Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

Regulating Artificial Intelligence: Challenges for Data Protection and Privacy in Developing Nations

[1]**Wasmiya Malik -Email-wasmia.malik@gmail.com**
[2]**Seema Gul -Email-gulseema03@gmail.com**
[3*]**Gohar Masood Qureshi -Email-goharqureshi12@gmail.com**
[1]MS Scholar International Islamic University, Islamabad, Pakistan
[2]Lecturer, Department of Law, University of Sialkot Pakistan
[3*]Lecturer, Department of Law, University of Sialkot, Sialkot, Punjab, Pakistan

Article Details:

Received on 12 April 2025
Accepted on 14 May 2025
Published on 16 May 2025

Corresponding Authors*:

Abstract

The rapid integration of artificial intelligence (AI) technologies in developing nations presents both opportunities for progress and significant challenges, particularly in the realms of data protection and privacy. This research examines the complex legal and institutional obstacles these countries face in regulating AI, with a focus on the lack of comprehensive data governance frameworks, weak enforcement mechanisms, and technological dependence on foreign-developed systems. The purpose of this study is to critically analyze the current regulatory landscape in developing nations, assess gaps in existing data protection laws, and explore the implications of AI deployment in low-capacity environments. Employing a qualitative legal research methodology, the study reviews relevant domestic legislation, soft law instruments, and international best practices. The findings reveal that developing nations often lack the institutional capacity and normative clarity required to regulate AI effectively, which exacerbates risks of surveillance, discrimination, and rights violations. The paper proposes a rights-based, context-specific regulatory approach, emphasizing legal reform, capacity building, and inclusive policymaking. Ultimately, this study highlights the urgent need for coherent AI governance strategies that prioritize human dignity and digital rights in the Global South. The rapid advancement of AI has raised profound legal and ethical concerns regarding data protection and privacy, particularly in developing nations. This paper examines the core regulatory challenges these countries face in safeguarding personal data and ensuring privacy amidst increasing AI adoption. By analyzing the intersection of AI technologies with existing legal infrastructures, the study highlights institutional, normative, and infrastructural deficits that inhibit effective regulation. It proposes a multi-tiered legal reform approach tailored to the needs and capacities of developing nations, aiming to balance innovation with rights protection.

Keywords: algorithmic accountability, digital rights, legal infrastructure, institutional capacity, automated decision-making, cross-border data flows, regulatory gaps, human dignity,surveillance risks, public sector AI deployment

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

Introduction

AI has emerged as a transformative technology, reshaping economies, governance structures, and public service delivery across the globe. While AI-driven innovations offer promising solutions to development challenges—particularly in sectors such as healthcare, agriculture, education, and law enforcement—they also raise serious legal and ethical concerns regarding data protection and privacy. These challenges are amplified in developing nations, where institutional, normative, and technological capacities are often limited. The integration of AI into government and commercial operations in such settings often occurs without adequate legal safeguards, leading to an increased risk of surveillance, discrimination, and rights violations (Sharma & Sharma, 2024).

This study aims to examine the legal and regulatory obstacles that developing nations face in addressing data protection and privacy concerns in the context of AI. The scope of this research includes a comparative review of existing legislative frameworks, identification of normative and institutional gaps, and exploration of international soft law mechanisms guiding AI governance. The central hypothesis is that the absence of robust and context-specific data governance frameworks in developing nations heightens vulnerabilities and undermines the ethical deployment of AI technologies. Key questions addressed include: What are the structural and legal weaknesses in current AI regulation? How can developing countries create effective, rights-respecting AI governance frameworks? Using a qualitative legal research methodology, this article draws upon domestic laws, international standards, academic literature, and policy documents to assess the extent of AI regulation in selected developing nations. The study highlights that while some countries have introduced data protection laws, most lack enforceable provisions for algorithmic accountability, consent management, and redress mechanisms. Moreover, enforcement agencies often lack the technical expertise and resources to implement existing laws effectively.

