Interdisciplinary Studies in Society, Law, and Politics 2026; 5(1): 1-9

ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

# Digital Borders and Virtual Walls: Legal Responses to Online Migration Control

Mariana. Figueiroa[1], Salma. Benyoussef[2*]

[1] Faculty of Law, University of São Paulo, São Paulo, Brazil
[2] Department of Political Science, Hassan II University, Casablanca, Morocco

*** Corresponding author email address**: salma.benyoussef@uh2c.ma

**Received:** 2025-07-22 **Revised:** 2025-12-15 **Accepted:** 2025-12-22 **Published:** 2026-01-01

**ABSTRACT**

This study aims to examine how legal frameworks have responded to the emergence of digital borders and virtual walls in the context of contemporary migration control. This study utilized a scientific narrative review approach combined with a descriptive analysis method to synthesize literature published between 2021 and 2024. Sources included academic journal articles, legal documents, international guidelines, and policy reports focused on algorithmic governance, biometric surveillance, data sharing, and extraterritorial border control. The review analyzed national, regional, and international legal instruments and case law to assess how current legal responses address the challenges posed by digital technologies in migration governance. The study identified four major dimensions of digital migration control: algorithmic decision-making in immigration procedures, biometric and surveillance technologies at borders, data collection and profiling, and virtual geofencing and border externalization. Each dimension introduces legal concerns related to transparency, consent, privacy, due process, and accountability. While some legal responses exist—such as data protection regulations and human rights treaties—they are often fragmented, limited in scope, and inadequately enforced. The findings reveal significant gaps in legal protection, particularly for migrants who are subject to decisions made by opaque digital systems and transnational data infrastructures. Digital technologies have fundamentally reshaped the mechanisms of migration control, yet legal systems have struggled to keep pace with their rapid deployment. Existing frameworks are insufficient to ensure transparency, fairness, and accountability in the digital governance of mobility. A comprehensive and coordinated legal response is urgently needed to safeguard migrants' rights in the digital age.

***Keywords:*** *Digital borders, virtual walls, migration governance, algorithmic decision-making, biometric surveillance, data protection, legal accountability.*

**How to cite this article:**

Figueiroa, M., & Benyoussef, S. (2026). Digital Borders and Virtual Walls: Legal Responses to Online Migration Control. *Interdisciplinary Studies in Society, Law, and Politics, 5*(1), 1-9. https://doi.org/10.61838/kman.isslp.458

## 1. Introduction

In the contemporary era of globalization, the nature of borders has undergone a profound transformation. No longer confined to physical barriers, borders have increasingly become digitized, forming what scholars and practitioners refer to as "digital borders" and "virtual walls." These terms describe a new form of migration governance in which states deploy advanced technologies to extend control beyond their territorial limits. Through tools such as facial recognition software, biometric databases, geofencing applications, and predictive analytics, governments can now monitor and

influence migration flows in real time, often before individuals reach national soil. This phenomenon reflects a paradigm shift in the exercise of sovereign power—one that is not limited by geography but amplified by digital infrastructure.

Digital technologies have become integral to how states manage mobility. For example, facial recognition systems are employed at airports, border checkpoints, and even in refugee camps to verify identity and track movements. Predictive analytics are increasingly used to assess the likelihood that an asylum seeker may be a security threat or violate visa conditions. These systems, often operated through opaque algorithms, can determine who is granted access to legal protection or detained for further scrutiny. The use of blockchain-based digital identification systems for stateless individuals and refugees is also expanding, offering new forms of traceability while simultaneously raising concerns over surveillance and data sovereignty. Technologies that were once peripheral to border control have now become central to the securitization of migration, shifting the locus of power from immigration officers to automated systems.

These developments, while technologically impressive, have outpaced existing legal frameworks, creating a significant regulatory mismatch. The current legal instruments governing migration and asylum, including those found in international human rights law and refugee law, were designed in an analog era. They do not adequately address the complexities introduced by digital decision-making processes, algorithmic profiling, and cross-border data flows. For instance, while the General Data Protection Regulation (GDPR) in the European Union provides some mechanisms for accountability in the use of personal data, it remains limited in its reach outside EU borders and is often insufficient to prevent discriminatory profiling practices embedded within algorithmic systems (Kalantari et al., 2021). Moreover, legal accountability becomes murky when decisions are made by artificial intelligence, especially in contexts where the source code or decision rules are proprietary and shielded from public scrutiny.

