

Research Article

DIGITAL RIGHTS OF LABOUR MIGRANTS IN KAZAKHSTAN: INTERNATIONAL STANDARDS, DIGITAL GOVERNANCE AND REGULATORY SAFEGUARDS

***Madina Abdramanova*, Amanzhol Nurmagambetov Sr.,
Anuar Nurmagambetov Sr. and Aigerim Zhumabayeva***

DOI:

<https://doi.org/10.33327/AJEE-18-9.3-a0001986>

Date of submission: 5 Jan 2026

Date of acceptance: 22 May 2026

Online First Publication: 29 Jun 2026

Last Publication: 05 Aug 2026

Disclaimer:

The authors declare that their opinions and views expressed in this manuscript are free from the influence of any organisations.

Copyright:

© 2026 Madina Abdramanova,
Amanzhol Nurmagambetov Sr.,
Anuar Nurmagambetov Sr.
and Aigerim Zhumabayeva

ABSTRACT

Background: *The digitalisation of migration governance and labour regulation has fundamentally changed the conditions under which labour migrants exercise their rights. In Kazakhstan, migrants increasingly depend on electronic public services, digital identification, biometric verification, interoperable databases, and platform-based labour intermediation. While these technologies may improve administrative efficiency, they also generate new legal risks, including opaque processing of personal and biometric data, excessive data collection, identification errors, digital exclusion, and limited access to effective remedies. These developments require a clearer conceptualisation of the digital rights of labour migrants and a more precise assessment of whether existing legal mechanisms in Kazakhstan are sufficient to protect them.*

Method: *The study employs a doctrinal and comparative legal methodology. It examines the legal content of digital rights of labour migrants through the analysis of international human rights and data protection standards, including Convention 108+, the case law of the European Court of Human Rights, Regulation (EU) 2024/1689 (the EU AI Act), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. These standards are compared with the legislation of the Republic of Kazakhstan in the fields of migration, labour, and personal data protection. The study also employs a risk-oriented analytical framework to identify regulatory gaps related to biometric processing, inter-agency data exchange, automated decision-making, and digital service delivery.*

Results and Conclusions: *The research demonstrates that Kazakhstan's legal framework contains important baseline guarantees but remains fragmented in its approach to digital risks affecting labour migrants. The law does not sufficiently articulate the principles of proportionality, purpose limitation, storage limitation, transparency, and accountability as operative legal standards. It also lacks explicit obligations concerning privacy-by-design, privacy-by-default, and data protection impact assessment for high-risk processing, particularly where biometric data or algorithmically supported decisions are involved. Procedural safeguards are also underdeveloped, particularly regarding the right to information, the correction of inaccurate data, the explanation of adverse digital outcomes, and the effective contestation of decisions.*

The article argues that the digital rights of labour migrants should be understood as a structured set of guarantees that ensure lawful, proportionate, and transparent data processing, non-discriminatory access to digital services, and procedural protections against harmful digital decisions. It proposes strengthening Kazakhstan's legal framework through clearer data protection principles, mandatory impact assessment for high-risk systems, enhanced safeguards for biometric data, and stronger procedural rights in digitally mediated migration governance.

1 INTRODUCTION

In recent years, migration policy and administration in many states, including the Republic of Kazakhstan, have increasingly relied on digital tools, including electronic public services, interagency information systems, biometric identification, online procedures for submitting and tracking applications, and digital employment platforms. This transformation enhances the manageability of migration processes and accelerates service delivery; however, it simultaneously creates new vulnerabilities for labour migrants as a group who are in an asymmetrical position vis-à-vis the state and employers. In practice, these vulnerabilities manifest in risks of non-transparent processing of personal and biometric data, identification errors, restricted access to services due to a lack of digital skills or infrastructure, and more complex access to effective legal remedies when challenging digital decisions.

In this context, the scholarly and normative conceptualisation of the category of “digital rights of labour migrants” is becoming increasingly relevant. Although international human rights instruments do not generally recognise “digital rights of labour migrants” as a standalone legal category, its substance can be derived from a set of fundamental rights and freedoms, including the right to respect for private life and protection against arbitrary interference, the right to equality and non-discrimination, the right to a fair procedure and an effective remedy, and the access to public services and administrative procedures without unjustified or discriminatory barriers. In the digital environment, these guarantees acquire a concrete legal dimension: requirements for the lawfulness and foreseeability of data processing, data minimisation, transparency regarding purposes and retention periods, security safeguards, as well as procedural mechanisms for appealing decisions and correcting errors in digital registers.

For the purposes of this article, the digital rights of labour migrants are understood as a specific set of legal guarantees protecting migrants in digital environments where access to migration status, employment, residence, public services, and remedies is mediated by data processing, digital identification, biometric verification, inter-agency data exchange, and platform-based labour intermediation. Their specificity lies in the fact that labour migrants are not merely data subjects in the abstract; they are persons whose legal status and access to work may depend directly on the accuracy, transparency, and contestability of digital systems. This creates migrant-specific vulnerabilities, including dependence on migration status, cross-border data flows, linguistic and procedural barriers, asymmetry vis-à-vis public authorities and employers, exposure to biometric identification, and reliance on digital labour platforms.

The research problem lies in the fact that the current legislation of Kazakhstan in the fields of migration, labour, and personal data - while providing basic legal frameworks - does not always contain sufficient detail on the principles and procedures necessary to protect migrants in the context of digitalisation. Of particular importance are issues related to the processing of biometric data, interagency data exchange, cross-border data transfers, and the use of automated and algorithmic tools in risk assessment and administrative decision-making. Accordingly, there is a need to compare national regulation with international standards and to develop practice-oriented proposals to strengthen legal protection mechanisms.

The purpose of this article is to identify the content of digital rights for labour migrants and to assess the adequacy of the legal mechanisms for their implementation and protection in the Republic of Kazakhstan, in light of international approaches to data protection and procedural guarantees. To achieve this purpose, the article addresses the following objectives: (1) conceptualising the digital rights of migrants and their key components; (2) analysing the risks associated with the digitalisation of migration procedures; (3) conducting a comparative legal assessment of international data protection standards and

Kazakhstan's national legislation; and (4) formulating proposals for improving legislation and law enforcement practice. The scientific novelty of the study lies in integrating data protection approaches (including risk-based governance and privacy-by-design) into the framework of migration regulation and substantiating the need for procedural safeguards for migrants affected by digital decisions made by the state and platforms.

2 LITERATURE REVIEW

In the early stages of research on digital rights, scholarship in information ethics played a key role. In *The Ethics of Information*, Floridi develops the idea that the informational space ("infosphere") is becoming an autonomous environment of human existence, and therefore traditional ethics and human rights must be rethought in light of the fact that an individual acts not only as a physical but also as an informational subject.¹ The further development of the concept of digital rights is linked to studies of "techno-regulation of law" and the transformation of legal autonomy in the context of "smart" technologies. In "Smart Technologies and the End(s) of Law", Hildebrandt shows how big data processing systems and predictive analytics gradually shift the centre of decision-making from humans to algorithms, undermining the classical guarantees of the rule of law, legal certainty, and procedural fairness.² Within digital citizenship research, digital rights are associated with internet access, digital inclusion, online freedom of expression, and equal participation in digital ecosystems.³ Studies on digital identity and data governance conceptualise digital rights as an individual's capacity to control their own data, protect privacy, and resist unwanted digital practices.⁴ In addition, research on digital surveillance and algorithmic systems highlights the importance of rights to explainability and algorithmic transparency, protection against automated discrimination, and mechanisms for appealing data-driven decisions.⁵

Taken together, this body of research demonstrates that digital rights emerge at the intersection of information ethics, techno-regulation, and digital citizenship, reflecting increasingly complex relationships between individuals, data, and algorithms. This understanding provides a methodological foundation for analysing more specific phenomena arising from the digitalisation of social processes, including the transformation of migration as a domain shaped by digital technologies.

- 1 Luciano Floridi, *The Ethics of Information* (OUP 2013) doi:10.1093/acprof:oso/9780199641321.001.0001.
- 2 Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2016).
- 3 Karen Mossberger, Caroline J Tolbert and Ramona S McNeal, *Digital Citizenship: The Internet, Society, and Participation* (MIT Press 2007) doi:10.7551/mitpress/7428.001.0001.
- 4 Engin Isin and Evelyn Ruppert, *Being Digital Citizens* (Rowman & Littlefield Publishers, 2015).
- 5 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books Ltd 2019).