The findings point to the urgent need for a rights-based and localized approach to AI regulation, one that balances innovation with privacy and data protection. The remainder of the article is structured as follows: Section two provides an overview of AI's data-driven nature and its implications for privacy. Section three reviews the legal landscape in selected developing countries. Section four identifies core regulatory challenges, while Section five discusses relevant international frameworks. Section six proposes strategic recommendations for building effective AI governance structures. Finally, Section seven concludes the study with reflections on the future of AI regulation in the Global South. Artificial intelligence is reshaping global economies, governance, and societal norms. While its benefits in healthcare, education, and public administration are increasingly acknowledged, the use of AI also raises significant data protection and privacy issues. Developing nations, eager to harness AI's potential, often do so without robust legal and technical safeguards. The absence of comprehensive data protection regimes, weak enforcement mechanisms, and limited institutional capacity heightens the risk of surveillance, discrimination, and privacy breaches.

Research Methodology:

This research employs a qualitative methodology to investigate the challenges of regulating AI and ensuring data protection in developing nations. The study relies on a combination of documentary analysis, case studies, and comparative legal research to explore the legal, social, and technological issues associated with AI governance. Primary sources, including national laws, international regulations, and reports from organizations such as the United Nations and the OECD, were analyzed to identify existing legal frameworks and the gaps in AI regulation. Additionally, case studies from countries such as Pakistan, Nigeria, and Brazil were examined to assess how national governments are addressing these challenges and the effectiveness of their policies. The study also draws upon secondary sources, including scholarly articles, policy papers, and reports from tech companies and NGOs, to analyze the broader implications of AI deployment in developing nations. The rationale for this methodological approach is to provide

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

a comprehensive understanding of the regulatory landscape and offer practical recommendations for future development of AI laws in the Global South.

The Rise of AI and Its Data Dependency

Artificial Intelligence, particularly machine learning and deep learning systems, functions through the consumption, processing, and analysis of massive datasets. The performance, accuracy, and adaptability of AI systems are largely contingent on the volume and variety of data fed into them. These datasets often include personal, sensitive, and even biometric information, raising fundamental concerns regarding data privacy, informed consent, and user autonomy. In developing nations, where digital infrastructure is expanding rapidly but legal safeguards remain underdeveloped, this dependency on data introduces unique vulnerabilities AI is increasingly deployed across critical public and private sectors in developing contexts. From facial recognition in law enforcement and automated welfare distribution systems to AI-driven education platforms and health diagnostics, these applications collect and process extensive personal data, frequently without clear legal authorization or oversight mechanisms. This growing reliance on data-centric AI intensifies the risk of mass surveillance, data breaches, and algorithmic bias—risks that are often compounded by the absence of robust data protection frameworks (Yanamala & Suryadevara, 2023).

Moreover, developing nations often rely on AI technologies developed in foreign jurisdictions, meaning that local data is processed by systems built around external privacy norms and standards. This creates a structural imbalance, where developing countries become data providers while having little control over how that data is used or stored. As a result, the unchecked use of data-intensive AI systems not only threatens individual rights but also undermines national data sovereignty The rise of AI in developing nations thus brings with it a pressing need to evaluate and strengthen legal mechanisms that govern data collection, processing, and usage. Addressing these concerns is essential to ensure that technological progress does not come at the cost of human dignity, transparency, and accountability. AI systems, particularly those using machine learning and big data analytics, thrive on vast datasets. These include personal, sensitive, and often biometric data. In developing nations, such data is collected with minimal oversight, leaving individuals vulnerable to misuse and exploitation. The use of AI in public services, from predictive policing to social benefit distribution, amplifies the need for stringent data governance frameworks (Mazurek & Małagocka, 2019).

