sağlayan mekanizmaları incelemelidir. Sürdürülebilir göç

yönetişimi yalnızca ileri düzey teknolojik yetkinlik değil; aynı zamanda adalet, şeffaflık ve insan merkezli politika yapımına yönelik tavizsiz bir normatif bağlılık gerektirmektedir.

Anahtar Kelimeler: Yapay Zekâ, Göç Güvenliği, Suriye Krizi, Biyometrik Kimliklendirme, Sınır Yönetimi.



www.turkishstudies.net/economy

Turkish Studies - Economics, Finance, Politics

eISSN: 2667-5625



ANKARA SCIENCE
UNIVERSITY

Artificial Intelligence-Based Border Technologies and Digital Migration Security in Türkiye

Introduction

The increasing volume and complex nature of international migration movements have made border security one of the fundamental components of states' national security policies. Today, while migration is an empirical and demographic phenomenon, it is addressed as a multi-dimensional security issue associated with public order, border control, counter-terrorism, and social stability. In particular, mass forced migration movements make it imperative to reevaluate the traditional understanding of border management. In this context, states are directed toward more effective, rapid, and technology-supported border management models.

One of the most critical components of this transformation is AI-powered border technologies. Big data analytics, biometric identity verification, algorithmic risk analysis, and real-time surveillance systems are increasingly utilized in monitoring irregular migration movements, risk assessment, and managing border security processes. Thus, border security goes beyond being limited to physical control activities, transforming into a data-driven governance domain supported by digital technologies.

This transformation also brings forth significant theoretical debates in the security studies literature. While securitization theory posits that migration is constructed as a security threat through political discourses (Buzan et al., 1998), surveillance studies draw attention to the role of digital technologies in monitoring, classifying, and governing individuals (Lyon, 2001). Similarly, Foucault's (1977) biopolitics approach explains how modern states govern populations through registration, data, and surveillance mechanisms. These theoretical approaches evaluate AI-powered border technologies not only as technical tools but also as socio-technical mechanisms that transform security policies and migration governance. Furthermore, Molnar's (2020) work highlights the risks posed by digital technologies used in border regions regarding human rights and accountability.

In the literature, AI-powered border technologies are predominantly examined in the context of the effectiveness of border security, the prevention of irregular migration, and the enhancement of operational capacity. Conversely, the mechanisms through which these technologies transform migration management, how they reshape securitization processes, and the ethical and legal consequences they produce have been addressed to a limited extent, particularly in the case of Türkiye.

Türkiye has become one of the countries making the most comprehensive use of digital border technologies due to its geopolitical position and the intense irregular migration mobility it has faced, especially following the Syrian civil war. The GöçNet system, biometric identity verification infrastructures, mobile migration points, unmanned aerial vehicles, thermal cameras, and AI-powered analysis systems constitute the core components of digitalization in border management.

Therefore, the case of Türkiye offers a significant research area for examining the impacts of AI-powered border technologies on migration management, securitization, and digital surveillance processes.

This research aims to examine the aforementioned literature gap through the case of Türkiye. This study seeks answers to the questions of through which mechanisms AI-powered border technologies transform migration management in Türkiye, how these technologies reproduce the securitization process, and what the ethical, legal, and social consequences of AI-powered border technologies are.

A qualitative research method was adopted in the study, and document analysis was utilized as the data collection technique (Bowen, 2009). The dataset of the research consists of reports and policy documents published between 2018 and 2026 by the Republic of Türkiye Ministry of Interior, Presidency of Migration Management, Presidency of Defense Industries, UNHCR, IOM, FRONTEX, and Europol. The documents were selected using purposive sampling in line with the purpose of the research; the data were evaluated using thematic analysis within the framework of themes such as biometric control and digital profiling, algorithmic risk analysis, and cross-border surveillance through data sharing. Because the study relies solely on institutional documents and reports, the findings obtained were interpreted on the basis of state policies and institutional practices rather than the individual experiences of migrants. In this regard, supporting the impacts of AI-powered border technologies on migrants' daily lives and social integration processes with field research is of importance for future studies.

The Role of Artificial Intelligence in the Field of Security

One of the most important features of artificial intelligence is its capacity to analyze large-volume datasets in a short time. This feature reduces the need for human labor in the fields of security and public administration while accelerating decision-making processes (Önder & Saygılı, 2018). Although it does not appear possible to completely mimic human cognitive processes through technological systems, developments in data processing capacity are progressively mainstreaming the use of artificial intelligence technologies in public spheres. Particularly in fields such as border security and migration management where high-volume data is generated, AI systems offer significant advantages in terms of operational efficiency.

AI systems are not merely technical tools that provide rapid access to data; they also possess the capacity to guide decision processes by analyzing data simultaneously. Algorithmic decision mechanisms prioritize the "most appropriate" option by detecting specific risk patterns within existing datasets. However, this situation causes decision processes to be carried out not over all data, but through specific parameters and classifications (Kokkalis, 2019, p. 310). The questions of which data algorithms prioritize, which risk categories they take as a basis, and which groups they exclude bring about important debates. Furthermore, the effective functioning of AI systems depends on advanced digital infrastructures, high processing capacity, and continuous data flow. Therefore, AI technologies require a robust data management system alongside technical capacity.

In order to evaluate the use of AI technologies in the field of migration security, it is necessary to take into account that migration has become a securitized phenomenon. Securitization theory posits that migration is constructed as a security problem through political discourses independently of objective threats. According to Buzan, Wæver, and de Wilde (1998), a subject becoming a security issue is associated with the discursive interventions of political actors. Within this framework, migrants can be defined within categories of "risk," "threat," or "the other," and extraordinary security practices can be legitimized. AI-powered border technologies reproduce this securitization process through digital surveillance mechanisms.

The securitization of migration leads to migrants transforming into constantly monitored data subjects within administrative and technological control mechanisms. According to Bellanova and Duez (2012, p. 110), digital border technologies produce socio-technical tools that evaluate migrants within algorithmic risk categories, despite carrying a claim of technical neutrality. When evaluated within the context of Foucault's biopolitics approach, digital border systems make it possible to govern populations through biometric data (Ajana, 2013, p. 598). Thus, border security ceases to be a mechanism consisting solely of physical control processes and expands with data collection, classification, and digital surveillance processes.

This transformation also generates significant effects on social integration processes. Security-centric digital applications cause migrants to become individuals who are continuously monitored and evaluated through risk scores. According to Amore (2006, p. 338), algorithmic security systems produce an exclusionary digital hierarchy by creating categories of "risky" and "integrable" migrants. This situation can weaken the trust relationship established by migrants with the host society and deepen digital othering processes. AI systems place not only the physical mobility of migrants under control, but also their digital footprints, social networks, and behavioral patterns (Zuboff, 2019, p. 25).

The use of AI technologies in the field of migration security expresses a political and administrative transformation beyond being a technical preference. The close relationship between technology and security policies establishes a new data-based control regime in migration management. Therefore, the integration of AI technologies into border operations is evaluated as a strategic priority by many states (Feldstein, 2019, p. 5). Facial recognition systems, biometric analysis tools, motion sensors, thermal cameras, and scanning software are among the core components of contemporary digital border management (Feldstein, 2019, p. 7). These systems accelerate security processes and increase data-based predictive capacity (Zuiderwijk, Chen, & Salem, 2021, p. 5).

AI-powered border technologies allow large border regions to be monitored with fewer personnel. In particular, unmanned aerial vehicles, automated analysis systems, and real-time data processing mechanisms expand the scope of border security operations. These developments demonstrate that digitalization and automation are occupying an increasingly central position in migration management.

Digital Border Security: AI-Based Applications at Entry Points

Today, in cases where traditional methods are insufficient for ensuring border security, artificial intelligence (AI)-based entry control systems stand out as a new paradigm. These systems play a critical role in regions with heavy migrant flows thanks to their high accuracy rates, processing speed, and automated analysis capacity. Especially in crisis zones where threats such as irregular migration, human trafficking, and unauthorized border crossings increase, AI systems enhance security. At the same time, they elevate the efficiency and transparency of migration management processes.

Artificial intelligence is a technology that imitates human reasoning by reaching rational decisions based on provided information. The EU's "High-Level Expert Group on Artificial Intelligence" (HLEG) defines artificial intelligence as systems that are given a complex goal and that collect, interpret, and process data, deciding on the best action to achieve the given goal based on this data (Dumbrava, 2021).

Regarding border control technologies, Gonzalez (2019) draws attention to the fact that "various technologies such as identity cards, license plate readers, facial recognition software, drone surveillance, video cameras, motion sensors, and radar systems" constitute a "new high-tech border." These technologies directly change how migrants appear to authorities and how they negotiate

mobility and space. Gonzalez's (2019) treatment of the border as a "logistical infrastructure" expands established approaches that evaluate the border not merely as a line on a map, but as a dispersed apparatus, infrastructure, or network established within bounding practices spread across different geographies.

Gillespie and colleagues (2018) define the intersection of digital and physical mobility as the "digital passage." In this context, Syrian refugees use smartphones and associated digital infrastructures to plan, navigate, and document their journeys. Sometimes, they use these tools to increase their visibility in order to survive at sea. The literature significantly focuses on the impact of digital technologies on migration processes and the vulnerable situations in which migrants find themselves. Thus, connections are established between individuals on the move utilizing digital technologies both for navigation and to become invisible in order to evade migration controls, and the critical support provided through activist groups in life-threatening situations. Within this framework, digital activism and digitally mediated mobilities exist within practices that visibly question and challenge border control.

In this context, protracted humanitarian crises such as the Syrian Crisis pave the way for artificial intelligence (AI)-based applications to play a central role in border security. Digital border security no longer merely involves monitoring crossings, but also encompasses multi-layered processes such as identity verification, risk analysis, and behavioral prediction. Within this framework, AI-based entry control systems will be examined under three main headings: (i) biometric verification systems, (ii) risk analysis and automated decision systems, and (iii) real-time monitoring and cross-border data sharing.

Biometric Verification Systems

In contemporary migration management practices, increasing the reliability and speed of identity verification processes is of strategic importance. Accordingly, biometric identity verification systems are positioned as a central tool in the identification and monitoring process of migrants and asylum seekers. Physical and behavioral characteristics belonging to individuals, such as fingerprints, facial recognition, retinal scans, and voice biometrics, are transferred to a digital environment. Thus, unique and tamper-proof identity verification processes are made possible (Maguire, 2009). Alongside identification, biometric data also function as the primary data source in multi-dimensional migration management activities such as digital profiling, risk analysis, and movement tracking (Ajana, 2013).

AI-powered border security applications stand out particularly through biometric recognition technologies. These systems largely eliminate the tamper-prone nature of traditional documents and automate the identity verification process at border crossings with high accuracy rates. Biometric verification ensures that an individual's identity is confirmed based on their physical and behavioral traits (Jain et al., 2000, p. 91). Artificial intelligence algorithms utilize deep learning and machine learning models in processing biometric data, yielding more precise and rapid results. Methods such as facial recognition, fingerprint analysis, and voice recognition are effectively used to verify individuals' identification information at border crossings. In particular, facial recognition technologies, developed using artificial neural networks, can operate with high accuracy even on low-resolution and partially occluded faces. Such systems can make real-time decisions while matching passport information with biometric data (Minaee et al., 2023, p. 8650).

At this point, machine learning algorithms are utilized to detect suspicious movement patterns by analyzing migrants' previous crossing data. For instance, systems like "iBorderCtrl," applied at some of the EU's external borders, evaluate the likelihood of false statements by conducting micro-expression analyses on the responses given by individuals. "iBorderCtrl" stands for Intelligent Border Control System (<https://www.iborderctrl.eu/>). Researchers developed an AI-based lie detector to help control the entry of non-EU nationals into the Schengen area (Dumbrava,

2021). Although such systems are open to ethical debates, data obtained in the field indicate that these applications provide deterrence in terms of security.

Risk Analysis and Automated Decision Systems

Artificial intelligence-supported systems have become not only supportive elements of migration security policies today, but also their guiding tools. Particularly in sudden and large-scale mass migration events, the ability of states to make rapid and accurate decisions regarding security and public order is made possible by the deployment of big data analytics and automation-based systems (Broussard, 2018). The intense migration movements experienced in countries affected by the Syrian crisis clearly demonstrate the necessity of using these technologies in both border control and internal security fields.

Risk analysis is a data-driven evaluation process aimed at proactively detecting security threats and social vulnerability levels carried by migrant individuals. Artificial intelligence systems used in this process process versatile data sources such as biometric recognition data, travel history, social media posts, and even psychosocial analyses in an integrated manner (Leese, 2014). Risk profiles are generated from data obtained from algorithms such as machine learning and natural language processing (NLP). For instance, online or field-based data indicating that an individual has had contact with armed groups in their past can be automatically analyzed, leading to their assignment to the "high risk" category. Similarly, the probability of women and children becoming victims of human trafficking can also be predicted by analyzing specific behavioral patterns (O'Neil, 2016).

The most common use of these systems appears in border security. Frontex, the European Border and Coast Guard Agency, has implemented pilot artificial intelligence applications supported by facial recognition systems, digital passport verification technologies, and behavioral analysis tools (Frontex, 2021). These systems can evaluate the risk of false statements by analyzing travelers' facial expressions, eye movements, stress levels, and speech patterns at border checkpoints.