In contemporary academic and practitioner-oriented literature, “digital migration” is not an established legal or socio-demographic category but rather a broad theoretical construct describing new forms of mobility and transnational connections mediated by digital technologies. Across studies, this phenomenon is articulated through related notions, such as “electronic diaspora,” “cyber-diaspora,” “networked diaspora,” and others, reflecting the diversity of approaches to conceptualising migrants’ digital connectivity and the transformation of traditional migration experiences. Marino, for example, characterises it as “digital togetherness”⁶, while Baldassar et al. describe it as “virtual proximity.”⁷ Leurs and Smets propose viewing digital migration as an analytical framework in which migration processes and digital practices mutually shape one another, generating new channels for communication, social inclusion, and access to services.⁸ In empirical research, Alencar suggests that digital migration can be understood through the everyday digital practices of migrants and refugees, particularly the use of mobile communication, social media, and online platforms to obtain information, maintain transnational ties, and interact with humanitarian and other organisations.⁹ The author shows that the digital environment simultaneously creates new opportunities (access to information, support, and navigation) and produces vulnerabilities related to digital inequality, misinformation, and the risk of digital control. Diminescu introduced the concept of the connected migrant, according to which the migrant is no longer defined primarily by physical distance but by digital connectedness that enables “presence-at-a-distance” and shapes a new form of transnational subjectivity.¹⁰

Thus, in contemporary academic literature, the concept of “digital migration” serves primarily as a flexible theoretical construct that captures the transformation of the migration experience in the wake of digital technologies. Across different studies, this phenomenon is described in diverse ways, including the maintenance of transnational ties, the formation of online identities, participation in networked communities, and the use of digital tools to obtain information and navigate host societies. The existence of multiple related labels, such as electronic, cyber, or networked diasporas, indicates the phenomenon's multidimensional character and the ongoing conceptual search in this field. Taken together,

-
- 6 Sara Marino, ‘Making Space, Making Place: Digital Togetherness and the Redefinition of Migrant Identities Online’ (2016) 1(2) *Social Media + Society* 1, doi:10.1177/2056305115622479.
 - 7 Loretta Baldassar and others, ‘ICT-Based Co-Presence in Transnational Families and Communities: Challenging the Premise of Face-to-Face Proximity in Sustaining Relationships’ (2016) 16 *Global Networks* 133, doi:10.1111/glob.12108.
 - 8 Koen H A Leurs and Kevin Smets, ‘Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe’ (2018) 4(1) *Social Media + Society* 1, doi:10.1177/2056305118764425.
 - 9 Amanda Alencar, ‘Mobile Communication and Refugees: An Analytical Review of Academic Literature’ (2020) 14(8) *Sociology Compass* e12802, doi:10.1111/soc4.12802.
 - 10 Dana Diminescu, ‘The Connected Migrant: An Epistemological Manifesto’ (2008) 47(4) *Social Science Information* 565, doi:10.1177/0539018408096447.

this allows digital migration to be understood as a shift from mobility conceived mainly in physical terms toward an expanded, networked form of presence and interaction, in which digital technologies become an integral part of migration processes and migrants' social life.

As migrants become integrated into digital ecosystems, the analysis of digital migration inevitably raises the need to assess how technologies and regulatory mechanisms safeguard their digital rights and data security while simultaneously generating new risks and constraints. Hoang notes that in the digital era, migration should be facilitated and regulated through effective digital tools to ensure legitimacy and sustainability across migration corridors and within collaborative projects.¹¹ Recent scholarship shows that digital technologies and infrastructures (biometrics, databases, algorithmic control systems) significantly affect migrants' rights by shaping new regimes of inclusion and exclusion. These ideas are articulated most fully in Amelung et al., where technologies are examined as elements of the material politics of citizenship.¹² Similar conclusions regarding the risks of algorithmic discrimination, identification errors, intensified surveillance, and migrants' vulnerability can be found in Pelizza, Pollozek & Passoth, Milan, and others,¹³ as well as in research on the materiality of borders.¹⁴ Taken together, this body of work demonstrates that digital technologies are no longer merely instruments of migration governance; they are key factors shaping migrants' access to rights and services, while also increasing vulnerability to algorithmic control, identification errors, and digital exclusion.

An important contribution to understanding the role of digital technologies in migration is provided by the study by Dekker and Engbersen,¹⁵ which shows that social networks radically transform migration networks, thereby facilitating the migration process itself.

- 11 Lan Anh Hoang, 'Migration Infrastructure, Digital Connectivity and Porous Borders: Vietnamese Migration to Australia' (2025) 31(1) *Population, Space and Place* e2868, doi:10.1002/psp.2868.
- 12 Nina Amelung and others, 'Technologies, Infrastructures and Migrations: Material Citizenship Politics' (2020) 24(5) *Citizenship Studies* 587, doi:10.1080/13621025.2020.1784636.
- 13 Annalisa Pelizza, 'Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-Construction of Individuals and Politics' (2020) 45(2) *Science, Technology, & Human Values* 262, doi:10.1177/0162243919827927; Silvan Pollozek and Jan-Hendrik Passoth, 'Infrastructuring European Migration and Border Control: The Logistics of Registration and Identification at Moria Hotspot' (2019) 37(4) *Environment and Planning D: Society and Space* 606, doi:10.1177/0263775819835819; Stefania Milan, Annalisa Pelizza and Yoren Lausberg, 'Making Migrants Visible to COVID-19 Counting: The Dilemma' (*OpenDemocracy*, 28 April 2020) <<https://www.opendemocracy.net/en/making-migrants-visible-covid-19-counting-dilemma/>> accessed 18 May 2026.
- 14 Francesca Esposito and others, 'Ecology of Sites of Confinement: Everyday Life in a Detention Center for Illegalized Non-Citizens' (2019) 63(1-2) *American Journal of Community Psychology* 190, doi:10.1002/ajcp.12313; Kim Rygiel, 'Bordering Solidarities: Migrant Activism and the Politics of Movement and Camps at Calais' (2011) 15(1) *Citizenship Studies* 1, doi:10.1080/13621025.2011.534911.
- 15 Rianne Dekker and Godfried Engbersen, 'How Social Media Transform Migrant Networks and Facilitate Migration' (2014) 14(4) *Global Networks* 401, doi:10.1111/glob.12040.

The authors identify four mechanisms of influence: maintaining strong family ties, activating weak ties, forming latent networks, and creating channels for obtaining insider, informal information about migration that increases potential migrants' "awareness" and lowers the threshold for relocation. These findings underscore that digital platforms not only accompany migration but also actively generate new forms of mobility, social capital, and migrants' digital agency.

A further contribution to the study of labour migrants' digital rights is offered by the report "Digital Labour Platforms and Migrant Workers", which analyses the impact of platform work on migrants' position in the digital economy.¹⁶ The report shows that digital labour platforms are becoming a key employment space for migrants, while simultaneously expanding access to income and increasing vulnerability. The authors stress that algorithmic systems for task allocation, ratings, and digital profiles create a new structure of labour relations in which migrants face algorithmic opacity, dependence on digital identity, a lack of social protections, and a high risk of discrimination. As a result, digital platforms produce an ambivalent effect: while lowering barriers to labour market entry, they also reproduce structural inequalities and intensify violations of migrants' digital and labour rights.

The study of digital migration has advanced significantly in scholarship addressing the digitalisation of border and migration governance. Among the most important contributions in this field are the analytical reports of the European Union Agency for Fundamental Rights. In its report *Under Watchful Eyes*,¹⁷ the FRA demonstrates that the legal significance of biometrics and large-scale information systems in the fields of asylum, migration, and border control extends far beyond questions of administrative efficiency. Rather, these systems constitute a data processing architecture that directly affects the right to respect for private life, the protection of personal data, non-discrimination, human dignity, and access to effective remedies. Of value is the report's emphasis that the risks arise not only from the mere collection of biometric data, but also from data quality, the accuracy of identification, the conditions governing access to such data, the expansion of the circle of system users, and the growing interoperability between different databases. The FRA stresses that increased interconnectedness of systems enhances not only the speed and completeness of information exchange, but also the likelihood of function creep, that is, the gradual use of data beyond the purposes originally declared, as well as the risks of misidentification, secondary use of information, and weakened control by data subjects themselves. In this way, the digital infrastructure of migration governance is revealed not as a neutral technical mechanism, but as a legal and institutional environment in which decisions concerning status, movement, and access to procedures are increasingly mediated

16 Wouter Zwysen and Agnieszka Piasna, *Digital Labour Platforms and Migrant Workers: Analysing Migrants' Working Conditions and (Over)Representation in Platform Work in Europe* (Working Paper, ETUI 2024) doi:10.2139/ssrn.4798982.

17 European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* (Publications Office of the EU 2018).

through data processing. From this perspective, the digital vulnerability of labour migrants is associated not only with the use of commercial platforms or everyday digital services, but also with their inclusion in state systems of identification, registration, and control, the functioning of which increasingly depends on the realisation and protection of their rights.

Petra Molnar's work has significantly deepened the critical analysis of migration control technologies by showing that the digitalisation of this field does not amount to neutral administrative modernisation, but rather constitutes the institutional entrenchment of an infrastructure of surveillance, classification, and exclusion.¹⁸ Its analytical value lies in shifting attention away from the technical efficiency of such tools and towards their embeddedness in power relations that shape the conditions of identification, categorisation, and assessment of mobile persons. From this perspective, migrants and refugees appear not merely as users of digital services or participants in administrative procedures, but as subjects of technological intervention under conditions of limited transparency, insufficient accountability, and weakened mechanisms of contestability. This applies both to surveillance and identification tools and to systems of risk assessment, prediction, and profiling that can mediate decisions on legal status, access to procedures, and the scope of guarantees. Such an approach makes it possible to conceptualise digital vulnerability as deriving not only from the migrant's social position, but also from the very architecture of digital governance, which is grounded in asymmetries of information and institutional control. In these circumstances, the legal significance lies not only in questions concerning the lawfulness of data processing but also in the ways in which technological systems redistribute power within the administrative process, impede understanding of the logic of decision-making, restrict the effective contestation of such decisions, and thereby reinforce structural inequality.