Current Legal Landscape in Developing Nations

Developing nations are at varying stages in the formulation and enforcement of data protection laws, yet most face significant gaps when it comes to regulating artificial intelligence specifically. Legal frameworks often remain fragmented, outdated, or in draft form, lacking the precision and enforceability needed to address the complex challenges posed by AI systems. In countries like Pakistan, for instance, the proposed *Personal Data Protection Bill* remains pending, with existing laws offering only piecemeal protection against data misuse. Nigeria's *Data Protection Regulation (NDPR)*, while a progressive step, remains limited in scope and does not adequately address automated decision-making or cross-border data transfers. Kenya's *Data Protection Act* includes more robust provisions, such as the requirement for Data Protection Impact Assessments, but enforcement has been inconsistent, and AI-specific concerns remain underregulated. Brazil's *LGPD*—inspired by the EU's GDPR—includes protections for automated processing, but its applicability in deeply data-driven AI contexts is still being tested. India's recently enacted *Digital Personal Data Protection Act* (2023) shows promise but has drawn criticism for centralized control and lack of independent oversight (Hasan, 2024). Across these jurisdictions, enforcement bodies often suffer from inadequate funding, technical limitations, and institutional fragility. Moreover, public awareness of data rights remains low, leaving individuals especially vulnerable to privacy violations and algorithmic harms. Collectively, these

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

issues highlight the need for developing nations to move beyond surface-level legislative reforms and build comprehensive, rights-based legal and institutional frameworks that can effectively regulate AI technologies in practice. Many developing countries lack standalone data protection legislation (Puertas-Bravo et al., 2024). Where laws do exist, they are often outdated, lack comprehensive coverage of automated decision-making, or do not align with international standards like the GDPR. Examples include:

Pakistan

Pakistan has made tentative strides toward establishing a data protection framework, but substantial regulatory gaps persist, particularly in the context of artificial intelligence. The proposed *Personal Data Protection Bill*, first introduced in 2020 and revised in subsequent years, remains under consideration and has yet to be enacted into law. Although the bill borrows heavily from global models like the EU's GDPR—incorporating provisions on consent, data subject rights, and cross-border data transfers—it lacks clarity on AI-specific risks such as automated decision-making, algorithmic profiling, and the need for transparency in machine-led processes. In the absence of a dedicated data protection authority, oversight and enforcement remain uncertain. Sectoral regulations, such as those under the *Prevention of Electronic Crimes Act (PECA) 2016* and telecommunications laws, offer fragmented and sometimes conflicting protections (Khan et al., 2025). Moreover, these frameworks often emphasize state surveillance and national security over individual privacy rights. The lack of institutional expertise, limited technical infrastructure, and minimal public awareness further undermine the ability to safeguard personal data in an AI-driven environment. As Pakistan accelerates the use of AI in areas such as e-governance, facial recognition, and predictive policing, the absence of a coherent regulatory framework increases the risk of privacy violations and unchecked algorithmic bias. This underscores the urgent need for Pakistan to adopt a rights-based, transparent, and enforceable AI governance strategy rooted in both local realities and international best practices. While the Personal Data Protection Bill has been proposed, it has not yet been enacted, and sector-specific laws offer fragmented protection (Khan & Ullah, 2024).

Nigeria

Nigeria represents one of the more proactive developing nations in initiating data protection measures, primarily through the *NDPR*, introduced in 2019 by the National Information Technology Development Agency (NITDA). The NDPR marked an important milestone in acknowledging the importance of digital rights and personal data protection. It outlines principles on consent, data minimization, and the obligations of data controllers and processors. However, the regulation is limited in scope and enforcement authority, and it does not explicitly address the implications of artificial intelligence or automated decision-making systems. While the NDPR mandates compliance audits and has initiated some enforcement actions, its reach is constrained by limited institutional capacity, insufficient funding, and lack of specialized personnel trained in emerging technologies (Lin & Song, 2024). Moreover, Nigeria lacks a comprehensive data protection law passed by the legislature, which would provide stronger legal standing and clearer guidance on AI governance. As AI-powered systems are increasingly adopted across public administration, finance, and security sectors, the absence of detailed provisions concerning algorithmic transparency, bias mitigation, and redress mechanisms poses serious risks to privacy and fairness. The ongoing development of a full-fledged Data Protection Bill is a positive sign, but until it is enacted and backed by a well-resourced regulatory authority, Nigeria's data governance framework will remain ill-equipped to address the challenges posed by AI. The NDPR provides a foundation but is limited in scope and enforcement (Khan, 2024).