The outputs of risk analysis are directly integrated into security processes through automated decision systems. Automated decision systems perform operations such as granting entry permits, applying detailed checks, or generating rejection decisions regarding individuals based on risk scores calculated by the system, without requiring human intervention (Wachter et al., 2017). While such systems save time, they also increase consistency in decision-making processes by reducing subjectivity and human error. However, the ethical dimension of these technologies is seriously debated. Artificial intelligence systems are dependent on the datasets they are trained on. Historical biases contained in these data carry the risk of being reproduced through algorithms (Eubanks, 2018). This situation raises the debate that certain groups may be subjected to systematic discrimination.

Therefore, explainable artificial intelligence principles gain importance in automated decision systems. Explainability means that a system can present why it reached a particular decision in a way that human users can understand (Wachter et al., 2017). Since the "right to a reasoned decision" is among the fundamental rights of individuals, particularly in international law, AI-based decisions must also be traceable and justifiable. Otherwise, individuals' avenues for seeking rights can be severely blocked, and systems can become open to arbitrary practices.

AI-powered risk analysis and automated decision systems are systems that provide high efficiency and speed in migration security, yet also harbor serious ethical, legal, and societal risks. Therefore, it is of great importance that these systems are developed and implemented not only with a security-oriented focus, but also within a human rights-based framework.

While automated decision systems and risk profiling technologies alleviate operational burden, they bring along discussions of algorithmic discrimination. FRONTEX, the European Union's border agency—to which Türkiye also provides data integration—directly drew attention to

the dangers harbored by this digital ecosystem in its official report: "Machine learning-supported analysis tools carry the risk of reflecting historical and structural biases in the datasets they are trained on and disproportionately classifying certain ethnic or demographic groups as risky" (FRONTEX, 2021, p. 14). This institutional finding is in complete harmony with Beduschi's (2021, p. 585) academic thesis that artificial intelligence systems erode legal guarantees by trapping migrants into predefined "suspicious" categories.

This demonstrates that AI-powered risk analysis applications are evaluated as tools supporting decision-making mechanisms in border security processes. These systems can contribute to the more rapid analysis of irregular migration movements and the direction of security units' resources according to risk priorities. Nevertheless, the presence of limited information regarding the datasets and criteria upon which algorithmic evaluations are performed brings along certain debates in terms of transparency and accountability. Therefore, it is important to handle algorithmic decision support systems within a balanced framework between security requirements and the protection of fundamental rights and freedoms.

Real-Time Monitoring and Cross-Border Data Sharing

The effectiveness of artificial intelligence-based border security applications has increased significantly with the development of real-time data collection and analysis mechanisms. Particularly in mobile and difficult-to-control border regions, surveillance capacity that cannot be provided by traditional methods transforms into a digitized control system with the activation of autonomous technologies. In this context, visual and sensory data coming from unmanned aerial vehicles (UAVs), thermal cameras, facial recognition systems, motion sensors, and fixed surveillance towers are processed in real time by artificial intelligence algorithms (Bellanova, 2017). These systems can detect unusual mobility on the border line, such as mass human crossings, frequent movement in specific areas, or behaviors aimed at concealment, and guide human operators through this data (Leese, 2014).

Alongside real-time monitoring applications, international data sharing is of great importance for the sustainability and holistic effectiveness of AI-based border security. Because migrants cross into multiple countries rather than just one and exhibit cross-border mobility, information flow and data coordination are required among countries. At this point, thanks to collaborations carried out with organizations such as INTERPOL, Europol, and Frontex, the digital footprints of suspect individuals are shared between countries, and multiple border crossing records and potential security threats are collected in common data pools (Bigo et al., 2013). Such platforms serve not only humanitarian purposes such as monitoring crime or terror suspects, but also finding missing migrants, identifying human trafficking victims, and improving refugee protection mechanisms.

Data sharing is not merely a technical matter; it is also a political, legal, and ethical process. The sensitivities of nation-states regarding data sovereignty can lead to severe limitations in cross-border data transfers (Jeandesboz, 2016). Therefore, data sharing systems need to be structured in compliance with both national legislation and international norms such as the General Data Protection Regulation (GDPR). Furthermore, the accuracy, timeliness, and neutrality of the data used by artificial intelligence systems are of vital importance for the reliability of the systems. Otherwise, problems such as misidentifications, individuals unfairly classified as risky, and data breaches can create serious crises in terms of individual rights and international cooperation (Wachter et al., 2017).

The integration of real-time monitoring technologies and international data sharing mechanisms reinforces the technical effectiveness and global legitimacy of AI-powered border security policies. However, this integration is not purely technical. It becomes meaningful and sustainable only when addressed with an awareness of ethical, legal, and political responsibility.

AI-Powered Migration Security in Türkiye

The Syrian civil war, which began in 2011, created a major humanitarian crisis at the regional level, displacing millions of people. During this process, Türkiye became the country accepting the highest number of Syrians due to its geographical and cultural proximity. As of 2026, there are 2,276,997 Syrians under Temporary Protection in Türkiye (Migration Management, 2026). This extraordinary population mobility has made it imperative for Türkiye to develop new policies and practices regarding border security, registration systems, social integration, and public order. In this context, artificial intelligence technologies have emerged as one of the prominent tools aimed at strengthening migration security processes.

Türkiye's strategy to combat irregular migration is built upon five fundamental stages in line with a multi-layered and holistic security approach. The first stage of this strategic framework involves measures aimed at bringing migration under control at its source. Within this scope, it is aimed to reduce the root causes of migration through diplomatic initiatives and cross-border cooperations. The second stage aims at the highest level of protection of land borders. Enhancing security capacity at the border line is prioritized through physical barriers, technological surveillance systems, and integrated border management applications. The third stage focuses on ensuring internal security through the detection of irregular migrants residing illegally within the country and effective law enforcement control against human trafficking. In this context, the deployment of digital monitoring systems such as mobile migration vehicles significantly increases field effectiveness. The fourth stage of the strategy encompasses combating irregular labor migration. Measures taken against the informal employment of migrants, who are rendered vulnerable to labor exploitation, point to the social dimension of migration policies. The fifth and final stage covers deportation processes conducted rapidly, systematically, and in compliance with human rights. This mechanism aims to ensure the return of irregular migrants to their own countries effectively and to increase the functionality of removal centers (Migration Management, Combating Irregular Migration). Türkiye's five-stage strategy points to a holistic policy orientation that handles migration management not only from a border security perspective, but also together with its socioeconomic, legal, and ethical dimensions.

In practices in Türkiye, AI systems do not make fully autonomous decisions; they operate alongside human supervision. This approach contributes to the protection of individual rights by establishing a balance between technological objectivity and human discretion. Furthermore, AI-powered systems allow migrants to be evaluated in a fairer and more systematic manner, thus supporting individuals who may acquire refugee status to access their rights more quickly and securely. In this framework, we will examine AI applications in Türkiye under the headings of biometric verification and digital profiling, risk analysis and automated decision systems, and real-time monitoring and cross-border data sharing.

Biometric Verification and Digital Profiling

Türkiye utilizes biometric verification systems as one of the primary tools of digital border management in managing irregular migration. Biometric data such as fingerprints, facial recognition, and iris scans are analyzed in real time, particularly at Mobile Migration Point applications and border crossing points. Thus, identity verification, legal status control, and operations aimed at detecting irregular migration are accelerated. Within the scope of the Mobile Migration Point application, the biometric data of foreigners unable to present identification are verified via the GöçNet system, and administrative procedures are executed in line with the obtained information.

Biometric data collected during the registration processes of Syrians under temporary protection are managed centrally through the GöçNet system (Presidency of Migration Management, 2020). This system ensures the integrated management of administrative records regarding public services alongside identity verification. Furthermore, biometric verification systems used at border

gates operate in integration with national databases, contributing to the detection of forged document usage and increasing the effectiveness of security controls (Frontex, 2021).

The proliferation of biometric systems increases operational efficiency while bringing along significant debates regarding personal data protection, privacy, and accountability. Applying the technical and administrative measures envisaged within the scope of the KVKK (Personal Data Protection Law) in the processing of biometric data is of great importance. Similarly, Wachter et al. (2017) draw attention to the fact that mismatches occurring in biometric systems can make individuals' avenues for seeking rights difficult. Therefore, a balanced approach must be adopted between security requirements and the protection of fundamental rights and freedoms in the processing of biometric data.

According to Ministry of Interior data, as of 2025, 4,572, 712 identity checks have been carried out via GöçNet integration in Mobile Migration Point vehicles (Ministry of Interior, 2025). These data demonstrate that biometric verification systems have reached significant operational capacity in Türkiye's irregular migration management. Nevertheless, UNHCR (2022) emphasizes that observing the principles of explicit consent, data security, and privacy in the processes of processing biometric data is a fundamental requirement in terms of the international protection regime.

The findings obtained indicate that biometric verification systems have become digital governance mechanisms supporting data-driven decision-making processes in migration management, alongside being technical tools facilitating identification. In the case of Türkiye, the proliferation of these systems points to border security heading toward a more integrated structure with digital technologies. When evaluated from the perspective of securitization theory, biometric technologies stand out as tools that strengthen digital surveillance capacity and support the risk-oriented border management approach. Nevertheless, studies based on field research are needed to reveal the impacts of these technologies on migrants' daily lives and social integration processes.

Risk Analysis and Automated Decision Systems

In recent years, the increasing role of digital technologies in migration management and border security policies has enabled states to head toward faster, more effective, and data-driven decision-making processes. Türkiye has become a significant actor in this transformation process and has made notable progress in integrating artificial intelligence-supported systems into the field of migration security. Particularly thanks to risk analysis and automated decision systems, taking preventive measures in a timely manner in combating irregular migration, utilizing resources more efficiently, and supporting strategic decisions in border management have been made possible.

One of the most controversial uses of artificial intelligence is the classification of migrants according to security risks. As seen in some algorithmic systems used in Europe, efforts to extract risk profiles through data such as specific behavioral patterns, travel history, and social media interaction are also observed in Türkiye (Frontex, 2022). Although the algorithmic structure of these systems is not officially disclosed, there are findings indicating that AI-supported pre-analyses are used in interviews and that certain applications are classified as low-priority or risky by these systems.

The reflections of the algorithmic bias risk frequently emphasized in international literature within the Turkish practice carry the potential to materialize specifically through GöçNet and Mobile Migration Points. For example, determining which neighborhoods Mobile Migration Points will be deployed in in metropolitan cities or determining individuals to undergo field identity checks based on AI-supported risk maps can reproduce socio-economic biases in past crime or irregular migration data upon which algorithms are trained. Although clear algorithmic risk scoring software directly

used in the Turkish practice is not included in official documents, possible future reflections of such systems in international literature are handled with caution.

Similar to European Union countries, applications aimed at generating risk profiles through various data such as individuals' digital footprints, travel history, border crossing attempts, and specific behavioral patterns are also developed in Türkiye (Frontex, 2022). These systems transform border security from being a physical intervention area into a preventive and analysis-based governance tool. Thanks to insights obtained from relevant data, migration movements are predicted more accurately, and decision processes can be based on objective grounds.

Border control systems supported by electro-optic surveillance systems developed by ASELSAN, unmanned aerial vehicles (UAVs), and motion-sensing radars have enabled instant tracking of migrant movements (ASELSAN, 2021). Artificial intelligence software used in these systems automatically classifies objects and movements detected in border regions. Alerts are sent to security units for actions defined as "suspicious" by the system.

Türkiye's applications in this field have also been cited as an example by Frontex, the European Union's border management agency. In Frontex's 2022-2032 strategic risk analysis report, it was emphasized that Türkiye's border security systems and early warning mechanisms are of great importance for Europe's security (Frontex, 2022).

These developments demonstrate that migration management in Türkiye is restructured within an increasingly digitalized and data-driven security architecture. While AI-powered systems increase operational coordination in border management processes, they also deepen data-based control mechanisms relying on the classification and monitoring of migrants. This situation shows that migration management is not limited to physical border control. It also reveals that it transforms into a multi-layered governance domain through digital surveillance, data analytics, and algorithmic evaluation processes.

Real-Time Monitoring and Cross-Border Data Sharing

Türkiye has invested in real-time monitoring technologies and increased cross-border cooperations in order to strengthen border security against irregular migration waves intensifying particularly after 2011. Thanks to systems developed within this scope, the tracking of migrant movements in Türkiye's border regions is carried out not only with physical patrols, but with an approach based on digital surveillance networks and data sharing.

The cornerstone of real-time monitoring capacity is the high-technology electro-optic surveillance systems established on Türkiye's southern borders. These systems developed by ASELSAN have been integrated into border units in Şanlıurfa, Hatay, Kilis, Gaziantep, and Mardin provinces and supported by Dragoneye platforms providing 24-hour uninterrupted surveillance. These platforms can distinguish human, vehicle, and animal movements within a 20-kilometer range and instantly transmit the target's location to command centers with GPS and digital compass support (ASELSAN, 2021).

Another element increasing the effectiveness of these systems is the data processing capability supported by image processing and artificial intelligence algorithms. For example, AI-supported classification systems capable of distinguishing whether an object approaching the border is a human, animal, or vehicle transmit not only images to security units in the field, but also alarm levels and intervention recommendations according to the situation.

Cross-border data sharing has developed within the scope of Türkiye's security cooperations, particularly with neighboring countries. Türkiye works in coordination with security units operating along the Iraq and Syria border line, establishing "Joint Data Sharing Points" in specific operation zones to share common threat data. These points aim to monitor border crossing mobility,

particularly directed toward smuggling and the fight against terrorism. UAV images, motion sensor data, and biometric identification results are shared mutually.