No less important are the works of Niovi Vavoula,¹⁹ which examine the use of artificial intelligence, automated data processing, algorithmic profiling, and facial recognition technologies at the external borders of the Schengen area. In these studies, such tools are understood not as autonomous technological solutions, but as components of a single infrastructure of interoperable large-scale IT systems. Accordingly, the source of legal risk is associated not only with a particular algorithm or a specific biometric identification procedure, but also with the cumulative effect of a digital ecosystem in which data are successively collected, matched, circulated across systems, and used in procedures of verification, categorisation, and risk assessment. This perspective makes it possible to analyse interferences with migrants' rights not as the result of isolated episodes of unlawful

18 Petra Molnar, 'Surveillance Sovereignty: Migration Management Technologies and the Politics of Privatization' in Idil Atak and Graham Hudson (eds), *Migration, Security, and Resistance: Global and Local Perspectives* (Routledge 2021) 66.

19 Niovi Vavoula, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) 23(4) *European Journal of Migration and Law* 457, doi:10.1163/15718166-12340114.

data processing, but rather as a result of the very architecture of digital mobility governance. In conditions of interconnected registries and automated procedures, the data subject becomes increasingly dependent on opaque logics of information processing, while their ability to understand the grounds for a decision, verify the accuracy of the data used, and obtain an effective review is substantially narrowed. In this sense, the literature on smart borders and algorithmic profiling demonstrates that a migrant's digital vulnerability is shaped not only at the level of individual technological tools, but also at the level of the entire environment of digital border governance, within which mobility is from the outset placed under a regime of heightened surveillance and predictive assessment.

The analysis of the digitalisation of migration governance shows that the category of personal data protection alone does not fully capture the range of legal risks that arise in this context. In this respect, the concept of data justice proves particularly productive, as it enables assessment of digital systems not only in terms of the lawfulness of data processing but also in terms of how they shape regimes of visibility, control, and the unequal distribution of vulnerability. In Linnet Taylor's classic formulation, justice in the digital society is linked not merely to compliance with data-processing requirements but also to the ways in which individuals are represented, classified, and governed through data.²⁰ This is of particular importance in the migration context, where migrants are more frequently subjected to intensive biometric identification, inter-agency data sharing, algorithmic profiling, and digital status verification. A closely related approach can also be found in the works of Razmetaeva, Barabash, and Lukianov,²¹ who emphasise that, in the digital age, the substance of human rights cannot be reduced to the classical guarantees of privacy alone but requires consideration of how technological systems reshape the very structure of access to rights, justice, and effective protection. This makes it possible to demonstrate more precisely that the digital vulnerability of labour migrants is formed not only through discrete violations of personal data protection rules, but within the broader digital infrastructure through which identity, migration status, the right to work, access to services, and the possibility of challenging decisions are established and mediated.

Region-specific scholarship also confirms the relevance of these issues for Kazakhstan and the broader Central Asian context. Recent studies on the digitalisation of labour migration within the EAEU point to the limited effectiveness of existing digital platforms, low user engagement, the absence of unified electronic document management standards, and the lack of a coordinated personal data protection policy.²² Research on digital transformation

20 Linnet Taylor, 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally' (2017) 4(2) *Big Data & Society* 1, doi:10.1177/2053951717736335.

21 Yuliia Razmetaeva, Yurii Barabash and Dmytro Lukianov, 'The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice' (2022) 5(3) *Access to Justice in Eastern Europe* 41, doi:10.33327/AJEE-18-5.3-a000327.

22 Zhanar Kadyrbek and Kalybek Koblandin, 'Digitalisation of Labour Migration within the EAEU Digital Agenda' (2025) 109(1) *International Relations and International Law Journal* 126, doi:10.26577/IRILJ2025109111.

in migration governance in Central Asia similarly emphasises that the impact of digital technologies on migration processes remains underexplored, despite their growing role in regulation and service delivery.²³ Kazakhstani studies on migration policy further show that Kazakhstan is increasingly positioned as a country of reception and transit, particularly for migrants from Central Asia and the CIS,²⁴ while national scholarship on personal data protection stresses that the current legal framework remains general and insufficiently specific with regard to data processing in information systems.²⁵ These regional sources support the article's central argument that international standards should be used not as abstract external models but as comparative tools to address concrete regulatory gaps in Kazakhstan's digital migration governance.

Thus, the existing scholarship shows that digitalisation is transforming migration not only in everyday communication and transnational connectivity but also in governance, identification, and access to rights. Digital technologies function simultaneously as infrastructures of mobility, employment, and communication and as mechanisms of classification, surveillance, and status control. Accordingly, the legal significance of digital migration lies not merely in the emergence of new opportunities for access to work, services, and transnational networks, but also in the production of new forms of vulnerability linked to biometric identification, interoperable databases, algorithmic profiling, platform dependence, and opaque decision-making. Taken together, this literature demonstrates that the digital rights of labour migrants cannot be reduced to questions of privacy or the formal lawfulness of data processing alone. They must also be examined through the broader structure of digital governance in which access to employment, legal status, services, and effective remedies is increasingly mediated by data-driven systems. This, in turn, requires a systematic analysis of technological transparency, contestability, non-discriminatory access to digital infrastructures, and the adequacy of legal safeguards against digital exclusion, structural inequality, and rights-restrictive uses of data.

23 Arsen Maltabarov and Meiram Sarybayev, 'Digital Transformation as a New Stage in Regulating Migration Processes in Central Asia' (2024) 88(1) *Public Administration and Civil Service* 106, doi:10.52123/1994-2370-2024-1164.

24 Leila Delovarova, 'Kazakhstan's Migration Policy: An Overview of the External Vector' (2024) 105(1) *International Relations and International Law Journal* 50, doi:10.26577/IRILJ.2024.v105.i1.05.

25 E Yerbolatov and others, 'Personal Data in the Republic of Kazakhstan: Problems of Ensuring Confidentiality in the Context of Digitalisation' (2020) 79(3) *Bulletin of Innovative Eurasian University* 49, doi:10.37788/2020-3/49-58; Saule Akhmetova, 'Some Aspects of Personal Data Protection Legislation' [2023] *Kazakhstan Law Review* <<https://kazlawreview.kz/nekotorye-aspekty-zakonodatelstva-o-zashhite-personalnyh-dannyh/>> accessed 18 May 2026.

3 METHODOLOGY

The methodological framework of the study combines doctrinal and comparative legal analysis with a risk-oriented assessment of digital migration governance. The research employs the comparative legal method to juxtapose international human rights and data protection standards, including the principles of lawfulness, proportionality, transparency, data minimisation, and purpose limitation, as well as the privacy-by-design/privacy-by-default approach, with the existing legislation of the Republic of Kazakhstan in the areas of migration, labour, and personal data protection. To ensure comparability, the study applies functional comparative analysis: it compares not only the wording of legal norms but also their regulatory function, namely, which risk in digital environments they are intended to prevent and what safeguards they provide for labour migrants.

A key component of the methodology is formal-legal (doctrinal) analysis, which examines the normative structures governing the rights and obligations of data processing actors (operators/database owners, competent authorities, and digital service providers), as well as the legal mechanisms for implementing and protecting migrants' rights within digital processes, including notification, access to data, rectification, restriction/cessation of processing, and the appeal of decisions and actions. In addition, a systems approach is used to consider migration regulation and personal data regulation as interconnected subsystems operating through interagency data exchanges, digital identification, and electronic services.

To identify “bottlenecks” in rights protection, the study incorporates elements of a risk-based approach (legal risk assessment). Specifically, it examines typical risks associated with the digitalisation of migration procedures, including digital exclusion, identification and verification errors, excessive data collection, opacity in interagency data exchange, information security vulnerabilities, and limited access to effective remedies for adverse digital outcomes. The identified risks are then mapped against the presence or absence of specific legal requirements and procedural safeguards in Kazakhstan's national legislation (for example, an obligation to assess the impact of data processing on data subjects' rights, document risk-mitigation measures, ensure accountability, and enable audits).