Kenya and Brazil

Kenya has emerged as a regional leader in data protection through the enactment of the *Data Protection Act* (DPA) in 2019, a comprehensive statute modeled in part on the EU's General

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

Data Protection Regulation (GDPR). The DPA established a legal framework for the processing of personal data and created the Office of the Data Protection Commissioner (ODPC) to oversee compliance. It mandates principles such as lawfulness, transparency, purpose limitation, and data minimization, and it requires Data Protection Impact Assessments (DPIAs) for high-risk processing activities. However, while the legislation is relatively progressive, its implementation remains uneven. The ODPC is still developing institutional capacity, and awareness of data rights among the public and stakeholders is limited. Crucially, the Act does not yet contain tailored provisions for regulating AI-specific risks such as algorithmic discrimination, automated profiling, or decision-making transparency. As Kenya increases its reliance on digital identity systems, surveillance technologies, and AI-driven public services, the absence of detailed AI governance provisions exposes individuals to significant privacy risks. To maintain its leadership position, Kenya must refine its legal framework to address the specific challenges posed by AI technologies (Khan, 2024).

Brazil, though often classified as an emerging economy, presents a useful comparative model for other developing nations due to its relatively advanced data protection regime. The *Lei Geral de Proteção de Dados* (LGPD), enacted in 2018 and fully effective since 2020, is Brazil's primary data protection law and shares several features with the GDPR. It governs the processing of personal data in both public and private sectors and applies extraterritorially. The LGPD includes provisions on automated decision-making, granting individuals the right to request explanations for decisions made solely by automated means—a key protection in the AI era. Brazil also established the National Data Protection Authority (ANPD) to enforce the LGPD and issue regulatory guidance (Khan & Jiliani, 2023). While Brazil's framework is one of the most comprehensive among developing countries, challenges remain in translating legal protections into practice. Enforcement is still maturing, public awareness is uneven, and the technical complexities of AI systems often exceed the capacity of existing institutions. Moreover, the LGPD does not yet include robust standards for algorithmic accountability or risk assessments tailored specifically to AI. Nevertheless, Brazil's progress highlights the importance of institutional autonomy, strong legal mandates, and rights-based principles in building effective AI governance. Kenya's Data Protection Act (2019) and Brazil's LGPD show promise, but enforcement remains uneven (Khan & Usman, 2023)

Core Challenges to Effective Regulation

Institutional Capacity Deficits

One of the most significant barriers to effective regulation of AI and data protection in developing nations is the lack of institutional capacity. Regulatory bodies tasked with overseeing AI and data protection often face severe resource constraints, both in terms of funding and expertise. The complexity of AI technologies, coupled with the fast pace of innovation, requires regulators to have specialized knowledge and technical proficiency—qualities that many developing countries struggle to provide. In many cases, data protection authorities or regulatory agencies lack the financial and human resources to carry out their mandate effectively. For example, while Kenya has established the ODPC, the office is under-resourced and faces challenges in scaling up its operations to meet the growing demand for regulatory oversight. Similarly, in countries like Pakistan and Nigeria, the regulatory bodies responsible for data protection are not equipped with the technical capabilities to understand and address the nuances of AI systems. This deficit makes it difficult to enforce compliance with existing laws, much less anticipate the new challenges posed by AI technologies, such as algorithmic bias, explainability, and automated decision-making (Khan et al., 2023).