In this context, a growing body of literature has begun to interrogate the legal, ethical, and political implications of digital migration control. Scholars have raised concerns about how such technologies may exacerbate existing inequalities, reinforce racial or ethnic biases, and erode fundamental rights such as the right to privacy, due process, and freedom of movement (Dingoyan et al., 2022). Yet, the fragmented nature of these analyses points to the need for a comprehensive synthesis of legal responses to digital borders and virtual walls. While some states have introduced national regulations or oversight bodies to monitor algorithmic governance in public services, these efforts are often reactive and lack coordination at the international level. Furthermore, the use of digital surveillance tools by private companies contracted by states introduces another layer of complexity regarding jurisdiction, accountability, and human rights compliance (Cronin et al., 2024).

The objective of this narrative review is to explore how legal systems have responded to the rise of digital borders and virtual walls as tools for migration control. It seeks to examine existing laws, case law, and international legal instruments to identify both the advancements and the shortcomings in regulating these technologies. The review is not intended to offer a normative judgment on the legitimacy of digital border control itself but rather to highlight the legal tensions and governance gaps that emerge when sovereignty is extended through digital means. In doing so, it aims to contribute to a more informed and nuanced understanding of how law interacts with technology in the evolving landscape of global migration governance.

The significance of this review lies in its potential to inform both legal scholars and policymakers about the pressing need for updated legal frameworks that can respond to the challenges of digital migration control. As the use of artificial intelligence and biometric systems continues to expand, the stakes are high—not only for migrants but for the legitimacy and accountability of legal systems themselves. By focusing on developments between 2021 and 2024, this review captures the most recent advancements and debates in the field, offering a timely intervention into a critical area of legal scholarship.

## 2. Methodology

This scientific narrative review was conducted using a descriptive analysis method, aiming to synthesize the emerging legal responses to the digitization of migration control mechanisms. The study focused on examining

how legal frameworks at both national and international levels have addressed—or failed to address—the use of digital technologies such as algorithmic decision-making, biometric surveillance, predictive analytics, and virtual border management in the governance of migration. Given the complexity and evolving nature of this subject, the narrative review approach allowed for a comprehensive and interpretive synthesis of interdisciplinary literature across legal studies, migration policy, digital rights, and international human rights law.

The source selection process was guided by thematic relevance, publication credibility, and recency, with a focus on works published between 2021 and 2024. Scholarly articles were identified through searches in leading academic databases such as Scopus, Web of Science, and JSTOR, using keyword combinations including "digital borders," "algorithmic migration control," "virtual walls," "AI in asylum procedures," "biometric surveillance and migration," and "legal frameworks for digital migration technologies." In addition to peer-reviewed journal articles, grey literature from reputable legal think tanks, non-governmental organizations, and international bodies was also included. These sources provided insight into contemporary debates and policy developments that are not always reflected in traditional academic publishing. Reports from organizations such as the European Union Agency for Fundamental Rights (FRA), the United Nations High Commissioner for Refugees (UNHCR), Privacy International, and the Electronic Frontier Foundation (EFF) offered important perspectives on legal accountability and rights-based concerns in digital border practices.

In analyzing the collected materials, the study relied on descriptive content analysis to identify key themes, recurring legal issues, and patterns of regulation or regulatory failure across jurisdictions. Special attention was paid to case law and legal instruments that have responded directly or indirectly to the use of digital tools in migration control. Examples include the General Data Protection Regulation (GDPR) in the European Union, the United Nations Guiding Principles on Business and Human Rights, and judgments from the European Court of Human Rights (ECHR) dealing with surveillance and data protection in the migration context. National laws and policies from technologically advanced states—such as Germany, the Netherlands, the United Kingdom, the United States, and Australia—were also analyzed to compare how different legal systems have approached the integration of digital technology into migration governance.

Ultimately, the chosen methodological framework allowed for the articulation of a comprehensive legal narrative that critically maps the evolving intersection between technology and migration control. This approach did not aim to generate quantitative data or statistical generalizations but rather to explore the legal discourse and identify normative challenges, gaps, and future directions within a rapidly transforming field. The emphasis on literature from 2021 to 2024 ensured that the review captured the most recent developments and debates in response to the global acceleration of digital border infrastructures.