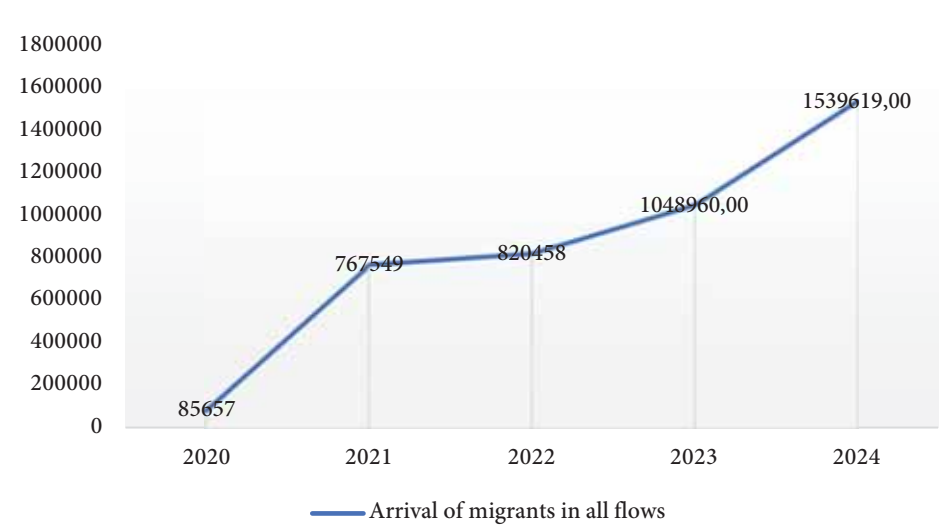
The study's source base consists of publicly available legal, regulatory, and official materials, including legislation, subordinate regulations, official statistical data, policy materials, international standards, and relevant case law. These sources are analysed qualitatively to identify regulatory gaps and formulate normatively grounded proposals to improve Kazakhstan's legal framework.

4 DISCUSSION

4.1. General Analysis of the Migration Situation in Kazakhstan
Based on Statistical Data

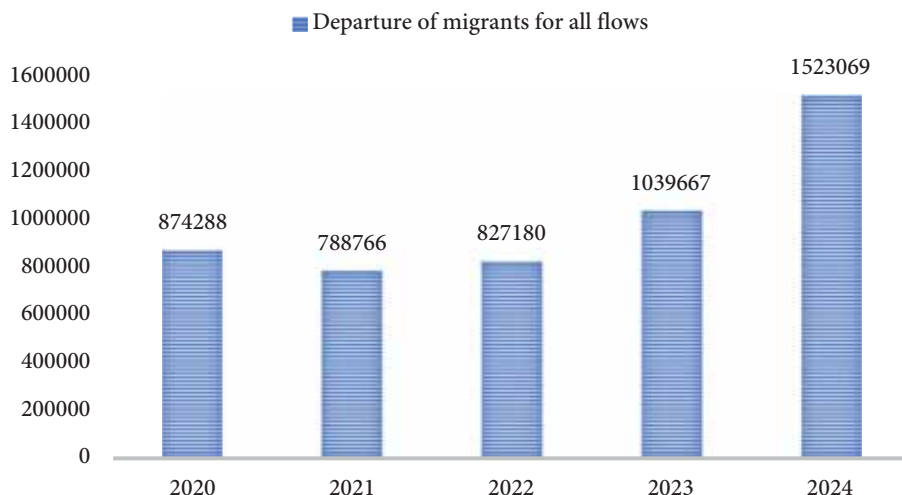
Data presented in Tables 1 and 2, reflecting migrant arrivals and departures across all migration flows in 2020–2024, indicate a substantial increase in the overall volume of migration turnover in Kazakhstan.

Table 1. Arrival of migrants in all flows²⁶



26 Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan, 'Arrival of Migrants in All Flows' (*Information-Analytical System of the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan*, 2025) <<https://taldau.stat.gov.kz/en/NewIndex/GetIndex/703870?regionId=741880&periodId=7>> accessed 18 May 2026.

Table 2. Departure of migrants for all flows²⁷



Over the period under review, arrivals rose from 85,657 persons in 2020 to 1,539,619 persons in 2024. The most significant increase occurred in 2021, when the number of arrivals grew severalfold compared to the previous year, marking a shift to a qualitatively different migration pattern. In the following years, the upward trend persisted: after reaching 767,549 persons in 2021, arrivals increased further to 820,458 in 2022, 1,048,960 in 2023, and 1,539,619 in 2024. This makes it possible to speak of a consistent expansion in the scale of migration mobility and a growing intensity of migration exchange.

Migrant departures over the same period demonstrated a different, yet equally revealing, trend. While in 2020 the number of departures stood at 874,288, it declined to 788,766 in 2021, after which growth resumed: 827,180 in 2022, 1,039,667 in 2023, and 1,523,069 in 2024. Thus, while departures remained quantitatively significant throughout the period under consideration, by its end they had also reached a substantially higher level than at the beginning of the observation period.

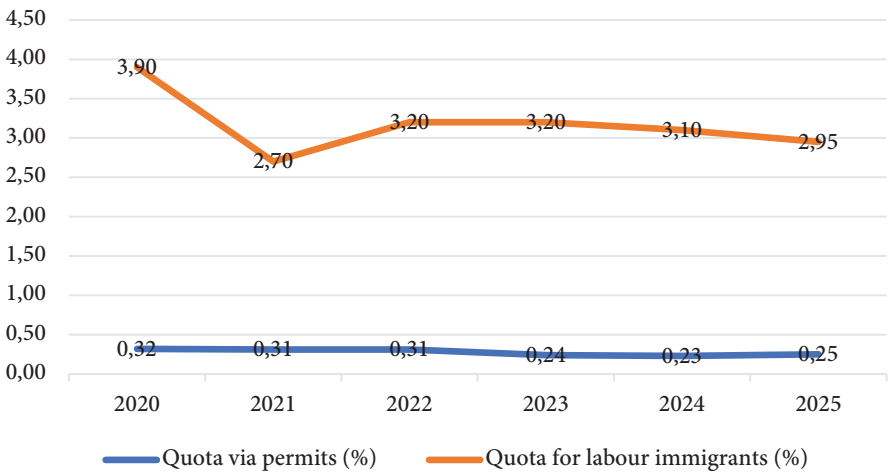
A comparison of arrivals and departures shows that in 2021–2024 migration flows gradually converged in volume. Whereas in 2020 there remained a significant gap between departures and arrivals, beginning in 2021 the scales of both became more proportionate, and in 2023–2024 they virtually reached quantitative equilibrium, with arrivals only slightly exceeding

²⁷ Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan, 'Departure of Migrants for All Flows' (*Information-Analytical System of the Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan*, 2025) <<https://taldau.stat.gov.kz/en/NewIndex/GetIndex/703871>> accessed 18 May 2026.

departures. In 2023, arrivals amounted to 1,048,960 persons, while departures totalled 1,039,667; in 2024, the corresponding figures reached 1,539,619 and 1,523,069, respectively. This trend indicates a high intensity of migration exchange and the growing importance of Kazakhstan as a space of attraction and redistribution of migration flows.

According to the Ministry of Labour and Social Protection of the Population of the Republic of Kazakhstan,²⁸ as of 1 April 2025, 13,891 foreign nationals were employed in Kazakhstan under permits issued by local executive authorities. Compared with 1 December 2024, when Kazakhstan recorded 13,743 such migrants, this change indicates that the quota- and permit-based system operates predictably, ensuring the inflow of labour strictly within labour market needs and avoiding sharp fluctuations in the number of migrants.

Table 3. Dynamics of quotas for attracting foreign labour in Kazakhstan (2020–2025)



Over the period 2020–2025, quotas for attracting foreign labour show a trend of gradual decline. The quota for permits issued by local executive authorities decreased from 0.32% in 2020 to 0.23% in 2024, then increased slightly to 0.25% in 2025. The quota for attracting labour immigrants also fell—from 3.9% in 2020 to 2.95% in 2025—although a short-term increase to 3.2% was observed in 2022–2023. These data reflect a strategic

28 Ministry of Labour and Social Protection of the Population of the Republic of Kazakhstan, ‘Nearly 14 Thousand Foreign Citizens Are Engaged in Labour Activity in Kazakhstan’ (*Official Website of the Government of the Republic of Kazakhstan*, 22 April 2025) <<https://www.gov.kz/memleket/entities/enbek/press/news/details/980686?lang=kk>> accessed 18 May 2026.

policy shift toward more targeted regulation of migration flows and a reduced reliance on foreign labour.²⁹

Taken together, the statistical analysis indicates that the scale and structure of migration flows are changing rapidly, increasing the pressure on the labour migration regulatory system. These trends heighten the importance of digital mechanisms in migration governance, since digital infrastructure is becoming increasingly relevant for access to services, identity verification, migration control, and the protection of labour rights.

At the same time, despite the substantial volume of demographic and economic migration statistics, Kazakhstan does not publish official data capturing the digital dimensions of labour migrants' situation, such as their access to e-government services, levels of digital literacy, use of digital employment platforms, frequency of errors in digital or algorithmic identification, or violations of digital rights.

This gap appears to be linked to the absence of a developed methodology and relevant indicators, the fragmentation of data across different agencies, and the uneven digitalisation of migration procedures. Legislation also does not impose a clear obligation to collect and regularly publish such data, while personal data protection concerns may further limit public disclosure. As a result, government monitoring remains largely focused on general migration indicators and does not fully reflect the digital accessibility of services or the barriers faced by labour migrants in the digital environment. In several jurisdictions, migration governance is increasingly assessed not only through applications and registration procedures, but also through digital traces, platform data, and big-data-based indicators. The absence of such statistics in Kazakhstan makes it more difficult to assess the effectiveness of digital regulatory mechanisms and identify the barriers that migrants face when exercising their rights online. This points to the need to develop a state system for monitoring migrants' digital rights that ensures comprehensive coverage, transparency, and regular publication of relevant data.