Türkiye's cross-border data sharing is not limited to the regional level; various data exchange protocols are also executed with institutions such as Interpol, Europol, UNHCR, and IOM. Within the framework of this cooperation, identity, fingerprint, and biometric data regarding irregular migrants deported or captured from Türkiye are shared with international systems; thus, the fight against migrant smuggling and transborder organized crime is conducted in a coordinated manner.

Real-time monitoring systems enable not only post-event intervention in migration management, but also preventive security practices based on data-driven prediction and risk analysis.

How the national security architecture transformed into a global surveillance network through cross-border data sharing materializes in the current operational statistics of institutions. Nevertheless, IOM points to data sovereignty and privacy issues by stating that this high-volume and "seamless" data flow among security agencies causes migrants' digital footprints to circulate permanently in criminal databases (IOM, 2022).

The security of central databases such as GöçNet, which house biometric data belonging to millions of migrants, must be evaluated within the scope of national critical infrastructure security. Protecting the integrity of these data networks against cross-border cyber threats is not merely a technical necessity. It is also a fundamental component of cyber deterrence strategies. Considering that data leaks or system manipulations can directly threaten national security, supporting these digital infrastructures with advanced encryption and proactive cyber defense mechanisms is extremely critical.

The findings demonstrate that digital border technologies render national security applications more integrated with international data sharing mechanisms. Türkiye's data sharing applications carried out with international organizations and regional cooperation mechanisms contribute to increasing operational capacity in the fight against irregular migration and transborder crimes. Nevertheless, cross-border data sharing has aspects that need to be evaluated carefully in terms of the protection of personal data, data security, and international legal responsibilities. In this framework, it is important for digital border governance to develop a balanced approach between effectiveness and the protection of fundamental rights.

AI-Supported Security Approaches and Social Integration

AI-supported migration security applications reshape not only migrants' border crossings, but also the relations they establish with the host society. Social integration, in this context, is a multi-dimensional process that is not limited solely to economic participation or legal status; it encompasses belonging, social acceptance, and mutual trust (Castles et al., 2014).

AI-based systems facilitate administrative integration on the one hand by regulating migrants' access to public services. Biometric data systems and digital registration mechanisms make individuals' access to health, education, and social services more systematic. However, this process simultaneously leads to migrants transforming into constantly monitored data subjects. As emphasized in surveillance literature, this means the regulation of individuals' behaviors on a data basis (Lyon, 2001).

AI-supported risk analysis and profiling systems can produce new forms of exclusion by dividing migrants into algorithmic categories. Such classifications can lead to the reproduction of biases existing in datasets, causing certain groups to fall into systematically disadvantaged positions (Eubanks, 2018). In this context, migrants become individuals evaluated not only through their physical mobility, but also through their digital profiles. This situation can also affect the relationships of belonging and trust established by migrants with the host society. As discussed in

surveillance literature, administrative practices aimed at keeping individuals under constant supervision carry the risk of carrying the relationship established by individuals with public institutions onto a security-oriented ground. Particularly the intensive use of biometric registration, digital tracking, and algorithmic evaluation processes can cause migrants to experience social acceptance processes within a security-oriented framework. Thus, social integration ceases to be an issue of legal status or access to services; it transforms into a multi-layered process where the relationship between digital surveillance and social belonging is reshaped.

Migration management transforms into a multi-layered governance domain that extends beyond physical borders and regulates individuals' behaviors. This situation can cause social integration to evolve into a structure shaped under surveillance and assimilation pressure rather than voluntary participation processes.

AI-supported security applications produce a dual-sided impact on social integration. While these technologies facilitate administrative integration, they can simultaneously limit social harmony through surveillance, classification, and exclusion mechanisms. Therefore, social integration should be evaluated not as a technical output, but as a political process shaped by the interaction between security policies, technological infrastructures, and social relations.

Ethical Debates and Inquiries Regarding the Future

The rise of AI-supported migration security applications has brought along multi-dimensional ethical problems such as human rights, data justice, surveillance society, and governance, not only in terms of technical efficiency. The proliferation of tools such as risk analysis, digital profiling, and automated decision systems means that migrant individuals' lives are guided by algorithmic decisions (Eubanks, 2018). Furthermore, AI-supported systems discussed in the international arena, such as iBorderCtrl, can impair individuals' presumption of innocence and right to a fair trial (Göktepe, 2025).

In the literature, it is argued that algorithmic security systems evaluate individuals within data-based risk categories and that this situation can strengthen exclusionary security practices (Amoore, 2006). The boundaries and potential transformation of artificial intelligence technologies need to be evaluated (Beduschi, 2021). With artificial intelligence playing a greater role in decision-making processes, the applicability of principles such as "explainability," "accountability," and "algorithmic transparency" is seriously debated (Wachter et al., 2017). For example, if the reason why a high-impact decision such as the deportation of an individual was taken cannot be explained, this threatens not only the individual's fundamental rights, but also the rule of law. The General Data Protection Regulation (GDPR) grants individuals the "right to object" against AI-based automated decision processes. However, how this right will function and how it will be supported technologically remains unclear (Veale & Edwards, 2018). Concepts of social participation and democratic legitimacy also hold a critical place in the construction of an ethical future. The involvement of migrants and civil society in the design, implementation, and auditing processes of these systems will be decisive not only in terms of ethical governance, but also for social harmony and peaceful coexistence. Technologies must be structured in a way that serves not only the state's security goals, but also individuals' rights and society's holistic welfare (Crawford & Calo, 2016).

AI-based migration security applications in Türkiye are developed within the framework of the claim to establish a balance between security policies and human rights norms. Biometric data usage, algorithmic classification, and digital surveillance applications bring along significant ethical debates in terms of data privacy, transparency, and accountability. In this framework, the extent to which AI-based migration security systems comply with ethical governance principles becomes one of the main headings of academic and legal debates. Alongside the efficiency provided by technological developments, concepts such as data privacy, explainability, and algorithmic accountability become an inseparable part of migration management. Türkiye's institutional capacity

and legislative infrastructure make the question of how the relationship between security policies and fundamental rights will be balanced more visible.

Conclusion

This study examined the role of AI-supported border technologies in Türkiye's migration management policies within the framework of securitization theory and the digital surveillance approach. As a result of document analysis conducted within the scope of the qualitative research method, it was determined that biometric verification systems, algorithmic risk analysis applications, and cross-border data sharing mechanisms have become increasingly visible in Türkiye's border management. The findings indicate that these technologies undertake significant functions in terms of increasing operational capacity in the fight against irregular migration, accelerating identity verification processes, and supporting border security with digital tools.

The findings obtained within the scope of the research show that AI-supported border technologies can be evaluated as applications contributing to the reshaping of migration management with a data-driven understanding, alongside being tools increasing technical capacity. In this framework, it can be said that biometric verification, algorithmic risk analysis, and data sharing applications support new governance practices associated with securitization processes. Nevertheless, existing findings allow evaluation on the basis of institutional policies and practices rather than directly revealing the impacts of these technologies on migrants' daily life experiences.

The study also demonstrates that the proliferation of digital border technologies brings along legal and ethical debates such as the protection of personal data, algorithmic transparency, accountability, and the protection of fundamental rights. Therefore, adopting a balanced approach between security needs and human rights principles in the development and use of AI-supported applications is of importance.

This research contributes to the literature in three aspects. First, it examines AI-supported border technologies in Türkiye holistically within the framework of securitization theory. Second, it evaluates biometric verification, algorithmic risk analysis, and cross-border data sharing within the same analytical framework. Third, it brings a current perspective to the subject by relating the case of Türkiye to international digital migration governance debates. Nevertheless, the study is limited solely to institutional documents and secondary data sources. In future research, combining qualitative field research to be conducted with migrants, implementing agency representatives, and other stakeholders with quantitative analyses will contribute to a more comprehensive assessment of the social impacts of AI-supported border technologies.



www.turkishstudies.net/economy

Turkish Studies - Economics, Finance, Politics

eISSN: 2667-5625



ANKARA SCIENCE
UNIVERSITY

Yapay Zekâ Destekli Sınır Teknolojileri: Türkiye'nin Dijital Göç Güvenliği

Giriş

Uluslararası göç hareketlerinin artan hacmi ve karmaşıklaşan yapısı, sınır güvenliğini devletlerin ulusal güvenlik politikalarının temel bileşenlerinden biri hâline getirmiştir. Günümüzde göç, insani ve demografik bir olgu olmakla birlikte kamu düzeni, sınır kontrolü, terörle mücadele ve toplumsal istikrarla ilişkili çok boyutlu bir güvenlik meselesi olarak ele alınmaktadır. Özellikle kitlesel zorunlu göç hareketleri, geleneksel sınır yönetimi anlayışının yeniden değerlendirilmesini zorunlu kılmaktadır. Bu çerçevede devletler daha etkin, hızlı ve teknoloji destekli sınır yönetimi modellerine yönelmektedir.

Bu dönüşümün en önemli bileşenlerinden biri yapay zekâ destekli sınır teknolojileridir. Büyük veri analitiği, biyometrik kimlik doğrulama, algoritmik risk analizi ve gerçek zamanlı gözetim sistemleri, düzensiz göç hareketlerinin izlenmesi, risk değerlendirmesi ve sınır güvenliği süreçlerinin yönetilmesinde giderek daha yaygın biçimde kullanılmaktadır. Böylece sınır güvenliği, fiziksel denetim faaliyetleriyle sınırlı olmaktan çıkarak veri odaklı ve dijital teknolojilerle desteklenen bir yönetim alanına dönüşmektedir.

Bu dönüşüm, güvenlik çalışmaları literatüründe önemli kuramsal tartışmaları da beraberinde getirmektedir. Güvenikleştirme kuramı, göçün siyasal söylemler aracılığıyla güvenlik tehdidi olarak inşa edildiğini ileri sürerken (Buzan vd., 1998), gözetim çalışmaları dijital teknolojilerin bireylerin izlenmesi, sınıflandırılması ve yönetilmesindeki rolüne dikkat çekmektedir (Lyon, 2001). Benzer biçimde Foucault'nun (1977) biyopolitika yaklaşımı, modern devletlerin nüfusu kayıt, veri ve gözetim mekanizmaları aracılığıyla yönetmesini açıklamaktadır. Bu kuramsal yaklaşımlar, yapay zekâ destekli sınır teknolojilerinin teknik araçlar olmanın yanında güvenlik politikalarını ve göç yönetişimini dönüştüren sosyo-teknik mekanizmalar olarak değerlendirilmektedir. Molnar'ın (2020) çalışması da sınır bölgelerinde kullanılan dijital teknolojilerin insan hakları ve hesap verebilirlik bakımından ortaya çıkardığı risklere dikkat çekmektedir.

Literatürde yapay zekâ destekli sınır teknolojileri çoğunlukla sınır güvenliğinin etkinliği, düzensiz göçün önlenmesi ve operasyonel kapasitenin artırılması bağlamında incelenmektedir. Buna karşılık, bu teknolojilerin göç yönetimini hangi mekanizmalar aracılığıyla dönüştürdüğü, güvenikleştirme süreçlerini nasıl yeniden şekillendirdiği ve ortaya çıkardığı etik ile hukuki sonuçlar, özellikle Türkiye örneğinde sınırlı düzeyde ele alınmıştır.

Türkiye, jeopolitik konumu ve özellikle Suriye iç savaşı sonrasında karşı karşıya kaldığı yoğun düzensiz göç hareketliliği nedeniyle dijital sınır teknolojilerini en kapsamlı kullanan ülkelerden biri hâline gelmiştir. GöçNet sistemi, biyometrik kimlik doğrulama altyapıları, mobil göç noktaları, insansız hava araçları, termal kameralar ve yapay zekâ destekli analiz sistemleri, sınır yönetiminde dijitalleşmenin temel bileşenlerini oluşturmaktadır. Bu nedenle Türkiye örneği, yapay zekâ destekli sınır teknolojilerinin göç yönetimi, güvenlikleştirme ve dijital gözetim süreçleri üzerindeki etkilerini incelemek açısından önemli bir araştırma alanı sunmaktadır.

Bu araştırma, söz konusu literatür boşluğunu Türkiye örneği üzerinden incelemeyi amaçlamaktadır. Bu çalışmada, Türkiye'de yapay zekâ destekli sınır teknolojilerinin göç yönetimini hangi mekanizmalar üzerinden dönüştürdüğü, bu teknolojilerin güvenlikleştirme sürecini nasıl yeniden ürettiği ve yapay zekâ destekli sınır teknolojilerinin etik, hukuki ve toplumsal sonuçlarının neler olduğu sorularına cevap aranmaktadır.