## 3. Conceptual and Theoretical Framework

To understand the legal dimensions of digital migration control, it is essential to define the key concepts that structure this inquiry. "Digital borders" refer to technologically mediated practices that extend border enforcement beyond physical checkpoints. These may include data-sharing systems, geofencing applications, and algorithmic screening mechanisms that operate before, during, or after physical travel. In contrast, "virtual walls" symbolize the invisible but powerful barriers created through surveillance infrastructures, digital identity verification, and real-time monitoring. Together, these constructs enable states to control access and mobility without relying solely on territorial boundaries (Xiao et al., 2024).

The term "algorithmic governance" is another crucial concept in this context. It denotes the delegation of decision-making authority to automated systems that rely on algorithms to process vast amounts of data and produce outcomes that affect individuals' legal status, security assessments, or eligibility for services. In migration control, algorithmic governance is used to prioritize visa applicants, flag potential threats, and automate asylum processing. While efficient, these systems often lack transparency and are susceptible to biases inherent in their training data or design (Xue et al., 2023). The increasing reliance on algorithmic tools also shifts the burden of proof to migrants, who may find it

difficult to contest decisions made by "black box" technologies.

Closely related is the notion of "digital sovereignty," which refers to a state's capacity to control data flows, digital infrastructure, and cyber operations within its jurisdiction. In the migration context, digital sovereignty becomes contentious when states exert control over data collected beyond their borders or when private actors, such as technology firms, operate transnationally without clear accountability mechanisms (Lan et al., 2023). Digital sovereignty also raises questions about who owns and controls migrant data, particularly when biometric information is stored in interoperable databases that are accessible by multiple states or institutions.

The theoretical underpinnings of this review are informed by digital surveillance theory, which posits that contemporary governance increasingly relies on the collection, analysis, and categorization of personal data to exert control. This theory highlights how surveillance is not merely a tool of observation but a mechanism of classification and exclusion. In the context of migration, surveillance can reinforce systemic discrimination by associating certain nationalities, ethnicities, or socio-economic profiles with risk, thereby justifying increased scrutiny or denial of entry (Dingoyan et al., 2022). Digital surveillance theory thus provides a critical lens for examining how new technologies reconfigure power relations between states and migrants.

Another relevant theoretical framework is the post-sovereignty model of legal regulation. This model suggests that traditional notions of territorial sovereignty are being transformed by global interdependence and technological integration. In this view, states no longer exercise control solely through physical enforcement but increasingly through networks, data infrastructures, and international cooperation agreements. This transformation has significant implications for migration law, as it challenges the assumption that legal responsibility ends at a state's territorial boundary (Cronin et al., 2024). The post-sovereignty lens allows for a more nuanced understanding of how digital migration control operates across multiple jurisdictions and involves both public and private actors.

Human rights law in the digital age also plays a crucial role in this theoretical landscape. Traditional legal instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) were not designed with digital technologies in mind. Yet, their principles—such as the right to privacy, non-discrimination, and due process—remain foundational. The challenge lies in applying these rights to new technological contexts in ways that uphold their protective intent. Legal scholars have begun to explore how these rights can be reinterpreted or extended to cover algorithmic decision-making, biometric data collection, and transnational data storage (Martirosyan, 2022).

This conceptual and theoretical framework provides the foundation for analyzing the legal responses to digital borders and virtual walls. By drawing on concepts such as algorithmic governance and digital sovereignty, and grounding the analysis in surveillance theory and post-sovereignty legal models, the review engages with the complex and evolving intersection of law, technology, and migration control. These frameworks not only illuminate the mechanisms of digital border enforcement but also expose the legal and ethical dilemmas that arise when technology is used to make life-altering decisions about who belongs and who does not. Through this lens, the review seeks to contribute to a critical understanding of how legal systems can adapt—or fail to adapt—to the realities of digital migration governance.

## 4. Key Dimensions of Digital Migration Control

The rise of digital borders and virtual walls has led to a transformation in how migration is managed, controlled, and restricted through the deployment of advanced technologies. The following thematic areas illustrate the key operational dimensions of digital migration control and their legal implications.