Moreover, the lack of trained personnel capable of evaluating the complexities of AI systems leads to a failure in holding organizations accountable for data breaches, discriminatory algorithms, or misuse of personal data. Without clear regulatory guidance and technical expertise, companies operating in these countries may not be incentivized to adopt responsible data practices or ensure that AI systems are transparent and fair. This capacity gap extends

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

beyond regulatory authorities to include the judicial system. Courts in many developing countries are not well-versed in the intricacies of AI and data protection issues, which complicates the enforcement of rights through litigation. Furthermore, limited access to legal recourse and public awareness of privacy rights exacerbate these issues, as citizens often lack the knowledge and support to challenge violations (Khan, 2023).

Addressing these institutional capacity deficits requires a multi-faceted approach, including increasing investments in training and education for regulators, fostering greater collaboration with international organizations, and creating specialized regulatory bodies capable of handling the unique challenges posed by AI. Additionally, leveraging technology and building technical infrastructure are crucial steps to ensure that regulatory agencies can monitor compliance effectively and respond to violations in a timely manner. Regulatory authorities often lack the resources, expertise, and autonomy to enforce compliance. Oversight bodies, if they exist, are underfunded and politically constrained (Liu et al., 2023).

Legal and Normative Gaps

In many developing nations, the legal frameworks governing data protection and AI are either inadequate or entirely absent, leaving significant gaps in the regulation of AI-driven technologies. These gaps not only undermine the protection of individual privacy but also hinder the responsible development and deployment of AI systems, contributing to ethical and legal risks. At the core of these challenges is the absence of laws that specifically address the unique risks and opportunities presented by AI. While general data protection laws exist in some countries, such as the *Personal Data Protection Bill* in Pakistan or the *NDPR*, these frameworks typically lack provisions tailored to AI-related issues, including algorithmic transparency, the accountability of automated decision-making systems, and the prevention of algorithmic bias. The evolving nature of AI technologies, characterized by complex, opaque algorithms and machine learning systems, creates a regulatory lag in which existing laws fail to keep up with the speed and scale of technological advancements (Khan & Ximei, 2022).

Moreover, the normative foundations of AI governance in developing nations are often weak. International norms and best practices, such as those found in the EU's GDPR or the OECD's guidelines on AI, may influence legal reforms, but they are not always directly applicable or sufficient for addressing the local context. In many developing countries, the ethical and cultural implications of AI deployment are underexplored, with limited public discourse on the balance between innovation and rights protection. For instance, in countries like Nigeria or Kenya, while privacy rights are enshrined in national constitutions or regulations, the application of these rights in the face of AI's growing influence remains unclear and insufficiently articulated in law (Khan et al., 2022).

Additionally, the cross-border nature of data flows and AI development further complicates these legal gaps. Developing nations often rely on AI technologies developed in more advanced jurisdictions, meaning that their citizens' data may be processed according to standards that differ significantly from those in their own country. This misalignment creates tensions around data sovereignty, as local regulations struggle to assert authority over data that is being processed abroad or by multinational corporations. The absence of international legal frameworks governing AI also leaves room for inconsistent enforcement and regulation across borders. Furthermore, legal uncertainty around emerging technologies has led to inconsistent enforcement of privacy and data protection rights. Without clear, comprehensive laws to guide the deployment of AI systems, companies and government entities may bypass ethical considerations, prioritizing innovation and economic growth over privacy and fairness. This lack of clarity not only weakens the public's trust in AI systems but also increases the risk of exploitation, discrimination, and human rights violations (Lin & Khan, 2021).

In addressing these legal and normative gaps, it is crucial for developing nations to create context-specific regulations that incorporate both international best practices and local realities. This should include clear guidelines for AI deployment, ensuring transparency,

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

accountability, and fairness. Additionally, creating robust public consultation processes and fostering multi-stakeholder dialogues can help to shape laws that are both innovative and rights-respecting. Such reforms are essential to ensuring that AI contributes positively to development without compromising fundamental privacy rights. Many legal frameworks fail to define AI systems, automated decision-making, or algorithmic accountability. There is a lack of legal clarity on issues like data minimization, purpose limitation, and consent in automated environments (Khan, 2022).