Araştırmada nitel araştırma yöntemi benimsenmiş, veri toplama tekniği olarak doküman analizinden yararlanılmıştır (Bowen, 2009). Araştırmanın veri setini Türkiye Cumhuriyeti İçişleri Bakanlığı, Göç İdaresi Başkanlığı, Savunma Sanayii Başkanlığı, UNHCR, IOM, FRONTEX ve Europol tarafından 2018–2026 yılları arasında yayımlanan raporlar ile politika belgeleri oluşturmaktadır. Belgeler, araştırmanın amacı doğrultusunda amaçlı örnekleme yöntemiyle seçilmiş; veriler tematik analiz kullanılarak biyometrik denetim ve dijital profillemeye, algoritmik risk analizi ile veri paylaşımı yoluyla sınır ötesi gözetim temaları çerçevesinde değerlendirilmiştir. Çalışmanın yalnızca kurumsal belge ve raporlara dayanması nedeniyle ulaşılan bulgular, göçmenlerin bireysel deneyimlerinden ziyade devlet politikaları ve kurumsal uygulamalar temelinde yorumlanmıştır. Bu bakımdan, yapay zekâ destekli sınır teknolojilerinin göçmenlerin gündelik yaşamı ve sosyal bütünleşme süreçleri üzerindeki etkilerinin saha araştırmalarıyla desteklenmesi, gelecekteki çalışmalar açısından önem taşımaktadır.

Yapay Zekânın Güvenlik Alanındaki Rolü

Yapay zekânın en önemli özelliklerinden biri, büyük hacimli veri kümelerini kısa sürede analiz edebilme kapasitesidir. Bu özellik, güvenlik ve kamu yönetimi alanlarında insan gücüne duyulan ihtiyacı azaltmakta ve karar alma süreçlerini hızlandırmaktadır (Önder, 2020). İnsan bilişsel süreçlerinin teknolojik sistemler aracılığıyla tamamen taklit edilmesi mümkün görünmese de, veri işleme kapasitesindeki gelişmeler yapay zekâ teknolojilerinin kamusal alanlardaki kullanımını giderek yaygınlaştırmaktadır (Gaihre, 2023). Özellikle yüksek hacimli verinin üretildiği sınır güvenliği ve göç yönetimi gibi alanlarda, yapay zekâ sistemleri operasyonel etkinlik açısından önemli avantajlar sunmaktadır.

Yapay zekâ sistemleri, yalnızca veriye hızlı erişim sağlayan teknik araçlar değildir. Bu sistemler, verileri eş zamanlı olarak analiz ederek karar süreçlerini yönlendirme kapasitesine de sahiptir. Algoritmik karar mekanizmaları, mevcut veri setleri içerisinde belirli risk örüntülerini tespit ederek “en uygun” seçeneği önceliklendirmektedir. Ancak bu durum, karar süreçlerinin bütün veriler üzerinden değil, belirli parametreler ve sınıflandırmalar üzerinden yürütülmesine neden olmaktadır (Kokkalis, 2019, s. 310). Algoritmaların hangi verileri öncelikli kabul ettiği, hangi risk kategorilerini esas aldığı ve hangi grupları dışarıda bıraktığı konusu önemli tartışmaları beraberinde getirmektedir. Ayrıca yapay zekâ sistemlerinin etkili biçimde çalışabilmesi, gelişmiş dijital altyapılara, yüksek işlem kapasitesine ve sürekli veri akışına bağlıdır. Bu nedenle yapay zekâ teknolojileri, teknik kapasitenin yanında güçlü bir veri yönetim sistemi de gerektirmektedir.

Yapay zekâ teknolojilerinin göç güvenliği alanındaki kullanımını değerlendirebilmek için, göçün güvenlikleştirilmiş bir olgu hâline geldiğini dikkate almak gerekmektedir. Güvenlikleştirme kuramı, göçün nesnel tehditlerden bağımsız biçimde siyasal söylemler aracılığıyla güvenlik sorunu olarak inşa edildiğini ileri sürmektedir. Buzan, Wæver ve de Wilde'a (1998) göre bir konunun güvenlik meselesi hâline gelmesi, siyasal aktörlerin söylemsel müdahaleleriyle ilişkilidir. Bu çerçevede göçmenler "risk", "tehdit" veya "öteki" kategorileri içerisinde tanımlanabilmekte; olağanüstü güvenlik uygulamaları meşrulaştırılabilmektedir. Yapay zekâ destekli sınır teknolojileri, bu güvenlikleştirme sürecini dijital gözetim mekanizmaları üzerinden yeniden üretmektedir.

Göçün güvenlikleştirilmesi, göçmenlerin idari ve teknolojik denetim mekanizmaları içerisinde sürekli izlenen veri öznelere dönüşmesine yol açmaktadır. Bellanova ve Duez'e (2012, s. 110) göre dijital sınır teknolojileri, teknik tarafsızlık iddiası taşısa da göçmenleri algoritmik risk kategorileri içerisinde değerlendiren sosyo-teknik araçlar üretmektedir. Foucault'nun biyopolitika yaklaşımı bağlamında değerlendirildiğinde, dijital sınır sistemleri nüfusun biyometrik veriler üzerinden yönetilmesini mümkün kılmaktadır (Ajana, 2013, s. 598). Böylece sınır güvenliği, yalnızca fiziksel kontrol süreçlerinden oluşan bir mekanizma olmaktan çıkmakta; veri toplama, sınıflandırma ve dijital gözetim süreçleriyle genişlemektedir.

Bu dönüşüm, sosyal bütünleşme süreçleri üzerinde de önemli etkiler yaratmaktadır. Güvenlik merkezli dijital uygulamalar, göçmenlerin sürekli denetlenen ve risk skorları üzerinden değerlendirilen bireyler hâline gelmesine neden olmaktadır. Amooore'a (2006, s. 338) göre algoritmik güvenlik sistemleri, "riskli" ve "entegre edilebilir" göçmen kategorileri oluşturarak dışlayıcı bir dijital hiyerarşi üretmektedir. Bu durum, göçmenlerin ev sahibi toplumla kurduğu güven ilişkisini zayıflatabilmekte ve dijital ötekileştirme süreçlerini derinleştirebilmektedir. Yapay zekâ sistemleri, göçmenlerin yalnızca fiziksel hareketliliğini değil; dijital izlerini, sosyal ağlarını ve davranış örüntülerini de denetim altına almaktadır (Zuboff, 2019, s. 25).

Yapay zekâ teknolojilerinin göç güvenliği alanındaki kullanımı, teknik bir tercih olmanın ötesinde siyasal ve yönetsel bir dönüşümü ifade etmektedir (Gaihre, 2023, s. 15). Teknoloji ile güvenlik politikaları arasındaki yakın ilişki, göç yönetiminde veri temelli yeni bir denetim rejimi oluşturmaktadır. Bu nedenle yapay zekâ teknolojilerinin sınır güvenliği operasyonlarına entegrasyonu, birçok devlet tarafından stratejik öncelik olarak değerlendirilmektedir (Feldstein, 2019, s. 5). Yüz tanıma sistemleri, biyometrik analiz araçları, hareket sensörleri, termal kameralar ve tarayıcı yazılımlar, çağdaş dijital sınır yönetiminin temel bileşenleri arasında yer almaktadır (Feldstein, 2019, s. 7). Bu sistemler, güvenlik süreçlerini hızlandırmakta ve veri temelli öngörü kapasitesini artırmaktadır (Zuiderwijk, Chen ve Salem, 2021, s. 5).

Yapay zekâ destekli sınır teknolojileri, geniş sınır bölgelerinin daha az personelle izlenmesine olanak sağlamaktadır. Özellikle insansız hava araçları, otomatik analiz sistemleri ve gerçek zamanlı veri işleme mekanizmaları, sınır güvenliği operasyonlarının kapsamını genişletmektedir (Tyler, 2022, s. 6). Bu gelişmeler, göç yönetiminde dijitalleşmenin ve otomasyonun giderek daha merkezi bir konuma yerleştiğini göstermektedir.

Dijital Sınır Güvenliği: Giriş Noktalarında Yapay Zekâ Tabanlı Uygulamalar

Günümüzde sınır güvenliğinin sağlanmasında geleneksel yöntemlerin yetersiz kaldığı durumlarda yapay zekâ (YZ) tabanlı giriş kontrol sistemleri, yeni bir paradigma olarak öne çıkmaktadır. Bu sistemler, yüksek doğruluk oranı, işlem hızı ve otomatik analiz kapasitesi sayesinde göçmen akışının yoğun olduğu bölgelerde kritik rol oynamaktadır. Özellikle düzensiz göç, insan kaçakçılığı ve sınırdan izinsiz geçişler gibi tehditlerin arttığı kriz bölgelerinde, YZ sistemleri güvenliği artırmaktadır. Aynı zamanda göç yönetimi süreçlerinin etkinliğini ve şeffaflığını da yükseltmektedir.

Yapay zekâ, verilen bilgilere dayanarak rasyonel kararlara ulaşarak insan muhakemesini taklit eden bir teknolojidir. AB'nin "Yapay Zekâ Yüksek Düzeyli Uzman Grubu" (HLEG), yapay zekâyı karmaşık bir hedef verilen ve veri toplayan, yorumlayan ve işleyen ve bu verilere dayanarak verilen hedefe ulaşmak için en iyi eyleme karar veren sistemler olarak tanımlamaktadır (Dumbrava, 2021).

Sınır kontrol teknolojilerine ilişkin olarak Gonzalez (2019), "kimlik kartları, plaka okuyucular, yüz tanıma yazılımları, drone gözetimi, video kameralar, hareket sensörleri ve radar sistemleri gibi çeşitli teknolojilerin yeni bir yüksek teknoloji sınırı" oluşturduğuna dikkat çekmektedir. Bu teknolojiler, göçmenlerin yetkililere nasıl görüldüğünü ve hareketlilik ile mekânı nasıl müzakere ettiklerini doğrudan değiştirmektedir. Gonzalez'in (2019) sınırı "lojistik altyapı" olarak ele alması, sınırı yalnızca harita üzerinde bir çizgi değil, farklı coğrafyalara yayılan sınırlandırma pratikleri içinde kurulan dağınık bir aygıt, altyapı ya da ağ olarak değerlendiren yerleşik yaklaşımları genişletmektedir.

Gillespie ve arkadaşları (2018), dijital ve fiziksel hareketliliğin kesişimini "dijital geçit" olarak tanımlamaktadır. Bu bağlamda, Suriyeli mülteciler akıllı telefonları ve ilişkili dijital altyapıları kullanarak yolculuklarını planlamakta, yön bulmakta ve belgelemektedir. Kimi zaman ise denizde hayatta kalabilmek için görünürlüklerini artırmak amacıyla bu araçları kullanmaktadır. Literatürde, dijital teknolojilerin göç süreçlerine ve göçmenlerin içinde bulunduğu kırılgan durumlara etkisine önemli ölçüde odaklanılmaktadır. Böylece hareket hâlindeki bireylerin göç kontrollerinden kaçınmak için dijital teknolojileri hem yön bulma hem de görünmez olma amacıyla kullanmaları ile birlikte, hayati tehlike arz eden durumlarda aktivist gruplar aracılığıyla sağlanan kritik destek arasındaki bağlantılar kurulmaktadır. Bu çerçevede, dijital aktivizm ve dijital aracılı hareketlilikler, sınır kontrolünü görünürde sorgulayan ve zorlayan pratikler içinde bulunmaktadır.

Bu çerçevede, Suriye Krizi gibi uzun soluklu insani krizler, yapay zekâ (YZ) tabanlı uygulamaların sınır güvenliğinde merkezi bir rol oynamasına zemin hazırlamaktadır. Dijital sınır güvenliği, artık sadece geçişlerin izlenmesi değil, aynı zamanda kimlik doğrulama, risk analizi ve davranışsal tahminlerde bulunma gibi çok katmanlı süreçleri içermektedir. Bu çerçevede, YZ tabanlı giriş kontrol sistemleri üç temel başlık altında incelenecektir: (i) biyometrik doğrulama sistemleri, (ii) risk analizi ve otomatik karar sistemleri(iii) gerçek zamanlı izleme ve sınır ötesi veri paylaşımı şeklindedir.

Biyometrik Doğrulama Sistemleri

Günümüz göç yönetimi pratiklerinde, kimlik doğrulama süreçlerinin güvenilirliği ve hızının artırılması stratejik bir öneme sahiptir. Bu doğrultuda, biyometrik kimlik doğrulama sistemleri, göçmenlerin ve sığınmacıların kimlik tespiti ve izlenmesi sürecinde merkezi bir araç olarak konumlanmaktadır. Parmak izi, yüz tanıma, retina taraması ve ses biyometrisi gibi yöntemlerle bireylere ait fiziksel ve davranışsal özellikler dijital ortama aktarılmaktadır. Böylece kişiye özgü ve sahteciliğe kapalı kimlik doğrulama süreçleri mümkün hâle gelmektedir (Maguire, 2009). Biyometrik veriler, kimlik tespitinin yanında dijital profillemeye, risk analizi ve hareket izleme gibi çok boyutlu göç yönetimi faaliyetlerinde de temel veri kaynağı işlevi görmektedir (Ajana, 2013).

Yapay zekâ destekli sınır güvenliği uygulamaları, özellikle biyometrik tanıma teknolojileri ile ön plana çıkmaktadır. Bu sistemler, geleneksel belgelerin sahteciliğe açık yapısını büyük ölçüde bertaraf etmektedir. Sınır geçişlerinde kimlik doğrulama sürecini yüksek doğruluk oranlarıyla otomatikleştirmektedir. Biyometrik doğrulama, bireyin fiziksel ve davranışsal özelliklerine dayalı olarak kimliğinin teyit edilmesini sağlamaktadır (Jain vd. 2000, s. 91). Yapay zekâ algoritmaları, biyometrik verilerin işlenmesinde derin öğrenme ve makine öğrenmesi modellerinden yararlanarak, daha hassas ve hızlı sonuçlar üretmektedir. Yüz tanıma, parmak izi analizi ve ses tanıma gibi

yöntemler, sınır geçişlerinde bireylerin kimlik bilgilerinin doğrulanmasında etkin biçimde kullanılmaktadır (Binhammad vd.,2024).