4.2. Comparative Analysis of Labour Migrants' Digital Rights and Their Protection in the Context of International and Kazakhstani Legal Regulation

The digitalisation of migration processes, along with states' transition to electronic databases, biometric identification, online employment platforms, and algorithmic decision-making systems, has contributed to the emergence of a new legal category:

29 Orders of the Minister of Labour and Social Protection of the Population of the Republic of Kazakhstan on Establishing Quotas for the Employment of Foreign Labour in the Republic of Kazakhstan for 2020–2025, including Order No 300 of 12 August 2020, Order No 560 of 31 December 2020, Order No 15 of 18 January 2022, Order No 540 of 30 December 2022, Order No 532 of 28 December 2023 and Order No 505 of 30 December 2024.

migrants' digital rights. Although this category has not yet been explicitly enshrined as a standalone concept in universal international treaties, its substance derives from general norms of international human rights law,³⁰ specialised instruments in the field of migration,³¹ data protection and digital privacy standards,³² as well as specific acts regulating digital platforms and artificial intelligence.³³

The International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with a person's privacy and guarantees the right to protection against such interference.³⁴ As clarified by the UN Human Rights Committee,³⁵ the protection under Article 17 of the ICCPR extends to the collection, storage, use, and disclosure of information about an individual's private life by both public and private actors—an understanding that, in contemporary doctrine, encompasses the processing of migrants' digital and biometric data. Similar fundamental guarantees are set out in the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, including the right to privacy, protection against arbitrary interference with private life by public authorities, and procedural safeguards, including access to information.³⁶ Notably, the Republic of Kazakhstan has not ratified this Convention to date.

30 Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) <<https://www.un.org/en/about-us/universal-declaration-of-human-rights>> accessed 18 May 2026; International Covenant on Civil and Political Rights (adopted 16 December 1966) [1983] UNTS 999/171.

31 Global Compact for Safe, Orderly and Regular Migration (adopted 19 December 2018 UNGA Res 73/195) UN Doc A/RES/73/19; Convention (No 97) Concerning Migration for Employment (Revised 1949) (adopted 1 July 1949) [1952] UNTS 120/71; *Convention (No 143) Concerning Migrations in Abusive Conditions and the Promotion of Equality of Opportunity and Treatment of Migrant Workers* (adopted 24 June 1975) [1978] UNTS 1120/323 *etc.*

32 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 28 January 1981) [1981] ETS 108; Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 10 October 2018) [2018] CETS 223; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

33 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L 2024/1689.

34 International Covenant on Civil and Political Rights (adopted 16 December 1966) [1983] UNTS 999/171, art 17.

35 UN Human Rights Committee, *General Comment No 16: Article 17, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (UN Doc HRI/GEN/1/Rev.1, 8 April 1988).

36 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (adopted 18 December 1990 UNGA Res 45/158) [2004] UNTS 2220/3, Arts. 14, 16 and 18.

Overall, the above fundamental rights and freedoms are enshrined in Kazakhstan's legal framework, including the Constitution of the Republic of Kazakhstan³⁷ and the laws of the Republic of Kazakhstan on the Legal Status of Foreigners,³⁸ on Population Migration,³⁹ and On Personal Data and Their Protection.⁴⁰

More narrowly tailored, specialised provisions on the protection of personal and biometric data can be found in several regional and sector-specific international instruments.

The Council of Europe Convention 108+⁴¹ establishes core data protection principles, including proportionality and fair balance (Art. 5(1)); explicit, specific and informed consent (Art. 5(2)); data minimisation, purpose limitation, accuracy, and storage limitation (Art. 5(4)); and privacy-by-design / privacy-by-default, i.e., an obligation to take risks into account when designing systems (Art. 10(2–3)). By contrast, the Law of the Republic of Kazakhstan “On Personal Data and Their Protection” is limited to the following principles: (1) observance of the constitutional rights and freedoms of the individual and citizen; (2) lawfulness; (3) confidentiality of personal data with restricted access; (4) equality of rights of data subjects, owners, and operators; and (5) ensuring the security of the individual, society, and the state. These principles are general and declaratory in nature and do not articulate either the principle of proportionality, requirements for the quality of consent, or a risk-based approach. At the same time, many of the Convention 108+ “substantive” principles are already dispersed throughout Kazakhstani law as technical rules. For example, only “necessary and sufficient” data may be collected (an element of data minimisation), and retention periods are linked to the achievement of the stated purpose of processing, after which the data must be destroyed; processing is permitted only for previously declared purposes, and any departure from those purposes requires consent; and the law provides for the rectification, blocking, and destruction of data where processing is carried out in violation of legal requirements. However, these requirements are not formulated as autonomous principles that courts and supervisory authorities can use as interpretive standards to assess the permissibility of interference.

Thus, in *S. and Marper v. the United Kingdom*,⁴² the European Court of Human Rights held that the indefinite retention of DNA profiles and fingerprints of persons not

37 Constitution of the Republic of Kazakhstan (adopted 30 August 1995) Art. 18 <<https://www.parlam.kz/en/Home/OpenFile?speechId=&culture=en&npld=1>> accessed 18 May 2026.

38 Law of the Republic of Kazakhstan No 2337 ‘On the Legal Status of Foreigners’ (adopted 19 June 1995) Art. 9 <https://adilet.zan.kz/eng/docs/U950002337_> accessed 18 May 2026.

39 Law of the Republic of Kazakhstan No 477-IV ‘On Population Migration’ (adopted 22 July 2011) <<https://adilet.zan.kz/eng/docs/Z1100000477>> accessed 18 May 2026.

40 Law of the Republic of Kazakhstan No 94-V ‘On Personal Data and Their Protection’ (adopted 21 May 2013) <<https://adilet.zan.kz/eng/docs/Z1300000094>> accessed 18 May 2026.

41 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 32).

42 *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008) <<https://hudoc.echr.coe.int/fre?i=001-90051>> accessed 18 May 2026.

convicted of a crime violated Article 8 of the European Convention on Human Rights, precisely because such interference was disproportionate to the aim of combating crime: it was “blanket and indiscriminate” and failed to take into account either the seriousness of the offence or the necessity of continued data retention. In other words, the principles of proportionality and fair balance operate in practice as concrete assessment criteria for information systems (e.g., police DNA databases, mass interception systems, and large-scale state databases), rather than as abstract declarations.

The proportionality test developed in *S. and Marper v. the United Kingdom* may be applied to Kazakhstan’s biometric migration system, particularly to mandatory dactyloscopic registration of foreigners and stateless persons. In Kazakhstan, dactyloscopic information is used for personal identification and is collected from foreigners and stateless persons in cases such as obtaining temporary or permanent residence permits, residence documents, refugee-related documents, visas, as well as in expulsion and readmission procedures. This makes it a concrete example of biometric processing in migration governance.

Such processing may pursue legitimate aims, including identity verification, migration control, public security, and prevention of unlawful stay or document fraud. However, under the proportionality test, a legitimate aim is not sufficient. The legal framework should clearly define the purpose of processing, the categories of biometric data collected, retention periods, authorities authorised to access the data, grounds for inter-agency transfer, and remedies for correcting inaccurate records. Without these safeguards, biometric registration may create risks of excessive retention, secondary use, misidentification, and disproportionate interference with migrants’ private lives.

Therefore, *S. and Marper* is relevant not only as a case on biometric data retention but as a doctrinal basis for requiring clearer safeguards in Kazakhstan’s digital migration infrastructure.

Convention 108+ treats consent as an independent substantive safeguard: processing is permitted either on the basis of “free, specific, informed and unambiguous consent” or on another lawful ground. In Kazakhstani legislation, consent is regulated primarily in procedural terms (written/electronic form, the possibility of withdrawal, including via the e-government platform and SMS code verification), but it does not clarify that consent must be freely given (without coercion or being imposed as a condition for a service where it is not objectively necessary), specific (linked to clearly defined purposes), informed, and unambiguous. In practice, this leads to operators “embedding” consent into a general contract or user agreement, while courts tend to verify mainly the formal existence of a signature/checkbox rather than the data subject’s genuine awareness and freedom of choice, as evidenced by law enforcement and judicial practice.⁴³

43 ‘Review of Judicial Practice on Personal Data in Kazakhstan’ (*Revera Kazakhstan*, 6 March 2025) <<https://kazakhstan.revera.legal/en/info-centr/news-and-analytical-materials/229-obzor-sudebnoj-praktiki-po-personalnym-dannym-v-kazaxstane/>> accessed 18 May 2026.