### *4.1. Algorithmic Decision-Making in Immigration Procedures*

One of the most significant innovations in digital migration governance is the use of artificial intelligence (AI) and algorithmic decision-making systems to manage immigration procedures. Governments have increasingly turned to these tools to process large volumes of asylum claims, assess visa eligibility, and determine deportation risks. These systems claim to improve efficiency, objectivity, and speed, yet their

deployment introduces complex legal and ethical challenges.

AI technologies are frequently utilized to automate visa screenings by assessing data points such as travel history, financial status, and biometric records. While ostensibly neutral, such systems often reflect biases embedded in their training datasets or design parameters. For example, the categorization of applicants based on risk profiling can result in the overrepresentation of certain nationalities or ethnic groups in high-risk categories, reproducing existing discriminatory structures under the guise of algorithmic neutrality (Xue et al., 2023). Moreover, in contexts such as asylum adjudication, where human judgment is critical for interpreting complex narratives and trauma, algorithmic systems can undermine the individualized consideration required by international refugee law (Cronin et al., 2024).

Legal concerns related to these technologies revolve around issues of transparency, due process, and the right to non-discrimination. When algorithmic systems make or inform immigration decisions, the reasoning behind these outcomes is often not disclosed to applicants, lawyers, or even decision-makers themselves. This lack of transparency inhibits meaningful appeals and violates procedural justice norms. Without access to the logic or datasets underlying the system's assessments, applicants cannot effectively challenge adverse decisions. In cases where deportation is determined based on algorithmic flags, the consequences may be severe, including the risk of refoulement or separation from family (Dingoyan et al., 2022). The challenge lies in reconciling the efficiency of automation with fundamental legal guarantees such as fairness and accountability.

### *4.2. Biometric and Surveillance Technologies at Borders*

Another prominent feature of digital migration control is the use of biometric and surveillance technologies at international borders and within migrant registration processes. These tools include facial recognition, iris scans, fingerprinting, and predictive surveillance mechanisms that monitor patterns of movement and behavior. These systems are increasingly embedded in border infrastructure and are used not only for identity verification but also for behavior prediction and anomaly detection.

Facial recognition systems, for instance, are widely deployed at airports and border crossings to match travelers' faces against biometric databases. While these systems aim to enhance security and reduce processing time, they raise serious human rights concerns, particularly regarding consent, privacy, and proportionality. The collection of biometric data is often mandatory for migrants, including asylum seekers and refugees, who may have little understanding of or ability to refuse such practices. In such contexts, the power imbalance is acute, and the potential for abuse is high (Chen et al., 2022). Moreover, facial recognition technologies have been found to have higher error rates among non-white populations, which introduces racial bias into an already contentious domain (Xiao et al., 2024).

Predictive surveillance tools that use behavioral analytics to identify suspicious travel patterns or associations can result in preemptive restrictions on movement or unwarranted detentions. These systems often operate without clear legal frameworks or oversight, raising concerns about the proportionality of their use in migration control. The application of such surveillance mechanisms to people who have not committed any wrongdoing—and who are simply attempting to cross borders in search of safety or opportunity—runs counter to the principles of necessity and minimal interference enshrined in human rights law (Sagala et al., 2021).

### *4.3. Data Collection, Sharing, and Digital Profiling*

A central pillar of digital migration governance is the vast amount of data collected, stored, and shared across borders. From biometric identifiers to social media activity, digital footprints are increasingly used to construct migrant profiles that influence access to asylum, visas, and social services. These profiles are stored in interoperable databases such as the European Union's Eurodac and Visa Information System (VIS), which are accessible to multiple agencies and often shared with third countries through bilateral or multilateral agreements (Martirosyan, 2022).

Digital profiling allows for the classification of individuals based on assumed risks or identities, which can lead to discriminatory treatment and exclusion from essential protections. The aggregation of personal data across systems raises serious questions about data

protection, particularly when individuals are unaware of how their information is used or shared. Legal redress mechanisms are limited, especially when data is stored in foreign jurisdictions or processed by private contractors operating across national boundaries (Kalantari et al., 2021).