Özellikle yüz tanıma teknolojileri, yapay sınır ağları kullanılarak geliştirilmiş olup, düşük çözünürlüklü ve kısmen örtülü yüzlerde dahi yüksek doğrulukla çalışabilmektedir. Bu tür sistemler, pasaport bilgileriyle biyometrik verilerin eşleştirilmesi sırasında gerçek zamanlı olarak karar verebilmektedir (Minaee vd., 2023, s. 8650).

Bu noktada makine öğrenimi algoritmaları, göçmenlerin önceki geçiş verilerini analiz ederek şüpheli hareket paternlerini tespit etmekte kullanılmaktadır. Örneğin, AB'nin bazı dış sınırlarında uygulanan "iBorderCtrl" gibi sistemler, kişilerin verdiği yanıtlarda mikromimik analizleri yaparak yalan beyan ihtimalini değerlendirmektedir. "iBorderCtrl" Akıllı Taşınabilir Sınır Kontrol Sistemi'nin kısaltmasıdır (<https://www.iborderctrl.eu/>). Araştırmacılar, AB vatandaşı olmayanların Schengen bölgesine girişini kontrol etmeye yardımcı olmak için yapay zekâ tabanlı bir yalan detektörü geliştirdiler (Dumbrava, 2021)..Her ne kadar bu tür sistemler etik tartışmalara açık olsa da, sahada elde edilen veriler bu uygulamaların güvenlik açısından caydırıcılık sağladığını göstermektedir.

Risk Analizi ve Otomatik Karar Sistemleri

Yapay zekâ destekli sistemler, günümüzde göç güvenliği politikalarının yalnızca destekleyici unsurları değil, aynı zamanda yönlendirici araçları hâline gelmiştir. Özellikle ani ve büyük ölçekli kitlesel göç olaylarında, devletlerin güvenlik ve kamu düzeni açısından hızlı ve isabetli kararlar verebilmesi, büyük veri analitiği ve otomasyon temelli sistemlerin devreye alınmasıyla mümkün olmaktadır (Broussard, 2018). Suriye krizinden etkilenen ülkelerde yaşanan yoğun göç hareketleri, bu teknolojilerin hem sınır kontrolü hem de iç güvenlik alanlarında kullanılması gerekliliğini açıkça ortaya koymaktadır.

Risk analizi, göçmen bireylerin taşıdığı güvenlik tehditlerini ve sosyal kırılganlık düzeylerini önceden tespit etmeye yönelik veri temelli bir değerlendirme sürecidir. Bu süreçte kullanılan yapay zekâ sistemleri; biyometrik tanıma verileri, seyahat geçmişi, sosyal medya paylaşımları ve hatta psikososyal analizler gibi çok yönlü veri kaynaklarını entegre biçimde işlemektedir (Eubanks, 2018). Makine öğrenimi ve doğal dil işleme (NLP) gibi algoritmalarından elde edilen verilerden risk profili oluşturulmaktadır. Örneğin, bireyin geçmişinde silahlı gruplarla temas kurduğuna dair çevrim içi veya saha temelli veriler, otomatik olarak analiz edilerek "yüksek riskli" sınıfına atanmasına neden olabilir. Benzer biçimde, kadın ve çocukların insan ticareti mağduru olma ihtimali de belirli davranış örüntüleri analiz edilerek tahmin edilebilmektedir (O'Neil, 2016).

Bu sistemlerin en yaygın kullanımı, sınır güvenliğinde karşımıza çıkmaktadır. Avrupa Birliği Sınır ve Sahil Güvenliği Ajansı olan Frontex, yüz tanıma sistemleri, dijital pasaport doğrulama teknolojileri ve davranışsal analiz araçları ile desteklenen pilot yapay zekâ uygulamalarını hayata geçirmiştir (Frontex, 2021). Bu sistemler, yolcuların sınır kapılarındaki yüz ifadelerini, göz hareketlerini, stres düzeylerini ve konuşma biçimlerini analiz ederek yalan beyan riskini değerlendirebilmektedir.

Risk analizinin çıktıları, otomatik karar sistemleri aracılığıyla doğrudan güvenlik süreçlerine entegre edilmektedir. Otomatik karar sistemleri, insan müdahalesine gerek duymadan, sistem tarafından hesaplanan risk skorlarına göre bireyler hakkında giriş izni verme, detaylı kontrol uygulama ya da ret kararı oluşturma gibi işlemleri gerçekleştirmektedir (Wachter vd., 2017). Bu tür sistemler zaman kazandırdığı gibi, öznellik ve insan hatasını azaltarak karar süreçlerinde tutarlılığı da artırmaktadır. Ancak bu teknolojilerin etik yönü ciddi biçimde tartışmalıdır. Yapay zekâ sistemleri, eğitildikleri veri setlerine bağımlıdır. Bu verilerde yer alan tarihsel önyargılar, algoritmalar aracılığıyla yeniden üretilme riski taşımaktadır (Eubanks, 2018). Bu durum, bazı

grupların sistematik biçimde ayrımcılığa uğramasına neden olabileceği tartışmasına neden olmaktadır.

Bu nedenle, otomatik karar sistemlerinde açıklanabilir yapay zekâ ilkeleri önem kazanmaktadır. Açıklanabilirlik; bir sistemin neden belirli bir karara vardığını insan kullanıcıların anlayabileceği şekilde sunabilmesi anlamına gelmektedir (Wachter vd., 2017). Özellikle uluslararası hukukta “gerekçeli karar hakkı” bireylerin temel hakları arasında yer aldığından, yapay zekâ temelli kararların da izlenebilir, gerekçelendirilebilir. Aksi hâlde, bireylerin hak arama yolları ciddi biçimde tıkanabilir ve sistemler keyfi uygulamalara açık hâle gelebilmektedir.

Yapay zekâ destekli risk analizi ve otomatik karar sistemleri, göç güvenliğinde yüksek verimlilik ve hız sağlayan, ancak aynı zamanda ciddi etik, hukuki ve toplumsal riskler barındıran sistemlerdir. Bu nedenle bu sistemlerin sadece güvenlik odaklı değil, aynı zamanda insan hakları temelli bir çerçevede geliştirilmesi ve uygulanması büyük önem taşımaktadır.

Otomatik karar sistemleri ve risk profillemeye teknolojileri, operasyonel yükü hafifletmekle birlikte, algoritmik ayrımcılık tartışmalarını beraberinde getirmektedir. Avrupa Birliği'nin sınır ajansı FRONTEX, Türkiye'nin de veri entegrasyonu sağladığı bu dijital ekosistemin barındırdığı tehlikelere resmi raporunda doğrudan dikkat çekmiştir: *"Makine öğrenimi destekli analiz araçları, eğitildikleri veri setlerindeki tarihsel ve yapısal önyargıları yansıtır ve belirli etnik veya demografik grupları orantısız bir biçimde riskli olarak sınıflandırma riski taşımaktadır"* (FRONTEX, 2021, s. 14). Bu kurumsal tespit, Beduschi'nin (2021, s. 585) yapay zekâ sistemlerinin göçmenleri önceden belirlenmiş "şüpheli" kategorilerine hapsederek hukuki güvenceleri aşındırdığı yönündeki akademik teziyle tam bir uyum içermektedir.

Yapay zekâ destekli risk analizi uygulamalarının sınır güvenliği süreçlerinde karar alma mekanizmalarını destekleyen araçlar olarak değerlendirildiğini göstermektedir. Bu sistemler, düzensiz göç hareketlerinin daha hızlı analiz edilmesine ve güvenlik birimlerinin kaynaklarını risk önceliklerine göre yönlendirmesine katkı sağlayabilmektedir. Bununla birlikte, algoritmik değerlendirmelerin hangi veri setleri ve ölçütler temelinde gerçekleştirildiğine ilişkin sınırlı bilgi bulunması, şeffaflık ve hesap verebilirlik açısından bazı tartışmaları da beraberinde getirmektedir. Bu nedenle, algoritmik karar destek sistemlerinin güvenlik gereksinimleri ile temel hak ve özgürlüklerin korunması arasında dengeli bir çerçevede ele alınması önem taşımaktadır.

Gerçek Zamanlı İzleme ve Sınır Ötesi Veri Paylaşımı

Yapay zekâ temelli sınır güvenliği uygulamalarının etkinliği, gerçek zamanlı veri toplama ve analiz mekanizmalarının gelişmesiyle birlikte önemli ölçüde artış göstermiştir (Latonero & Kift, 2018). Özellikle hareketli ve kontrolü zor sınır bölgelerinde, geleneksel yöntemlerle sağlanamayan gözetim kapasitesi, otonom teknolojilerin devreye girmesiyle dijitalleştirilmiş bir kontrol sistemine dönüşmektedir. Bu bağlamda insansız hava araçları (İHA'lar), termal kameralar, yüz tanıma sistemleri, hareket algılayıcılar ve sabit gözetim kulelerinden gelen görsel ve sensörel veriler, gerçek zamanlı olarak yapay zekâ algoritmaları tarafından işlenmektedir (Bellanova, 2017). Bu sistemler, sınır hattında olağandışı hareketlilikleri, örneğin toplu insan geçişlerini, belirli alanlarda sıklaşan hareketi ya da gizlenmeye yönelik davranışları tespit edebilmekte; insan operatörleri bu veriler üzerinden yönlendirmektedir (Leese, 2014).

Gerçek zamanlı izleme uygulamalarının yanında, yapay zekâ temelli sınır güvenliğinin sürdürülebilirliği ve bütüncül etkinliği açısından uluslararası veri paylaşımı büyük önem taşımaktadır. Göçmenlerin yalnızca bir ülkeye değil, birden fazla ülkeye geçiş yapmaları ve sınırlar arası hareketlilik göstermeleri nedeniyle, ülkeler arasında bilgi akışı ve veri eşgüdümü gereklidir. Bu noktada INTERPOL, Europol ve Frontex gibi kuruluşlarla yürütülen iş birlikleri sayesinde, şüpheli bireylerin dijital izleri ülkeler arasında paylaşmakta; çoklu sınır geçiş kayıtları ve olası güvenlik tehditleri ortak veri havuzlarında toplanmaktadır (Bigo et al., 2013). Bu tür platformlar, yalnızca suç

veya terör şüphelisi kişilerin izlenmesini değil; aynı zamanda kayıp göçmenlerin bulunması, insan ticareti mağdurlarının tanımlanması ve mülteci koruma mekanizmalarının iyileştirilmesi gibi insani amaçlara da hizmet etmektedir.

Veri paylaşımı yalnızca teknik bir mesele değil; aynı zamanda siyasal, hukuki ve etik bir süreçtir. Ulus devletlerin veri egemenliği konusundaki hassasiyetleri, sınır ötesi veri transferlerinde ciddi sınırlamalara yol açabilmektedir (Jeandesboz, 2016). Bu nedenle, veri paylaşım sistemlerinin hem ulusal mevzuatlarla hem de Avrupa Genel Veri Koruma Tüzüğü (GDPR) gibi uluslararası normlarla uyumlu olarak yapılandırılması gerekmektedir. Ayrıca, yapay zekâ sistemlerinin kullandığı verilerin doğruluğu, güncelliği ve tarafsızlığı da sistemlerin güvenilirliği açısından hayati önemdedir. Aksi takdirde, yanlış eşleşmeler, haksız yere riskli sınıfa alınan bireyler ve veri ihlalleri gibi sorunlar, bireysel haklar ve uluslararası iş birlikleri açısından ciddi krizler doğurabilir (Wachter vd., 2017).

Gerçek zamanlı izleme teknolojileri ile uluslararası veri paylaşımı mekanizmalarının entegrasyonu, yapay zekâ destekli sınır güvenliği politikalarının teknik etkinliğini ve küresel meşruiyetini pekiştirmektedir (Gordon, 2019). Ancak bu entegrasyon, yalnızca teknik değildir. Aynı zamanda etik, hukuki ve siyasal sorumluluk bilinciyle ele alındığında anlamlı ve sürdürülebilir hâle gelmektedir.

Türkiye'de Yapay Zekâ Destekli Göç Güvenliği

2011 yılında başlayan Suriye iç savaşı, bölgesel düzeyde büyük bir insani kriz yaratmış ve milyonlarca insan yerinden edilmiştir. Bu süreçte Türkiye, coğrafi ve kültürel yakınlığı nedeniyle en fazla Suriyeliyi kabul eden ülke olmuştur. 2026 itibarıyla Türkiye'de Geçici Koruma kapsamında 2.276.997 Suriyeli bulunmaktadır. (Göç İdaresi, 2026). Bu olağanüstü nüfus hareketliliği, Türkiye'nin sınır güvenliği, kayıt sistemleri, toplumsal uyum ve kamu düzeni açısından yeni politika ve uygulamalar geliştirmesini zorunlu kılmıştır. Bu kapsamda yapay zekâ teknolojileri, göç güvenliği süreçlerinin güçlendirilmesi amacıyla öne çıkan araçlardan biri olmuştur.