Article 10 of Convention 108+ requires controllers, prior to commencing processing, to assess the likely impact on data subjects' rights and freedoms and to ensure that systems and processes are designed with data protection requirements embedded at all stages of processing.⁴⁴ In Kazakhstan's national legislation, there is an obligation to adopt "necessary organisational and technical measures" (Article 25) to protect data and prevent unauthorised access, as well as general duties to ensure the integrity, confidentiality, and destruction of data once the purpose of processing has been achieved.⁴⁵ It should be noted that Kazakhstan has experienced instances of major data leaks involving databases held by both public and private operators, including the Central Election Commission, Kazpost, and Yandex.Eda, Sportmaster, and others. Recent amendments introduced in 2023–2024 additionally incorporated the concept of a "personal data security breach," established a duty to notify the competent authority of breaches, prohibited the collection and storage of paper copies of identity documents, and empowered the competent authority to conduct unscheduled inspections and to apply a 33-item checklist of data processing requirements. However, the Law "On Personal Data and Their Protection" still does not impose a general obligation to carry out an *ex ante* impact assessment for high-risk processing (such as biometrics, large state registers, scoring and profiling systems, and algorithmic decision-making), nor does it include a "privacy-by-default" principle requiring, by default, the minimisation of the data collected, retention periods, and the scope of access.

It should be clarified, however, that Convention 108+ is not directly binding on Kazakhstan, since Kazakhstan is not a party to this instrument. Therefore, the relevance of Convention 108+ for the present study is not based on its direct applicability, but on its value as a comparative and normative benchmark for assessing the adequacy of national data protection rules. This distinction is important: the article does not suggest a mechanical legal transplant of Convention 108+ into Kazakhstani law, but rather a selective and functional adaptation of those principles that address the risks posed by digital migration governance. This approach is also supported by the Council of Europe's earlier assessment of Kazakhstan's data protection framework, which identified several areas requiring clarification or strengthening, including the application of data protection guarantees to all individuals regardless of nationality or residence, the prevention of excessive data processing, data accuracy, safeguards for special categories of data, and independent supervisory oversight.

43 'Results of Public Discussion of Amendments on Issues of Rapid Response to Personal Data Leakage' (*Eurasian Digital Foundation*, 21 December 2023) <<https://digitalrights.asia/analytic/public-hearings-results-on-prompt-response-to-data-leakage/>> accessed 18 May 2026.

44 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (n 32).

45 Law of the Republic of Kazakhstan No 94-V (n 40).

In this regard, it is proposed to amend the article on the principles of personal data processing by expressly adding, alongside the existing principles, the following:

- the “principle of proportionality and fair balance of interests,” under which the scope and nature of processing must be necessary and proportionate to the purpose, taking into account the rights and freedoms of data subjects;
- the “principle of data minimisation and purpose limitation,” under which only data that are necessary and sufficient for specifically defined and legitimate purposes may be collected, and processing incompatible with those purposes is not permitted, except in cases expressly provided for by law;
- the “principle of storage limitation,” requiring the destruction or anonymisation of data once the purpose has been achieved or the lawful retention period has expired;
- the “principle of transparency of processing,” establishing an obligation for operators to provide data subjects with clear information on the purposes, legal grounds, and recipients of the data;
- the “principle of accountability and data protection by design and by default,” obliging operators both to demonstrate compliance of processing with the law and to design processes and systems from the outset to minimise risks to data subjects’ rights.

We consider it necessary to clarify the rules on data subject consent. In the provisions governing the conditions for collection and the form of consent, it should be specified that consent must be “freely given, specific, informed, and unambiguous,” may be withdrawn as easily as it was given, and may not be made a condition for the provision of a service beyond the extent of processing that is objectively necessary to deliver that service. This would enable courts and the competent authority, when assessing individual cases, to examine not only the existence of a formal document but also the data subject’s genuine awareness, voluntariness, and the specificity of the consent.

We also consider it necessary to introduce into the Law “On Personal Data and Their Protection” a specific provision on a “personal data protection impact assessment” (data protection impact assessment). Such an assessment could be made mandatory for categories of processing that inherently entail elevated risks, including large-scale state databases (tax, migration, electoral registers), biometric data processing, profiling and automated decision-making, and cross-border transfers to jurisdictions that do not provide an adequate level of protection.

Further development of these approaches is evident in the latest European instruments governing the use of artificial intelligence. Whereas Convention 108+ is concerned primarily with the protection of personal data and with safeguards for lawful, proportionate,

and secure processing, Regulation (EU) 2024/1689 (the EU AI Act)⁴⁶ and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law⁴⁷ shift the focus to a broader question: how digital and algorithmic systems capable of significantly affecting human rights should be legally constrained, including where they interfere with the right to privacy, the protection of personal data, non-discrimination, procedural fairness, and effective remedies. The European Commission expressly characterises the AI Act as the first comprehensive legal framework for artificial intelligence based on a risk-based approach, while the Council of Europe describes its Convention as the first legally binding international treaty in this field, aimed at ensuring that the use of AI remains compatible with human rights, democracy, and the rule of law.

Of particular importance in the fields of migration, asylum, and border management is the fact that the AI Act does not treat the use of AI in this area as a form of technically neutral administrative automation, but rather as the deployment of high-risk systems capable of directly affecting the fundamental rights of persons in vulnerable situations who are dependent on decisions taken by public authorities. In this regard, Recital 60 emphasises the requirements of accuracy, transparency, and non-discrimination applicable to such systems, since it is through these safeguards that compliance with freedom of movement, the right to privacy, the protection of personal data, non-discrimination, the right to international protection, and the right to good administration is to be ensured. At the same time, the Act expressly provides that the use of AI in migration, asylum, and border management must not serve to circumvent the international obligations of states, including those arising under the 1951 Convention relating to the Status of Refugees.⁴⁸

Normatively, this is reflected in the fact that Annex III of the AI Act classifies as high-risk AI systems a number of systems used in migration, asylum, and border control, including tools for risk assessment, the recognition and identification of persons, as well as systems used in the examination of applications for asylum, visas, and residence permits. Such classification means that the risk to human rights in this field is understood to be structural, since digital systems can directly affect access to status, procedure, territory, documentation, or protection.

A more operational reading of the EU AI Act shows that its relevance for Kazakhstan lies not only in classifying AI systems for migration, asylum, and border management as high-risk, but also in the specific obligations attached to that classification. Article 6 provides the entry point by determining when an AI system is considered high-risk. For migration governance, this approach is important because systems used for risk assessment, identity

46 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence [2024] OJ L 2024/1689.

47 Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law (adopted 17 May 2024) [2024] CETS 225.

48 Convention Relating to the Status of Refugees (adopted 28 July 1951) [1954] UNTS 189/137.

verification, profiling, or support in decisions on visas, residence, or access to employment may directly affect a person's legal status and access to rights.

The most transferable elements for Kazakhstan are not the EU market-access mechanisms or CE conformity procedures, but rather the substantive safeguards applicable to high-risk systems. Article 9 requires a lifecycle risk management system; Article 10 requires data governance, including attention to data quality, representativeness, errors, gaps, and bias; Article 13 requires transparency and sufficient information on the system's intended purpose, accuracy, limitations, risks, and interpretation of outputs; and Article 14 requires effective human oversight, including the ability to understand, disregard, override, or stop the system's output where necessary. These obligations are directly relevant to migration procedures because inaccurate data, biased datasets, or over-reliance on automated outputs may result in wrongful refusal, delay, misidentification, or restriction of a migrant's access to work and residence.

Articles 26 and 27 are particularly important for legislative adaptation because they concern the duties of deployers, including public authorities. A Kazakhstani model could require public bodies using high-risk AI or algorithmically supported systems in migration and labour regulation to use such systems only for legally defined purposes, appoint responsible officials for human oversight, maintain logs, monitor accuracy and discriminatory effects, suspend use where serious risks are identified, and conduct a prior fundamental rights impact assessment before deployment. Such an assessment should describe the purpose and context of use, categories of affected persons, types of data processed, foreseeable risks, safeguards, human oversight measures, and remedies available to the person concerned.

Accordingly, the EU AI Act should not be understood as a model to be transposed mechanically. Rather, it provides a regulatory toolkit that Kazakhstan could adapt selectively: classification of high-risk digital systems in migration and employment of foreigners; mandatory risk and rights impact assessment; data quality and bias-control duties; transparency obligations; human review of adverse digital outcomes; logging and audit mechanisms; and institutional accountability of public authorities deploying such systems.

The Council of Europe Framework Convention on Artificial Intelligence complements this sector-specific and risk-based approach by establishing a broader regulatory model grounded in human rights, democracy, and the rule of law. Unlike the EU AI Act, it is not limited to classifying high-risk systems but also establishes general obligations for public authorities and, where appropriate, for private actors involved in the design or use of AI systems. Of particular importance are its requirements concerning transparency, accountability, non-discrimination, protection of private life and personal data, effective remedies, procedural safeguards, and the assessment and mitigation of AI-related risks and impacts. Against this background, Kazakhstan's regulatory framework still appears fragmented: while it focuses primarily on the security of data processing, it does not yet provide for a general category of high-risk digital or AI-supported systems, mandatory prior assessment of impacts on rights, or developed requirements concerning transparency, human oversight, contestability, and institutional accountability in algorithmically supported decision-making.

5 RESULTS

The analysis identifies four key problem areas: labour migrants' growing dependence on digital identification and interagency registers; insufficient legal articulation of data minimisation, purpose limitation, transparency, accountability, privacy-by-design and privacy-by-default; heightened risks linked to biometric processing and interagency data exchange, as illustrated by mandatory dactyloscopic registration of foreigners and stateless persons; and the need for procedural safeguards in algorithmically supported decision-making, including risk assessment, data governance, transparency, human review, logging, explanation, correction and appeal.