The right to data protection is enshrined in various international and regional instruments, yet its application in migration contexts remains uneven. Migrants, particularly those without legal status, are often excluded from protections available to citizens or residents. The result is a legal gray zone in which powerful technologies are used to make critical decisions about people's lives without sufficient transparency, consent, or accountability (Du et al., 2022).

### *4.4. Virtual Geofencing and Border Externalization*

One of the most profound shifts in migration control has been the externalization of borders through virtual geofencing technologies. These digital walls allow states to exert control beyond their physical territory by monitoring and influencing migrant movement before individuals even arrive. This is achieved through mobile apps, online visa systems, satellite tracking, and pre-clearance procedures that operate extraterritorially.

Geofencing applications can track the location of asylum seekers and alert authorities when individuals cross predetermined digital boundaries. Satellite surveillance can monitor movements in border regions and maritime routes, allowing states to intercept or divert migrants long before they reach national territory. Additionally, digital platforms are used to process visa applications and conduct interviews remotely, creating virtual barriers that filter applicants based on algorithmic risk assessments (Ren, 2023).

The legal implications of virtual border control are significant. When states enforce migration restrictions extraterritorially, questions arise about the applicability of human rights obligations. Under international law, states are required to uphold certain protections for individuals within their jurisdiction. However, when digital tools are used to influence movement outside territorial borders, it becomes unclear whether jurisdiction—and thus responsibility—applies. This ambiguity creates legal loopholes that undermine accountability and facilitate rights violations without clear mechanisms for recourse (Lan et al., 2023).

Moreover, the reliance on third countries to implement digital border policies—often in exchange for financial aid or development incentives—raises concerns about coercion and the outsourcing of migration control. These practices can entrench structural inequalities and shift the burden of responsibility to states with fewer legal safeguards, thereby exacerbating the vulnerability of migrants.

## 5. Legal Responses and Gaps

As the deployment of digital technologies in migration governance accelerates, legal systems have begun to respond through various frameworks at the international, regional, and national levels. These efforts aim to regulate the collection and use of data, protect individual rights, and ensure accountability. However, significant gaps remain in enforcement, consistency, and jurisdiction.

The European Union's General Data Protection Regulation (GDPR) stands as a prominent example of a legal framework that addresses digital data governance. It establishes clear principles around data minimization, consent, transparency, and the right to access or rectify personal information. For migrants within the EU, the GDPR provides a layer of protection that can be invoked in cases of unjust data processing or profiling (Kalantari et al., 2021). Similarly, the European Convention on Human Rights (ECHR) has been interpreted by the European Court of Human Rights to extend privacy protections in cases of surveillance and data misuse. The International Covenant on Civil and Political Rights (ICCPR) also enshrines the right to privacy, non-discrimination, and due process, which are relevant to digital migration control.

In addition, the UN Guiding Principles on Business and Human Rights recognize the responsibilities of private actors, including tech companies, in upholding human rights. These principles have been invoked in cases where companies provide surveillance infrastructure to states without adequate oversight. At the national level, countries such as Germany, the Netherlands, and Australia have introduced legislation to regulate algorithmic decision-making and biometric data use in public administration. These efforts, while commendable, are often piecemeal and reactive rather than proactive (Chen et al., 2022).

Despite these frameworks, major challenges persist. One key issue is the lack of enforcement mechanisms, particularly when violations occur across borders or involve private actors. Many legal instruments do not have binding consequences or offer only limited access to justice for affected individuals. Additionally, digital rights protections tend to be fragmented and unevenly applied in migration contexts, with migrants often receiving fewer safeguards than citizens (Dingoyan et al., 2022). This creates a hierarchy of rights that runs counter to the universality principle underpinning international human rights law.

Another challenge is the phenomenon of digital statelessness—where individuals are denied legal recognition or access to services due to errors, exclusions, or discriminatory practices within digital systems. Migrants who lack official documentation or whose identities are misrepresented in databases may find themselves excluded from protection or subject to arbitrary detention. This form of exclusion is particularly difficult to contest, as it is embedded in opaque digital infrastructures that are difficult to audit or challenge (Yuan et al., 2022).