Türkiye'nin düzensiz göçle mücadele stratejisi, çok katmanlı ve bütüncül bir güvenlik yaklaşımı doğrultusunda beş temel aşama üzerine inşa edilmiştir. Bu stratejik çerçevenin ilk basamağında, göç hareketlerinin kaynağında kontrol altına alınmasına yönelik önlemler yer almaktadır. Bu kapsamda diplomatik girişimler ve sınır ötesi iş birlikleri aracılığıyla göçün itici nedenlerinin azaltılması hedeflenmektedir. İkinci basamak, kara sınırlarının en üst düzeyde korunmasını amaçlamaktadır. Fiziki bariyerler, teknolojik gözetim sistemleri ve entegre sınır yönetimi uygulamaları ile sınır hattında güvenlik kapasitesinin artırılması ön planda tutulmaktadır. Üçüncü basamak ise, ülke içerisinde yasa dışı olarak bulunan düzensiz göçmenlerin tespiti ve insan kaçakçılığına karşı etkin kolluk denetimi yoluyla iç güvenliğin sağlanmasına odaklanmaktadır. Bu bağlamda mobil göç araçları gibi dijital izleme sistemlerinin devreye alınması, saha etkinliğini önemli ölçüde artırmaktadır. Stratejinin dördüncü aşaması, düzensiz işgücü göçüyle mücadeleyi kapsamaktadır. Emek sömürsüne açık hâle gelen göçmenlerin kayıt dışı çalıştırılmasına karşı alınan önlemler, göç politikalarının sosyal boyutuna işaret etmektedir. Beşinci ve son aşama ise, hızlı, sistematik ve insan haklarına uygun biçimde yürütülen sınır dışı süreçlerini kapsamaktadır. Bu mekanizma, düzensiz göçmenlerin kendi ülkelerine dönüşlerinin etkin biçimde sağlanmasını ve geri gönderme merkezlerinin işlevselliğinin artırılmasını hedeflemektedir (Göç İdaresi, Düzensiz Göçle Mücadele). Türkiye'nin bu beş aşamalı stratejisi, göç yönetimini sadece sınır güvenliği perspektifinden değil; aynı zamanda sosyoekonomik, hukuki ve etik boyutlarıyla birlikte ele alan bütüncül bir politika yönelimine işaret etmektedir.

Türkiye'deki uygulamalarda, YZ sistemleri tamamen otomatik kararlar vermemekte, insan denetimiyle birlikte çalışmaktadır. Bu yaklaşım, teknolojik objektiflik ile insani takdir arasında bir denge kurarak, birey haklarının korunmasına katkı sağlamaktadır. Ayrıca, YZ destekli sistemler,

göçmenlerin daha adil ve sistematik bir biçimde değerlendirilmesine olanak tanımakta, böylece mülteci statüsü kazanabilecek kişilerin daha hızlı ve güvenli bir şekilde haklarına erişmesini desteklemektedir. bu çerçevede Türkiye'deki YZ uygulamalarını biyometrik kimlik doğrulama ve dijital profil oluşturma, risk analizi ve otomatik karar sistemleri ve gerçek zamanlı izleme ve sınır ötesi veri paylaşımı şeklinde çalışmamızda inceleyeceğiz.

Biyometrik Kimlik Doğrulama ve Dijital Profil Oluşturma

Türkiye, düzensiz göçün yönetiminde biyometrik doğrulama sistemlerini dijital sınır yönetiminin temel araçlarından biri olarak kullanmaktadır. Parmak izi, yüz tanıma ve iris taraması gibi biyometrik veriler, özellikle Mobil Göç Noktası uygulamaları ve sınır geçiş noktalarında gerçek zamanlı olarak analiz edilmektedir. Böylece kimlik doğrulama, yasal statü kontrolü ve düzensiz göçün tespitine yönelik işlemler hızlandırılmaktadır.

Geçici koruma kapsamındaki Suriyelilerin kayıt süreçlerinde alınan biyometrik veriler, GöçNet sistemi aracılığıyla merkezi olarak yönetilmektedir (Göç İdaresi Başkanlığı, 2021). Bu sistem, kimlik doğrulamanın yanı sıra kamu hizmetlerine ilişkin idari kayıtların bütünlük biçimde yönetilmesini sağlamaktadır. Ayrıca sınır kapılarında kullanılan biyometrik doğrulama sistemleri, ulusal veri tabanlarıyla entegre çalışarak sahte belge kullanımının tespitine ve güvenlik kontrollerinin etkinliğinin artırılmasına katkı sunmaktadır (Frontex, 2021).

Biyometrik sistemlerin yaygınlaşması, operasyonel etkinliği artırırken kişisel verilerin korunması, mahremiyet ve hesap verebilirlik bakımından önemli tartışmaları da beraberinde getirmektedir. Biyometrik verilerin işlenmesinde KVKK kapsamında öngörülen teknik ve idari tedbirlerin uygulanması büyük önem taşımaktadır. Benzer şekilde Wachter vd. (2017), biyometrik sistemlerde meydana gelebilecek hatalı eşleşmelerin bireylerin hak arama süreçlerini zorlaştırabileceğine dikkat çekmektedir. Bu nedenle biyometrik verilerin işlenmesinde güvenlik gereksinimleri ile temel hak ve özgürlüklerin korunması arasında dengeli bir yaklaşımın benimsenmesi gerekmektedir.

İçişleri Bakanlığı verilerine göre 2025 yılı itibarıyla Mobil Göç Noktası araçlarında GöçNet entegrasyonu aracılığıyla 4 milyon 572 bin 712 kimlik kontrolü gerçekleştirilmiştir (İçişleri Bakanlığı, 2025). Bu veriler, biyometrik doğrulama sistemlerinin Türkiye'nin düzensiz göç yönetiminde önemli bir operasyonel kapasiteye ulaştığını göstermektedir. Bununla birlikte UNHCR (2022), biyometrik verilerin işlenmesi süreçlerinde açık rıza, veri güvenliği ve mahremiyet ilkelerinin gözetilmesinin uluslararası koruma rejimi açısından temel bir gereklilik olduğunu vurgulamaktadır.

Elde edilen bulgular, biyometrik doğrulama sistemlerinin kimlik tespitini kolaylaştıran teknik araçların yanında göç yönetiminde veri temelli karar alma süreçlerini destekleyen dijital yönetim mekanizmaları hâline geldiğini göstermektedir. Türkiye örneğinde bu sistemlerin yaygınlaşması, sınır güvenliğinin dijital teknolojilerle daha bütünlük bir yapıya yöneldiğine işaret etmektedir. Güvenikleştirme kuramı açısından değerlendirildiğinde biyometrik teknolojiler, göç yönetiminde dijital gözetim kapasitesini güçlendiren ve risk odaklı sınır yönetimi anlayışını destekleyen araçlar olarak öne çıkmaktadır. Bununla birlikte, bu teknolojilerin göçmenlerin gündelik yaşamı ve sosyal bütünleşme süreçleri üzerindeki etkilerinin ortaya konulabilmesi için saha araştırmalarına dayalı çalışmalara ihtiyaç bulunmaktadır.

Risk Analizi ve Otomatik Karar Sistemleri

Son yıllarda göç yönetimi ve sınır güvenliği politikalarında dijital teknolojilerin artan rolü, devletlerin daha hızlı, etkin ve veri temelli karar alma süreçlerine yönelmelerine imkân tanımaktadır. Türkiye, bu dönüşüm sürecinde önemli bir aktör hâline gelmiş ve yapay zekâ destekli sistemleri göç güvenliği alanına entegre etme konusunda kayda değer ilerlemeler kaydetmiştir. Özellikle risk analizi ve otomatik karar sistemleri sayesinde, düzensiz göçle mücadelede önleyici tedbirlerin

zamanında alınması, kaynakların daha verimli kullanılması ve sınır yönetiminde stratejik kararların desteklenmesi mümkün hâle gelmiştir.

Yapay zekânın en tartışmalı kullanımlarından biri, göçmenlerin güvenlik risklerine göre sınıflandırılmasıdır. Avrupa'da kullanılan bazı algoritmik sistemlerde olduğu gibi, Türkiye'de de belirli davranış kalıpları, seyahat geçmişi, sosyal medya etkileşimi gibi veriler üzerinden risk profili çıkarma çabaları görülmektedir (Frontex, 2022). Resmi olarak bu sistemlerin algoritmik yapısı açıklanmasa da, mülakatlarda yapay zekâ destekli ön analizlerin kullanıldığı, bazı başvuruların bu sistemler tarafından düşük öncelikli ya da riskli olarak sınıflandırıldığına dair bulgular mevcuttur.

Uluslararası literatürde sıkça vurgulanan algoritmik önyargı riskinin Türkiye pratiğindeki yansımaları, özellikle GöçNet ve Mobil Göç Noktaları üzerinden somutlaşma potansiyeli taşımaktadır. Örneğin, Mobil Göç Noktalarının büyükşehirlerde hangi mahallelerde konuşlandırılacağı veya sahada kimlik kontrolü yapılacak kişilerin yapay zekâ destekli risk haritalarına göre belirlenmesi, algoritmaların eğitildiği geçmiş suç veya düzensiz göç verilerindeki sosyo-ekonomik sapmaları yeniden üretebilir.

Avrupa Birliği ülkelerinde olduğu gibi, Türkiye'de de bireylerin dijital izleri, seyahat geçmişi, sınır geçiş girişimleri ve belirli davranış kalıpları gibi çeşitli veriler üzerinden risk profili oluşturulmasına yönelik uygulamalar geliştirilmektedir (Frontex, 2022). Bu sistemler, sınır güvenliğini fiziksel bir müdahale alanı olmaktan çıkarıp, aynı zamanda önleyici ve analiz temelli bir yönetim aracı hâline dönüştürmektedir. İlgili verilerden elde edilen öngörüler sayesinde göç hareketleri daha doğru tahmin edilmekte ve karar süreçleri nesnel temellere dayandırılabilir.

ASELSAN tarafından geliştirilen elektro-optik gözetim sistemleri, insansız hava araçları (İHA) ve hareket algılayıcı radarlarla desteklenen sınır kontrol sistemleri, göçmen hareketlerinin anlık takibini mümkün kılmıştır (ASELSAN, 2021). Bu sistemlerde kullanılan yapay zekâ yazılımları, sınır bölgelerinde tespit edilen nesne ve hareketleri otomatik olarak sınıflandırmaktadır. Sistem tarafından "şüpheli" olarak tanımlanan eylemler için güvenlik birimlerine uyarı gönderilmektedir.

Türkiye'nin bu alandaki uygulamaları, Avrupa Birliği'nin sınır yönetimi ajansı Frontex tarafından da örnek olarak gösterilmiştir. Frontex'in 2022-2032 stratejik risk analiz raporunda, Türkiye'nin sınır güvenliği sistemleri ve erken uyarı mekanizmalarının Avrupa'nın güvenliği açısından büyük önem taşıdığı vurgulanmıştır (Frontex, 2022).

Bu gelişmeler, Türkiye'de göç yönetiminin giderek daha fazla dijitalleşen ve veri temelli bir güvenlik mimarisi içerisinde yeniden yapılandırıldığını göstermektedir. Yapay zekâ destekli sistemler, sınır yönetimi süreçlerinde operasyonel koordinasyonu artırırken, göçmenlerin sınıflandırılması ve izlenmesine dayalı veri temelli denetim mekanizmalarını da derinleştirmektedir. Bu durum, göç yönetiminin fiziksel sınır kontrolüyle sınırlı kalmadığını göstermektedir. Ayrıca dijital gözetim, veri analitiği ve algoritmik değerlendirme süreçleri üzerinden çok katmanlı bir yönetim alanına dönüştüğünü ortaya koymaktadır.

Gerçek Zamanlı İzleme ve Sınır Ötesi Veri Paylaşımı

Türkiye, özellikle 2011 sonrası yoğunlaşan düzensiz göç akınları karşısında sınır güvenliğini güçlendirmek amacıyla hem gerçek zamanlı izleme teknolojilerine yatırım yapmış hem de sınır ötesi iş birliklerini artırmıştır. Bu kapsamda geliştirilen sistemler sayesinde, Türkiye'nin sınır bölgelerinde göçmen hareketlerinin takibi sadece fiziki devriyelerle değil, dijital gözetim ağları ve veri paylaşımı temelli bir yaklaşım ile gerçekleştirilmektedir.

Gerçek zamanlı izleme kapasitesinin temel taşı, Türkiye'nin güney sınırlarında kurulan yüksek teknolojiye sahip elektro-optik gözetim sistemleridir. ASELSAN tarafından geliştirilen bu sistemler; Şanlıurfa, Hatay, Kilis, Gaziantep ve Mardin illerinde sınır birliklerine entegre edilmiş ve

24 saat kesintisiz gözetim sağlayan Dragoneye platformlarıyla desteklenmiştir. Bu platformlar, 20 kilometre menzile içinde insan, araç ve hayvan hareketlerini ayırt edebilmekte, GPS ve dijital pusula desteğiyle hedefin konumunu anlık olarak komuta merkezlerine iletmektedir (ASELSAN, 2021).

Bu sistemlerin etkinliğini artıran bir diğer unsur, görüntü işleme ve yapay zekâ algoritmalarıyla desteklenen veri işleme yeteneğidir. Örneğin, sınıra yaklaşan bir nesnenin insan, hayvan veya araç olup olmadığını ayırt edebilen yapay zekâ destekli sınıflandırma sistemleri, sahadaki güvenlik birimlerine yalnızca görüntü değil; aynı zamanda duruma göre alarm seviyeleri ve müdahale önerileri de iletmektedir. Tüm bu sistemler, Jandarma Entegre Bilgi Sistemi (JABS) ve GöçNet ile eş zamanlı çalışmakta; hareket tespiti, müdahale ve raporlama süreçleri tek bir dijital çatı altında birleştirilmektedir.