These findings are set out below as a proposed set of digital rights and regulatory safeguards for labour migrants.

Table 4. A Framework of digital rights and regulatory safeguards for labour migrants

Digital right of a labour migrant	Digital Rights of a Labour Migrant
The labour migrant's digital right to proportionate and purpose-limited processing of personal and migration-related data.	The processing of labour migrants' personal and migration-related data shall be permitted only to the extent and by the means that are necessary and proportionate to specifically defined and legitimate purposes of processing. The collection and use of personal data that have no direct relevance to the purpose of processing, as well as any subsequent processing incompatible with the initially stated purposes, shall not be permitted, except in cases expressly provided for by the laws of the Republic of Kazakhstan
The labour migrant's digital right to freely given, specific, and informed consent to data processing.	A data subject's consent to the processing of their personal and biometric data shall be freely given, specific, informed, and unambiguous. Consent shall not be considered freely given where the processing of personal data is not objectively necessary for the provision of the relevant public service, the performance of labour or migration procedures, or is imposed as a mandatory condition for access to such services without lawful grounds.
The labour migrant's digital right to enhanced protection of biometric data.	The processing of labour migrants' biometric data shall be permitted exclusively based on a specific legal ground established by law or the data subject's separate explicit consent. The storage of biometric data shall be allowed only for the period objectively necessary to achieve the purpose of processing, followed by the mandatory destruction or anonymisation of such data

Digital right of a labour migrant	Digital Rights of a Labour Migrant
The labour migrant's digital right to data protection.	Operators processing labour migrants' personal and biometric data through information systems shall ensure data protection by design and by default, including the minimisation of the volume of processed data, limitation of retention periods, and restriction of the circle of persons having access to the data. For types of processing that create heightened risks to the rights and freedoms of data subjects, a prior assessment of the impact of processing on the rights and freedoms of data subjects shall be carried out.
The right to a prior risk assessment in high-risk digital data processing.	In cases where labour migrants' personal and biometric data are processed using information systems that pose heightened risks to the rights and freedoms of data subjects, the operator shall, prior to commencing the processing, conduct a personal data processing impact assessment, document its results, implement risk-mitigation measures, and provide such assessment to the competent authority upon request.
The labour migrant's digital right to proportionate safeguards in biometric registration.	Mandatory biometric registration of labour migrants, including dactyloscopic registration, shall be permitted only based on a clear legal ground and for specifically defined legitimate purposes. The law shall establish the categories of biometric data collected, retention periods, competent authorities entitled to access the data, grounds for inter-agency transfer, audit mechanisms, and remedies for correcting inaccurate records or challenging adverse outcomes.
The labour migrant's digital right to human oversight and contestation of algorithmically supported decisions.	Where digital or AI-supported systems are used in migration or labour-related decision-making, labour migrants shall have the right to meaningful human review, information on the role of the system, correction of inaccurate data, and access to effective appeal mechanisms. Public authorities and private platforms deploying such systems shall ensure risk management, data quality control, transparency, logging, monitoring of discriminatory effects, and prior assessment of impacts on rights.

6 CONCLUSION

The study confirms that the digitalisation of migration administration and the labour market is transforming the position of the labour migrant: the exercise of key rights increasingly depends on the quality of digital procedures, the architecture of information systems, and the rules governing the processing of personal and biometric data. In this context, the “digital rights of labour migrants” should be understood not as an abstract doctrinal construct, but as a practice-oriented set of guarantees ensuring: (1) the lawfulness, proportionality, and transparency of data processing; (2) access to digital public services without discriminatory barriers; and (3) procedural fairness and effective remedies in cases of register errors, digital identification failures, and adverse digital decisions.

The comparative legal analysis of international approaches and Kazakhstan’s national legislation indicates normative insufficiency in relation to the principles and procedures of data processing, especially regarding biometrics, interagency data exchange, and potential algorithmic components of decision-making. Clearer legal requirements are needed for data minimisation, purpose and storage limitation, transparency, accountability, and the mandatory integration of risk considerations into the design of digital services (privacy-by-design/privacy-by-default). At the same time, procedural safeguards require strengthening, including access to information about digital processes, the ability to promptly correct errors, clear and rapid appeal mechanisms, and institutional accountability of operators and public authorities for data quality and processing security.

Beyond purely legal compliance, the responsible use of migrants’ data should be treated as an ethical and institutional requirement of digital migration governance. Biometric data, inter-agency data exchange, and algorithmic profiling may directly affect a migrant’s legal status, access to work, residence, and public services. Therefore, such data should not be used as a general-purpose instrument of surveillance or control, but only for clearly defined, lawful, necessary, and proportionate purposes. Safeguards against misuse should include purpose limitation, strict access control, retention limits, audit trails, independent oversight, prohibition of unjustified secondary use, mechanisms for correcting inaccurate data, and effective remedies against adverse digital outcomes. These obligations should apply not only to public authorities, but also to private digital platforms involved in labour intermediation, rating systems, digital profiling, or algorithmic management of migrant work.

The analysis indicates that Kazakhstan’s existing data protection framework should be further specified in the context of labour migration. In this sphere, digital data are not merely an object of privacy protection, but a legal precondition for access to migration registration, residence, lawful employment, employer reporting procedures, and, increasingly, platform-mediated work. Errors, omissions, or non-transparent data exchanges in migration, labour, or biometric systems may therefore directly affect a labour migrant’s legal status, access to work, and ability to obtain an effective remedy. For this

reason, the article distinguishes between general safeguards applicable to all data subjects and additional guarantees required in labour migration governance. General safeguards should include data minimisation, purpose limitation, transparency, storage limitation, security, and accountability. Labour-migration-specific safeguards should include accelerated correction of inaccurate records affecting residence or work authorisation, notification and explanation of adverse digital outcomes, meaningful human review of decisions supported by digital or algorithmic systems, clear rules on employer and platform data reporting, and effective complaint and appeal procedures where digital data influence access to lawful employment or migration-related procedures.

REFERENCES

1. Akhmetova S, 'Some Aspects of Personal Data Protection Legislation' [2023] Kazakhstan Law Review
2. Alencar A, 'Mobile Communication and Refugees: An Analytical Review of Academic Literature' (2020) 14(8) Sociology Compass e12802, doi:10.1111/soc4.12802
3. Amelung N and others, 'Technologies, Infrastructures and Migrations: Material Citizenship Politics' (2020) 24(5) Citizenship Studies 587, doi:10.1080/13621025.2020.1784636
4. Baldassar L and others, 'ICT-Based Co-Presence in Transnational Families and Communities: Challenging the Premise of Face-to-Face Proximity in Sustaining Relationships' (2016) 16 Global Networks 133, doi:10.1111/glob.12108
5. Dekker R and Engbersen G, 'How Social Media Transform Migrant Networks and Facilitate Migration' (2014) 14(4) Global Networks 401, doi:10.1111/glob.12040
6. Delovarova L, 'Kazakhstan's Migration Policy: An Overview of the External Vector' (2024) 105(1) International Relations and International Law Journal 50, doi:10.26577/IRILJ.2024.v105.i1.05
7. Diminescu D, 'The Connected Migrant: An Epistemological Manifesto' (2008) 47(4) Social Science Information 565, doi:10.1177/0539018408096447
8. Esposito F and others, 'Ecology of Sites of Confinement: Everyday Life in a Detention Center for Illegalized Non-Citizens' (2019) 63(1-2) American Journal of Community Psychology 190, doi:10.1002/ajcp.12313
9. Floridi L, *The Ethics of Information* (OUP 2013) doi:10.1093/acprof:oso/9780199641321.001.0001
10. Hildebrandt M, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2016)
11. Hoang LA, 'Migration Infrastructure, Digital Connectivity and Porous Borders: Vietnamese Migration to Australia' (2025) 31(1) Population, Space and Place e2868, doi:10.1002/psp.2868