Furthermore, the rise of algorithmic and biometric governance has introduced new forms of inequality based on data-driven assessments. Migrants who are flagged as high-risk based on flawed or biased algorithms may face disproportionate scrutiny or denial of rights, with little recourse for appeal or correction. As these systems become more entrenched, there is a growing risk that digital tools will institutionalize exclusion and invisibilize the suffering of those caught within them (Calamlam et al., 2021).

Ultimately, the legal response to digital migration control remains fragmented, inconsistent, and inadequate to meet the scale and complexity of the challenge. A coordinated international effort is needed to develop binding norms, enhance accountability mechanisms, and ensure that digital technologies do not erode the fundamental rights of migrants. Without such action, digital borders and virtual walls will continue to expand unchecked, reinforcing global inequalities under the pretext of efficiency and security.

## 6. Conclusion

The integration of digital technologies into migration governance has led to the emergence of digital borders and virtual walls, fundamentally transforming the ways in which states manage human mobility. These technologies—ranging from algorithmic decision-making systems to biometric surveillance and virtual geofencing—have introduced new forms of border enforcement that operate not only at the territorial periphery but also in digital and extraterritorial spaces. While such innovations have been justified on the grounds of efficiency, security, and data-driven governance, they raise significant legal, ethical, and human rights concerns that have not been adequately addressed by existing legal frameworks.

One of the central issues with digital migration control lies in the lack of transparency and accountability surrounding the use of artificial intelligence in immigration procedures. Algorithms used to evaluate visa applications, asylum claims, and deportation risks often operate as "black boxes," making decisions without human oversight or the ability to contest outcomes. This undermines core principles of due process and legal fairness, particularly when individuals affected by these systems are unable to access the criteria or data used in decision-making. Furthermore, algorithmic tools may perpetuate or even exacerbate existing forms of discrimination, especially when trained on biased datasets or designed without sufficient safeguards.

The use of biometric and surveillance technologies has also expanded rapidly, enabling states to monitor and control individuals' movements through facial recognition, fingerprint scanning, and predictive behavior analysis. These technologies often function without informed consent, particularly in contexts where migrants are required to provide biometric data as a precondition for entry, asylum, or access to services. The collection and storage of such sensitive data pose serious privacy risks and create vulnerabilities for misuse, hacking, or unauthorized data sharing, especially in the absence of robust oversight mechanisms.

Cross-border data sharing and digital profiling further complicate the legal landscape, as information collected in one jurisdiction can be accessed and used by multiple actors across different legal systems. This raises challenges related to jurisdiction, legal redress, and the consistency of rights protections. Migrants may find themselves subjected to decisions made by foreign authorities or private contractors based on data they neither consented to share nor can contest. In such cases,

digital profiling becomes a tool of exclusion, undermining the principle of individual assessment in asylum and immigration procedures.

Virtual geofencing and externalization strategies represent a new frontier in migration control, where states seek to prevent the arrival of migrants through digital means before they ever reach a physical border. These strategies blur the boundaries of jurisdiction and legal responsibility, making it difficult to determine when and where human rights obligations apply. By leveraging technology to enforce migration policy beyond their own borders, states effectively extend their sovereign reach while evading the accountability traditionally associated with territorial jurisdiction.

Despite the growing reliance on digital tools, legal responses remain fragmented and insufficient. While some regional instruments, such as data protection regulations, offer limited protections, they are often inapplicable or ineffective in transnational contexts. National laws may provide some oversight, but they frequently lag behind technological developments and vary significantly in scope and enforcement. As a result, digital migration control has advanced largely in a legal vacuum, where technological innovation outpaces regulatory safeguards.

There is an urgent need for a coherent and comprehensive legal framework that addresses the unique challenges posed by digital borders and virtual walls. This includes establishing clear standards for algorithmic transparency, data protection, human rights compliance, and extraterritorial accountability. Legal mechanisms must be developed to ensure that individuals affected by these technologies have access to remedies and that states and private actors are held accountable for violations. Furthermore, greater international cooperation is needed to harmonize legal standards, prevent jurisdictional loopholes, and ensure that the rights of migrants are not subordinated to the imperatives of technological efficiency or national security.