Sınır ötesi veri paylaşımı, Türkiye'nin özellikle komşu ülkelerle olan güvenlik iş birlikleri kapsamında gelişmiştir. Türkiye, Irak ve Suriye sınır hattında faaliyet gösteren güvenlik birimleriyle koordinasyon içinde çalışmakta; belirli operasyon bölgelerinde "Müşterek Veri Paylaşım Noktaları" kurarak ortak tehdit verilerini paylaşmaktadır. Bu noktalar, özellikle kaçakçılık ve terörle mücadeleyle yönelik sınır geçiş hareketliliğini izleme amacı taşımaktadır. İHA görüntüleri, hareket sensörü verileri, biyometrik tanımlama sonuçları karşılıklı olarak paylaşılmaktadır.

Türkiye'nin sınır ötesi veri paylaşımı yalnızca bölgesel düzeyle sınırlı kalmamakta, Interpol, Europol, UNHCR ve IOM gibi kurumlarla da çeşitli veri alışverişi protokolleri yürütülmektedir. Bu iş birliği çerçevesinde, Türkiye'den sınır dışı edilen veya yakalanan düzensiz göçmenlere ilişkin kimlik, parmak izi ve biyometrik veriler uluslararası sistemlerle paylaşmakta; bu sayede özellikle göçmen kaçakçılığı ve sınır aşan organize suçlarla mücadele koordineli şekilde yürütülmektedir.

Gerçek zamanlı izleme sistemleri, sınır yönetiminde yalnızca olay sonrası müdahaleyi değil; aynı zamanda veri temelli öngörü ve risk analizine dayalı önleyici güvenlik pratiklerini de mümkün hâle getirmektedir (Kosłowski & Schulzke, 2018).

Ulusal güvenlik mimarisinin sınır ötesi veri paylaşımı ile nasıl küresel bir gözetim ağına dönüştüğü, kurumların güncel operasyonel istatistiklerinde vücut bulmaktadır.

Milyonlarca göçmene ait biyometrik verileri barındıran GöçNet gibi merkezi veri tabanlarının güvenliği, ulusal kritik altyapı güvenliği kapsamında değerlendirilmelidir (Erden, 2026). Sınır aşan siber tehditlere karşı bu veri ağlarının bütünlüğünü korumak yalnızca teknik bir zorunluluk değildir. Aynı zamanda siber caydırıcılık stratejilerinin de temel bir bileşenidir. Veri sızıntılarının veya sistem manipülasyonlarının ulusal güvenliği doğrudan tehdit edebileceği göz önüne alındığında, bu dijital altyapıların ileri düzey şifreleme ve proaktif siber savunma mekanizmalarıyla desteklenmesi son derece kritiktir.

Bulgular, dijital sınır teknolojilerinin ulusal güvenlik uygulamalarını uluslararası veri paylaşımı mekanizmalarıyla daha bütünleşik hâle getirdiğini göstermektedir. Türkiye'nin uluslararası kuruluşlar ve bölgesel iş birliği mekanizmalarıyla yürüttüğü veri paylaşımı uygulamaları, düzensiz göç ve sınır aşan suçlarla mücadelede operasyonel kapasitenin artırılmasına katkı sağlamaktadır. Bununla birlikte, sınır ötesi veri paylaşımının kişisel verilerin korunması, veri güvenliği ve uluslararası hukuki sorumluluklar bakımından dikkatle değerlendirilmesi gereken yönleri bulunmaktadır. Bu çerçevede, dijital sınır yönetişiminin etkinlik ile temel hakların korunması arasında dengeli bir yaklaşım geliştirmesi önem arz etmektedir.

Yapay Zekâ Destekli Güvenlik Yaklaşımları ve Sosyal Bütünleşme

Yapay zekâ destekli göç güvenliği uygulamaları, göçmenlerin yalnızca sınır geçişlerini değil, aynı zamanda ev sahibi toplumla kurdukları ilişkileri de yeniden şekillendirmektedir. Sosyal bütünleşme, bu bağlamda yalnızca ekonomik katılım veya hukuki statü ile sınırlı olmayan; aidiyet, toplumsal kabul ve karşılıklı güven gibi çok boyutlu bir süreçtir (Castles vd., 2014).

Yapay zekâ temelli sistemler, bir yandan göçmenlerin kamu hizmetlerine erişimini düzenleyerek idari entegrasyonu kolaylaştırmaktadır. Biyometrik veri sistemleri ve dijital kayıt mekanizmaları, bireylerin sağlık, eğitim ve sosyal hizmetlere erişimini daha sistematik hale getirmektedir. Ancak bu süreç aynı zamanda göçmenlerin sürekli izlenen veri öznelere dönüşmesine yol açmaktadır. Bu durum, gözetim literatüründe vurgulandığı üzere, bireylerin davranışlarının veri temelli olarak düzenlenmesi anlamına gelmektedir (Lyon, 2001).

Yapay zekâ destekli risk analizi ve profillemeye sistemleri, göçmenleri algoritmik kategorilere ayırarak yeni dışlanma biçimleri üretebilmektedir. Bu tür sınıflandırmalar, veri setlerinde yer alan önyargıların yeniden üretilmesine yol açarak belirli grupların sistematik biçimde dezavantajlı konuma düşmesine neden olabilmektedir (Eubanks, 2018). Bu bağlamda göçmenler, yalnızca fiziksel hareketlilikleri üzerinden değil, aynı zamanda dijital profilleri üzerinden de değerlendirilen bireyler haline gelmektedir. Bu durum, göçmenlerin ev sahibi toplumla kurduğu aidiyet ve güven ilişkilerini de etkileyebilmektedir. Sürekli denetim altında tutulmaya yönelik idari pratiklerin, gözetim literatüründe tartışıldığı üzere, bireylerin kamu kurumlarıyla kurduğu ilişkiyi güvenlik eksenli bir zemine taşıma riski barındırdığı söylenebilir. Özellikle biyometrik kayıt, dijital takip ve algoritmik değerlendirme süreçlerinin yoğun biçimde kullanılması, göçmenlerin toplumsal kabul süreçlerini güvenlik eksenli bir çerçeve içinde deneyimlemelerine neden olabilmektedir. Böylece sosyal bütünleşme, yalnızca hukuki statü veya hizmetlere erişim meselesi olmaktan çıkmakta; aynı zamanda dijital gözetim ile toplumsal aidiyet arasındaki ilişkinin yeniden şekillendiği çok katmanlı bir süreç dönüşmektedir.

Göç yönetimi, fiziksel sınırların ötesine geçen ve bireylerin davranışlarını düzenleyen çok katmanlı bir yönetim alanına dönüşmektedir. Bu durum, sosyal bütünleşmenin gönüllü katılım süreçlerinden ziyade, gözetim ve uyum baskısı altında şekillenen bir yapıya evrilmesine neden olabilmektedir (Abdulahitoğlu vd.2025).

Yapay zekâ destekli güvenlik uygulamaları sosyal bütünleşme üzerinde çift yönlü bir etki üretmektedir. Bu teknolojiler, idari entegrasyonu kolaylaştırırken aynı zamanda gözetim, sınıflandırma ve dışlanma mekanizmaları aracılığıyla toplumsal uyumu sınırlandırabilmektedir. Bu nedenle sosyal bütünleşme, teknik bir çıktı değil; güvenlik politikaları, teknolojik altyapılar ve toplumsal ilişkiler arasındaki etkileşimle şekillenen politik bir süreç olarak değerlendirilmelidir (Koca, 2022).

Etik Tartışmalar ve Geleceğe Dair Sorgulamalar

Yapay zekâ destekli göç güvenliği uygulamalarının yükselişi, sadece teknik verimlilik açısından değil, aynı zamanda insan hakları, veri adaleti, gözetim toplumu ve yönetim gibi çok boyutlu etik sorunları da beraberinde getirmiştir (Hristozov & Shishkov, 2017). Risk analizi, dijital profillemeye ve otomatik karar sistemleri gibi araçların yaygınlaşması, göçmen bireylerin yaşamlarının algoritmik kararlarla yönlendirilmesi anlamına gelmektedir (Eubanks, 2018). Ayrıca, uluslararası alanda tartışılan iBorderCtrl gibi yapay zekâ destekli sistemler, bireylerin masumiyet karinesi ve adil yargılanma haklarını zedeleyebilmektedir (Göktepe, 2025).

Literatürde, algoritmik güvenlik sistemlerinin bireyleri veri temelli risk kategorileri içerisinde değerlendirdiği ve bu durumun dışlayıcı güvenlik pratiklerini güçlendirebildiği ileri sürülmektedir (Amoore, 2006). Yapay zekâ teknolojilerin sınırları ve potansiyel dönüşümünün değerlendirilmesi gerekmektedir (Beduschi, 2021). Yapay zekânın karar alma süreçlerinde daha fazla rol oynamasıyla birlikte, “açıklanabilirlik”, “hesap verebilirlik” ve “algoritmik şeffaflık” gibi ilkelerin uygulanabilirliği ciddi biçimde tartışılmaktadır (Wachter vd., 2017). Örneğin, bir bireyin sınır dışı edilmesi gibi yüksek etkili bir kararın neden alındığı açıklanamıyorsa, bu durum sadece bireyin temel haklarını değil, aynı zamanda hukukun üstünlüğünü de tehdit etmektedir. Avrupa Veri Koruma Tüzüğü (GDPR), yapay zekâ temelli otomatik karar süreçlerine karşı bireylere “itiraz hakkı”

tanımlanmaktadır. Ancak bu hakkın nasıl işleyeceği ve teknolojik olarak nasıl destekleneceği hâlâ netleşmemiştir (Veale ve Edwards, 2018). Etik geleceğin inşasında ayrıca toplumsal katılım ve demokratik meşruiyet kavramları da kritik bir yer tutmaktadır. Göçmenlerin ve sivil toplumun bu sistemlerin tasarımı, uygulanması ve denetlenmesi süreçlerine dâhil edilmesi, sadece etik yönetim açısından değil; aynı zamanda sosyal uyum ve barışçıl birlikte yaşam açısından da belirleyici olacaktır. Teknolojinin yalnızca devletin güvenlik hedeflerine değil, aynı zamanda bireylerin haklarına ve toplumun bütünsel refahına hizmet edecek şekilde yapılandırılması gerekmektedir (Crawford ve Calo, 2016).

Türkiye’de yapay zekâ temelli göç güvenliği uygulamaları, güvenlik politikaları ile insan hakları normları arasında denge kurma iddiası çerçevesinde geliştirilmektedir. Biyometrik veri kullanımı, algoritmik sınıflandırma ve dijital gözetim uygulamaları; veri mahremiyeti, şeffaflık ve hesap verebilirlik açısından önemli etik tartışmaları da beraberinde getirmektedir. Bu çerçevede, yapay zekâ temelli göç güvenliği sistemlerinin etik yönetim ilkeleriyle ne ölçüde uyumlu olduğu, akademik ve hukuki tartışmaların temel başlıklarından biri hâline gelmektedir. Teknolojik gelişmelerin sağladığı verimliliğin yanında, veri gizliliği, açıklanabilirlik ve algoritmik hesap verebilirlik gibi kavramlar da göç yönetiminin ayrılmaz bir parçası hâline gelmektedir. Türkiye’nin kurumsal kapasitesi ve mevzuat altyapısı, güvenlik politikaları ile temel haklar arasındaki ilişkinin nasıl dengeleneceği sorusunu daha görünür hâle getirmektedir.

Sonuç

Bu çalışma, yapay zekâ destekli sınır teknolojilerinin Türkiye’nin göç yönetimi politikalarındaki rolünü güvenlileştirme kuramı ve dijital gözetim yaklaşımı çerçevesinde incelemiştir. Nitel araştırma yöntemi kapsamında gerçekleştirilen doküman analizi sonucunda, biyometrik doğrulama sistemleri, algoritmik risk analizi uygulamaları ve sınır ötesi veri paylaşımı mekanizmalarının Türkiye’nin sınır yönetiminde giderek daha görünür hâle geldiği tespit edilmiştir. Bulgular, söz konusu teknolojilerin düzensiz göçle mücadelede operasyonel kapasitenin artırılması, kimlik doğrulama süreçlerinin hızlandırılması ve sınır güvenliğinin dijital araçlarla desteklenmesi bakımından önemli işlevler üstlendiğine işaret etmektedir.

Araştırma kapsamında elde edilen bulgular, yapay zekâ destekli sınır teknolojilerinin teknik kapasiteyi artıran araçlar olmasının yanında göç yönetiminin veri temelli bir anlayışla yeniden şekillenmesine katkı sağlayan uygulamalar olarak değerlendirilebileceğini göstermektedir. Bu çerçevede biyometrik doğrulama, algoritmik risk analizi ve veri paylaşımı uygulamalarının güvenlileştirme süreçleriyle ilişkili yeni yönetim pratiklerini desteklediği söylenebilir. Bununla birlikte, mevcut bulgular bu teknolojilerin göçmenlerin gündelik yaşam deneyimleri üzerindeki etkilerini doğrudan ortaya koymaktan ziyade, kurumsal politika ve uygulamalar temelinde değerlendirme yapılmasına imkân sağlamaktadır.