12. Isin E and Ruppert E, *Being Digital Citizens* (Rowman & Littlefield Publishers, 2015)
13. Kadyrbek Z and Koblandin K, 'Digitalisation of Labour Migration within the EAEU Digital Agenda' (2025) 109(1) *International Relations and International Law Journal* 126, doi:10.26577/IRILJ2025109111
14. Leurs KHA and Smets K, 'Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe' (2018) 4(1) *Social Media + Society* 1, doi:10.1177/2056305118764425
15. Maltabarov A and Sarybayev M, 'Digital Transformation as a New Stage in Regulating Migration Processes in Central Asia' (2024) 88(1) *Public Administration and Civil Service* 106, doi:10.52123/1994-2370-2024-1164
16. Marino S, 'Making Space, Making Place: Digital Togetherness and the Redefinition of Migrant Identities Online' (2016) 1(2) *Social Media + Society* 1, doi:10.1177/2056305115622479
17. Milan S, Pelizza A and Lausberg Y, 'Making Migrants Visible to COVID-19 Counting: The Dilemma' (*OpenDemocracy*, 28 April 2020) <<https://www.opendemocracy.net/en/making-migrants-visible-covid-19-counting-dilemma/>> accessed 18 May 2026
18. Molnar P, 'Surveillance Sovereignty: Migration Management Technologies and the Politics of Privatization' in Atak I and Hudson G (eds), *Migration, Security, and Resistance: Global and Local Perspectives* (Routledge 2021) 66
19. Mossberger K, Tolbert CJ and McNeal RS, *Digital Citizenship: The Internet, Society, and Participation* (MIT Press 2007) doi:10.7551/mitpress/7428.001.0001
20. Pelizza A, 'Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-Construction of Individuals and Politics' (2020) 45(2) *Science, Technology, & Human Values* 262, doi:10.1177/0162243919827927
21. Pollozek S and Passoth JH, 'Infrastructuring European Migration and Border Control: The Logistics of Registration and Identification at Moria Hotspot' (2019) 37(4) *Environment and Planning D: Society and Space* 606, doi:10.1177/0263775819835819
22. Razmetaeva Yu, Barabash Yu and Lukianov D, 'The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice' (2022) 5(3) *Access to Justice in Eastern Europe* 41, doi:10.33327/AJEE-18-5.3-a000327
23. Rygiel K, 'Bordering Solidarities: Migrant Activism and the Politics of Movement and Camps at Calais' (2011) 15(1) *Citizenship Studies* 1, doi:10.1080/13621025.2011.534911
24. Taylor L, 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally' (2017) 4(2) *Big Data & Society* 1, doi:10.1177/2053951717736335

25. Vavoula N, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) 23(4) European Journal of Migration and Law 457, doi:10.1163/15718166-12340114
26. Yerbolatov E and others, 'Personal Data in the Republic of Kazakhstan: Problems of Ensuring Confidentiality in the Context of Digitalisation' (2020) 79(3) Bulletin of Innovative Eurasian University 49, doi:10.37788/2020-3/49-58
27. Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books Ltd, 2019)
28. Zwysen W and Piasna A, *Digital Labour Platforms and Migrant Workers: Analysing Migrants' Working Conditions and (Over)Representation in Platform Work in Europe* (Working Paper, ETUI 2024) doi:10.2139/ssrn.4798982

AUTHORS' INFORMATION

Madina Abdramanova*

PhD student, Jurisprudence, Astana International University, Astana, Republic of Kazakhstan
zvezdageneral001@gmail.com

<https://orcid.org/0009-0000-2516-6179>

Corresponding author, responsible for conceptualisation, data curation, formal analysis, writing – original draft

Amanzhol Nurmagambetov Sr.

Doctor of juridical sciences, Jurisprudence, Astana International University Higher Law School, Astana, Republic of Kazakhstan
amanzholnurmagambetov@gmail.com

<https://orcid.org/0000-0001-9026-9019>

Co-author, responsible for conceptualisation, methodology, writing – original draft

Anuar Nurmagambetov Sr.

Candidate of Sciences (Law), Jurisprudence, Kokshetau University named after Abay Myrzakhmetov, Kokshetau, Republic of Kazakhstan
an.nurmagambetov@gmail.com

<https://orcid.org/0009-0006-4362-9556>

Co-author, responsible for methodology, project administration, writing – review & editing

Aigerim Zhumabayeva

PhD (Law), Department of Material and Technical Support, REM «Institute of Parliamentarism», Astana, Republic of Kazakhstan
aigerimzhumabayeva9933@gmail.com

<https://orcid.org/0000-0003-3376-4325>

Co-author, responsible for methodology, validation, writing – review & editing

Competing interests: No competing interests were disclosed. The authors must disclose any potential conflict of interest.

Disclaimer: The authors declare that their opinions and views expressed in this manuscript are free from the influence of any organisations.

RIGHTS AND PERMISSIONS

Copyright: © 2026 Madina Abdramanova, Amanzhol Nurmagambetov Sr., Anuar Nurmagambetov Sr., Aigerim Zhumabayeva. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing editor – Valentina Krivolapova. **English Editor** – Robert Reddin.

Ukrainian language Editor – Liliia Hartman.

ABOUT THIS ARTICLE

Cite this article

Abdramanova M, Nurmagambetov AmSr, Nurmagambetov AnSr and Zhumabayeva A, 'Digital Rights of Labour Migrants in Kazakhstan: International Standards, Digital Governance and Regulatory Safeguards' (2026) 9(3) Access to Justice in Eastern Europe 278-308 <<https://doi.org/10.33327/AJEE-18-9.3-a0001986>>

DOI: <https://doi.org/10.33327/AJEE-18-9.3-a0001986>

Summary: 1. Introduction. – 2. Literature Review – 3. Methodology. – 4. Discussion. – 4.1. *General Analysis of the Migration Situation in Kazakhstan Based on Statistical Data.* – 4.2 *Comparative Analysis of Labour Migrants' Digital Rights and Their Protection in the Context of International and Kazakhstani Legal Regulation.* – 5. Results. – 6. Conclusion.

Keywords: labour migrants; biometric data; migration governance; algorithmic decision-making; digital rights.

DETAILS FOR PUBLICATION

Date of submission: 5 Jan 2026

Date of acceptance: 22 May 2026

Online First Publication: 29 Jun 2026

Last Publication: 05 Aug 2026

Was the manuscript fast-tracked? – No.

Number of reviewer reports submitted in the first round: 2 reports.

Number of revision rounds: 2 rounds with major and minor revisions

Technical tools were used in the editorial process

Plagiarism checks - Turnitin from iThenticate

<https://www.turnitin.com/products/ithenticate/>

Scholastica for Peer Review

<https://scholasticahq.com/law-reviews>

AI DISCLOSURE STATEMENT

We confirm that no artificial intelligence tools or services were used at any stage of writing, translating, editing, or analysing content for this manuscript.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ЦИФРОВІ ПРАВА ТРУДОВИХ МІГРАНТІВ У КАЗАХСТАНІ: МІЖНАРОДНІ СТАНДАРТИ, ЦИФРОВЕ УПРАВЛІННЯ ТА РЕГУЛЯТОРНІ ЗАХОДИ

**Мадіна Абдраманова*, Аманжол Нурмагамбетов ст.,
Ануар Нурмагамбетов ст. та Айгерім Жумабаєва**

АНОТАЦІЯ

Вступ. Цифровізація управління міграцією та регулювання праці докорінно змінила умови, за яких трудові мігранти реалізують свої права. У Казахстані мігранти дедалі більше залежать від електронних державних послуг, цифрової ідентифікації, біометричної верифікації, сумісних баз даних та посередництва у сфері праці на основі платформ. Хоча ці технології можуть підвищити адміністративну ефективність, вони також створюють нові правові ризики, зокрема непрозору обробку персональних та

біометричних даних, надмірний збір даних, помилки ідентифікації, цифрову ізоляцію та обмежений доступ до ефективних засобів правового захисту. Ці тенденції вимагають чіткішої концептуалізації цифрових прав трудових мігрантів та точнішої оцінки того, чи є наявні правові механізми в Казахстані достатніми для їх захисту.

Методи. У дослідженні використовується доктринальна та порівняльно-правова методологія. Воно розглядає правовий зміст цифрових прав трудових мігрантів за допомогою аналізу міжнародних стандартів у сфері прав людини та захисту даних, зокрема Конвенції 108+, практики Європейського суду з прав людини, Регламенту (ЄС) 2024/1689 (Акту ЄС про штучний інтелект) та Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права. Ці стандарти порівнюються із законодавством Республіки Казахстан у сферах міграції, праці та захисту персональних даних. У дослідженні також використовується ризик-орієнтований аналітичний підхід до виявлення регуляторних прогалів, пов'язаних з біометричною обробкою, міжвідомчим обміном даними, автоматизованим ухваленням рішень та наданням цифрових послуг.

Результати та висновки. Дослідження демонструє, що правова база Казахстану містить важливі базові гарантії, але залишається фрагментованою у своєму підході до цифрових ризиків, що впливають на трудових мігрантів. Законодавство недостатньо чітко формулює принципи пропорційності, обмеження мети, обмеження зберігання, прозорості та підзвітності як дієві правові стандарти. У ньому також бракує зазначення чітких зобов'язань щодо захисту приватності на етапі проектування, захисту приватності за замовчуванням та оцінки впливу на захист даних для обробки з високим рівнем ризику, особливо коли йдеться про біометричні дані або рішення, ухвалені за допомогою алгоритмів. Процедурні гарантії також недостатньо розвинені, зокрема щодо права на інформацію, виправлення неточних даних, пояснення несприятливих цифрових наслідків та ефективного оскарження рішень.

У статті стверджується, що цифрові права трудових мігрантів слід розуміти як структурований набір гарантій, що забезпечують законну, пропорційну та прозору обробку даних, недискримінаційний доступ до цифрових послуг та процесуальний захист від несприятливих цифрових рішень. У статті пропонується посилити правову базу Казахстану за допомогою чіткішого закріплення принципів захисту даних, запровадження обов'язкової оцінки впливу для систем високого ризику, посилення гарантій біометричних даних та розширення процесуальних прав у сфері цифрового управління міграцією.

Ключові слова. Трудові мігранти; біометричні дані; управління міграцією; рішення, ухвалені за допомогою алгоритмів; цифрові права.