In conclusion, while digital technologies have introduced new capabilities in managing migration, they have also redefined the relationship between states and individuals in ways that challenge foundational legal principles. The unchecked expansion of digital migration control risks entrenching structural inequalities and eroding rights protections for some of the world's most vulnerable populations. Addressing these challenges requires a deliberate and sustained effort to align technological innovation with legal and ethical standards that prioritize human dignity, accountability, and justice.

## Authors' Contributions

Authors contributed equally to this article.

## Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

## Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

## Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

## Declaration of Interest

The authors report no conflict of interest.

## Funding

According to the authors, this article has no financial support.

## Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

## References

Calamlam, J. M. M., Ferran, F. M., & Macabali, L. G. (2021). Perception on Research Methods Course's Online Environment and Self-Regulated Learning During the COVID-19 Pandemic. *E-Learning and Digital Media*, *19*(1), 93-119. https://doi.org/10.1177/20427530211027722

Chen, L., Yan, J., Zhang, H., Xu, J., & Chen, X. (2022). CircSTAM Inhibits Migration and Invasion of Trophoblast Cells by Regulating miR-148a-5p/PTEN Axis. *Journal of Assisted Reproduction and Genetics*, *40*(1), 201-210. https://doi.org/10.1007/s10815-022-02660-4

Cronin, K., Dally, J., & Neale, C. (2024). Child Migration: Family and Immigration Laws. https://doi.org/10.5040/9781526502230

Dingoyan, D., Metzner, F., Kongur, A., Arslan, Ö., Pust, G. E. A., & Weierstall-Pust, R. (2022). The Impact of Perceived

Discrimination on Cultural Identification, Psychological Stress, Emotion Regulation and Aggressive Tendencies in Individuals With Turkish Migration Background in Germany. *Frontiers in Sociology*, *7*. https://doi.org/10.3389/fsoc.2022.705027

Du, W., Nair, P. R., Johnston, A., Wu, P. H., & Wirtz, D. (2022). Cell Trafficking at the Intersection of the Tumor–Immune Compartments. *Annual Review of Biomedical Engineering*, *24*(1), 275-305. https://doi.org/10.1146/annurev-bioeng-110320-110749

Kalantari, S., Put, A., & Decker, B. D. (2021). Trackers in Your Inbox: Criticizing Current Email Tracking Practices. 156-167. https://doi.org/10.1007/978-3-030-76663-4_9

Lan, L., Cao, H., Zhao, L., Cui, W., & Wang, B. (2023). PTPN12 Down-Regulated by miR-146b-3p Gene Affects the Malignant Progression of Laryngeal Squamous Cell Carcinoma. *Open Medicine*, *18*(1). https://doi.org/10.1515/med-2023-0727

Martirosyan, D. G. (2022). Legal Labor Migration Regulation From Third Countries Under European Union Law. *Scientific Review Series 1 Economics and Law*(1), 121-131. https://doi.org/10.26653/2076-4650-2022-1-09

Ren, Y. (2023). Analysis on the Accounting Problems of Incentive Policies for Online Sales Based on the New Revenue Standard—Taking Bear Electric Appliance Co., Ltd. As an Example. *Accounting Auditing and Finance*, *4*(2). https://doi.org/10.23977/accaf.2023.040205

Sagala, G. H., Hasibuan, A. F., & Suharianto, J. (2021). Readiness to Implement Digital Learning. https://doi.org/10.2991/aebmr.k.210616.050

Xiao, J., Xiao, Q., Luo, T. Y., & Zhong, H. (2024). What Happens After "Nora Leaves Home"? Chinese Female Rural-to-Urban Migrants in the Sex Webcamming Industry. *Feminist Criminology*. https://doi.org/10.1177/15570851241297655

Xue, J., Xu, X., Wu, Y., & Hu, P. (2023). Student Perceptions of the Community of Inquiry Framework and Satisfaction: Examining the Role of Academic Emotion and Self-Regulation in a Structural Model. *Frontiers in Education*, *8*. https://doi.org/10.3389/feduc.2023.1046737

Yuan, D., Chen, J., Hao, Q., Zhang, P., & Chen, Z. (2022). Methyltransferase-Like 3 Aggravates HCC Development via Mediating N6-Methyladenosine of Ubiquitin-Specific Protease 7. *Journal of Oncology*, *2022*, 1-9. https://doi.org/10.1155/2022/6167832