Çalışma ayrıca, dijital sınır teknolojilerinin yaygınlaşmasının kişisel verilerin korunması, algoritmik şeffaflık, hesap verebilirlik ve temel hakların korunması gibi hukuki ve etik tartışmaları da beraberinde getirdiğini göstermektedir. Bu nedenle, yapay zekâ destekli uygulamaların geliştirilmesi ve kullanımında güvenlik ihtiyaçları ile insan hakları ilkeleri arasında dengeli bir yaklaşımın benimsenmesi önem taşımaktadır.

Bu araştırma literatüre üç açıdan katkı sunmaktadır. İlk olarak Türkiye’de yapay zekâ destekli sınır teknolojilerini güvenlileştirme kuramı çerçevesinde bütüncül biçimde incelemektedir. İkinci olarak biyometrik doğrulama, algoritmik risk analizi ve sınır ötesi veri paylaşımını aynı analitik çerçevede değerlendirmektedir. Üçüncü olarak Türkiye örneğini uluslararası dijital göç yönetimi tartışmalarıyla ilişkilendirerek konuya güncel bir perspektif kazandırmaktadır. Bununla birlikte, çalışma yalnızca kurumsal belgeler ve ikincil veri kaynaklarıyla sınırlıdır. Gelecek araştırmalarda göçmenler, uygulayıcı kurum temsilcileri ve diğer paydaşlarla gerçekleştirilecek nitel

saha arařtırmaları ile nicel analizlerin birlikte kullanılması, yapay zekâ destekli sınır teknolojilerinin toplumsal etkilerinin daha kapsamlı biçimde değeriendirilmesine katkı sağlayacaktır.

References

- Abdulahitoğlu, A., Güçlüten, Ç., & Tunca, H. Ö. (2025). A multi-criteria decision-making approach to enhancing border security against irregular migration. *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 23(4), 379–396.
- Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25(3), 336–351.
- Ajana, B. (2013). *Governing through biometrics: The biopolitics of identity*. Palgrave Macmillan.
- ASELSAN. (2021). *Sınır güvenlik sistemleri*. <https://www.aselsan.com/tr/haberler/detay/16/sinir-guvenligi>
- Beduschi, A. (2021). International migration management in the age of artificial intelligence. *Migration Studies*, 9(3), 576–596.
- Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, 20(3), 329–347.
- Bellanova, R., & Duez, D. (2012). A different view on the “making” of European security: The EU Passenger Name Record system as a socio-technical assemblage. *European Foreign Affairs Review*, 17(2), 109–124.
- Bigo, D., Carrera, S., Hayes, B., Guild, E., & Jeandesboz, J. (2013). *Mass surveillance of personal data by EU Member States and its compatibility with EU law*. CEPS ve European Parliament.
- Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, 15(2), 245–278.
- Broussard, M. (2018). *Artificial unintelligence: How computers misunderstand the world*. MIT Press.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/qj0902027>
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Castles, S., de Haas, H., & Miller, M. J. (2014). *The age of migration: International population movements in the modern world* (5th ed.). Palgrave Macmillan.
- Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, 538(7625), 311–313. <https://doi.org/10.1038/538311a>.
- Dumbrava, C. (2021). *Artificial intelligence at EU borders: Overview of applications and key issues*. European Parliamentary Research Service. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698792](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792).
- Erden, K. (2026). Türkiye’de göç politikalarının banoptikon çerçevesinde iletişimsel analizi: Göçnet sistemi üzerinden dijital gözetim pratikleri. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 14(1), 764–791. <https://doi.org/10.19145/e-gifder.1851725>
- European Commission. (2020). *A new pact on migration and asylum*. <https://eur-lex.europa.eu>
- European Union Agency for Fundamental Rights (FRA). (2021). *Getting the future right – Artificial intelligence and fundamental rights*. <https://fra.europa.eu>.

- Europol. (2024). *Consolidated annual activity report (CAAR) 2024*. <https://www.europol.europa.eu/publications-events/publications/consolidated-annual-activity-report-caar-2024>.
- Feldstein, S. (2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace. <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>
- Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books.
- Frontex. (2021). *Artificial intelligence-based capabilities for the European Border and Coast Guard: Final report*. European Border and Coast Guard Agency. <https://www.frontex.europa.eu/media-centre/news/news-release/artificial-intelligence-based-capabilities-for-european-border-and-coast-guard-1Dczge>.
- Frontex. (2022). *Strategic risk analysis 2022*. Publications office of the European Union. <https://doi.org/10.2819/76165>
- Gaihre, Shiva Prasad. (2023). *Artificial intelligence and border security in Nepal* [Yüksek lisans tezi]. APF Command and Staff College, Tribhuvan University.
- Gillespie, M., Osseiran, S., & Cheesman, M. (2018). Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social Media + Society*, 4(1), 1-12. <https://doi.org/10.1177/2056305118764440>.
- Gordon, F. (2019). Virginia Eubanks (2018) Automating inequality: How high-tech tools profile, police, and punish the poor. *Law, Technology and Humans*, 1(1), 162-164. <https://doi.org/10.5204/lthj.v1i0.1386>.
- Göç İdaresi Başkanlığı. (2021). *2020 yılı göç raporu*. T.C. İçişleri Bakanlığı. https://www.goc.gov.tr/kurumlar/goc.gov.tr/YillikGocRaporlari/2020-Yili-Goc-Raporu_M.pdf.
- Göç İdaresi Başkanlığı. (2026). *Geçici koruma kapsamındaki Suriyeliler*. <https://www.goc.gov.tr/gecici-koruma5638>
- Göktepe, O. (2025). Yapay zekâ ve ulusal güvenlik: Fırsatlar, tehditler ve stratejik yönelimler. In *Marmara Siyasal Bilimler Kongresi özet bildiri kitabı*.
- Gonzalez, D. (2019). Logistical borderlands: Latinx migrant labor in the information age. *Society and Space Magazine*. <https://www.societyandspace.org/articles/logistical-borderlandslatinx-migrant-labor-in-the-information-age>
- Hristozov, S., & Shishkov, B. (2017). Usability assessment of drone technology with regard to land border security. In *Proceedings of the Seventh International Symposium on Business Modeling and Software Design (BMSD 2017)* (pp. 216–222).
- International Organization for Migration. (2022). *World migration report 2022*. <https://publications.iom.int/books/world-migration-report-2022>.
- Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 90–98.
- Jeandesboz, J. (2016). Smartening border security in the European Union: An associational inquiry. *Security Dialogue*, 47(4), 292–309. <https://doi.org/10.1177/0967010616650226>
- Koca, B. (2022). Bordering processes through the use of technology: The Turkish case. *Journal of Ethnic and Migration Studies*, 48(8), 1909–1926.

- Kokkalis, K. (2019). *Contribution of artificial intelligence to border security* [Master's thesis, Naval Postgraduate School].
- Koslowski, R., & Schulzke, M. (2018). Drones along borders: Border security UAVs in the United States and the European Union. *International Studies Perspectives*, 19(4), 305–324. <https://doi.org/10.1093/isp/eky002>
- Latonero, M., & Kift, P. (2018). On digital passages and borders: Refugees and the new infrastructure for movement and control. *Social Media + Society*, 4(1). <https://doi.org/10.1177/2056305118764432>.
- Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, 45(5), 494–511. <https://doi.org/10.1177/0967010614544204>.
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.
- Maguire, M. (2009). The birth of biometric security. *Anthropology Today*, 25(2), 9–14. <https://doi.org/10.1111/j.1467-8322.2009.00654.x>
- Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. *Artificial Intelligence Review*, 56(8), 8647–8695.
- Molnar, P. (2020). *Technological testing grounds: Migration management experiments and reflections from the ground up*. EDRi & Refugee Law Lab.
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
- Önder, M. (2020). Yapay zekâ: Kavramsal çerçeve. In İ. Demir (Ed.), *Disiplinlerarası politika vizyonu ve stratejiler* (pp. 91–102). Iksad Publishing House.
- Önder, M., & Saygılı, H. (2018). Yapay zekâ ve kamu yönetimine yansımaları. *Türk İdare Dergisi*, 90(487), 629–668.
- T.C. İçişleri Bakanlığı. (2025). *105 mobil göç aracı hizmete alım törenimizi gerçekleştirdik* [Basın açıklaması]. <https://www.icisleri.gov.tr/105-mobil-goc-araci-hizmete-alim-torenimizi-gerceklestirdik>
- Tyler, H. (2022). *The increasing use of artificial intelligence in border zones prompts privacy questions*. Migration Policy Institute. <https://www.migrationpolicy.org/article/artificial-intelligence-border-zones-privacy>
- UNHCR. (2015). *Policy on the protection of personal data of persons of concern to UNHCR*. United Nations High Commissioner for Refugees. <https://www.refworld.org/docid/553661eb4.html>.
- United Nations High Commissioner for Refugees. (2022). *General policy on personal data protection and privacy*. <https://www.unhcr.org/what-we-do/data-and-publications/data-and-statistics/data-protection>.
- UNHCR. (2023). *Syria emergency*. United Nations High Commissioner for Refugees. <https://www.unhcr.org/syria-emergency.html>.
- Veale, M., & Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398–404. <https://doi.org/10.1016/j.clsr.2017.12.002>.

- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3), 101577. <https://doi.org/10.1016/j.giq.2021.101577>

ETHICAL DECLARATIONS**Research and Publication Ethics**

The author(s) declare that this manuscript is an original work prepared in accordance with the principles of scientific research and publication ethics. The manuscript has not been previously published and is not currently under consideration for publication elsewhere. All sources used in the preparation of this study have been properly cited and referenced. The author(s) confirm that the work contains no plagiarism, fabrication, falsification, or manipulation of data. The research findings are presented honestly and transparently in accordance with the principles of academic integrity.

Author Contributions

All authors have significantly contributed to the conception, design, analysis, and preparation of the manuscript. All authors have read and approved the final version of the manuscript and agree to its submission and publication.

Conflict of Interest

The author(s) declare that there is no conflict of interest regarding the publication of this manuscript.

Funding

This research did not receive any specific grant, financial support, or funding from any public, commercial, or non-profit funding agencies.

Artificial Intelligence (AI) Usage Disclosure

During the preparation of this manuscript, artificial intelligence tools may have been used solely for limited purposes such as language editing, translation assistance, and stylistic improvement. Any AI-assisted translations or language corrections were carefully reviewed and verified by the author(s). Artificial intelligence tools were not used to generate the core scientific content, research design, analysis, or scholarly conclusions. All academic responsibility for the content of the manuscript rests entirely with the author(s).

Copyright and Permissions

The author(s) confirm that all necessary permissions for copyrighted materials have been obtained where required and that the manuscript does not violate any intellectual property rights.

Author Approval

All authors confirm that they have read and approved the final version of the manuscript and consent to its submission and publication.

ETİK BEYANLAR**Araştırma ve Yayın Etiği**

Yazar(lar), bu makalenin özgün bir çalışma olduğunu ve bilimsel araştırma ve yayın etiği ilkelerine uygun olarak hazırlandığını beyan eder. Makale daha önce herhangi bir yerde yayımlanmamış olup başka bir dergide değerlendirme sürecinde değildir.

Çalışmada kullanılan tüm kaynaklar akademik kurallara uygun biçimde atıflanmıştır. Yazar(lar), çalışmanın intihal, veri uydurma, veri tahrifi veya manipülasyon içermediğini; araştırma bulgularının bilimsel dürüstlük ilkelerine uygun şekilde sunulduğunu beyan eder.

Yazar Katkısı

Tüm yazarlar çalışmanın tasarlanması, yürütülmesi, analizi ve makalenin hazırlanmasına önemli ölçüde katkı sağlamıştır. Tüm yazarlar makalenin son hâlini okuyup onaylamış ve yayımlanmasını kabul etmiştir.

Çıkar Çatışması

Yazar(lar), bu makalenin yayımlanmasına ilişkin herhangi bir çıkar çatışması bulunmadığını beyan eder.

Finansal Destek

Bu araştırma herhangi bir kamu kurumu, ticari kuruluş veya kâr amacı gütmeyen kuruluş tarafından finansal olarak desteklenmemiştir.

Yapay Zekâ Kullanım Beyanı

Makalenin hazırlanması sürecinde yapay zekâ araçlarından yalnızca dil düzenleme, çeviri desteği ve anlatım iyileştirmesi amacıyla sınırlı ölçüde yararlanılmış olabilir. Yapay zekâ araçları tarafından yapılan çeviri ve dil düzenlemeleri yazar(lar) tarafından dikkatle kontrol edilmiştir. Yapay zekâ araçları çalışmanın bilimsel içeriğinin, araştırma tasarımının, analizlerinin veya akademik sonuçlarının oluşturulmasında kullanılmamıştır. Makalenin içeriğine ilişkin tüm akademik sorumluluk yazar(lar)a aittir.

Telif Hakları ve İzinler

Yazar(lar), telif hakkı gerektiren materyaller kullanılmışsa gerekli izinlerin alındığını ve çalışmanın herhangi bir fikrî mülkiyet hakkını ihlal etmediğini beyan eder.

Yazar Onayı

Tüm yazarlar makalenin son hâlini okuduklarını, onayladıklarını ve yayımlanmasını kabul ettiklerini beyan eder.