Technological Asymmetry and Digital Colonialism

A critical challenge in the regulation of AI in developing nations is the deepening technological asymmetry between the Global South and the more technologically advanced Global North. This asymmetry is not only reflected in the disparity of resources and technical expertise but also in the unequal power dynamics that shape data flows, AI development, and regulatory practices on a global scale. In this context, developing nations often find themselves in a vulnerable position, where they rely on technologies designed, developed, and controlled by multinational corporations headquartered in the Global North. This phenomenon can be understood through the concept of digital colonialism, which describes the ways in which global power imbalances are perpetuated through digital technologies, especially AI. In a world where data has become a new form of capital, multinational companies and foreign governments hold disproportionate control over personal data collected from developing nations. This creates a situation where these countries are, in effect, the "data providers" to more developed countries that control the infrastructure, algorithms, and platforms through which data is processed, analyzed, and monetized. Developing nations, often with limited regulatory capacity, are not only unable to protect the data of their citizens effectively but also lack the means to ensure that AI technologies deployed in their contexts are ethically designed and implemented (Khan & Wu, 2021).

The digital divide in AI is driven by several factors. First, the unequal distribution of technological infrastructure means that developing nations often rely on foreign technology providers for AI solutions, ranging from cloud computing services to surveillance systems. This reliance increases the risk that these technologies will be implemented with little regard for local norms, values, or privacy rights. In many cases, foreign firms may not be subject to the same legal constraints as local governments, which exacerbates privacy violations and undermines the agency of national regulators (Abdelrehim Hammad et al., 2021).

Second, there is a lack of local capacity in AI research and development, which limits the ability of developing nations to create homegrown technologies that align with their societal needs and regulatory frameworks. This technological dependency means that AI systems in use across public and private sectors in these countries are often developed with minimal input from local stakeholders and may operate based on frameworks that prioritize profit, efficiency, or political interests over human rights and ethical considerations. Moreover, the data extraction practices of multinational tech companies can also be seen as a form of modern colonialism. Developing nations, especially those rich in natural resources, are increasingly becoming sources of valuable data that are extracted by foreign companies for economic gain. While the data generated by citizens in these countries powers AI systems that benefit global markets, the benefits of AI advancements rarely flow back into local economies in a meaningful or equitable way. This results in an exploitative cycle where developing nations provide vast amounts of data but are left with little control over its use or the economic value derived from it (Khan et al., 2021).

In addition to the economic and technological consequences, digital colonialism also has profound ethical implications. AI systems deployed in developing countries without proper safeguards or regulatory oversight can exacerbate existing inequalities, leading to discriminatory practices. For example, AI-powered systems in law enforcement or financial services may unintentionally reinforce racial, ethnic, or socio-economic biases if they are not

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

designed with local cultural sensitivities in mind. This raises fundamental questions about the role of AI in perpetuating systemic injustice, particularly in post-colonial contexts where historical inequalities continue to influence societal structures. To address these issues, developing nations must push for greater digital sovereignty, ensuring that they have more control over their own data and AI technologies. This includes implementing stronger data protection laws, fostering local innovation in AI, and creating frameworks for international collaboration that do not leave developing nations at the mercy of multinational corporations. Digital colonialism can be resisted through the establishment of equitable partnerships, where technological development is not only driven by the interests of the Global North but also reflects the needs, values, and aspirations of developing nations. Developing nations often rely on imported AI systems developed in jurisdictions with different privacy norms. This leads to the imposition of foreign data practices, sometimes described as "digital colonialism," undermining sovereignty and local accountability (Khan et al., 2020).

Socioeconomic Disparities and Low Public Awareness

Socioeconomic disparities and low public awareness significantly contribute to the challenges of regulating AI and ensuring data protection in developing nations. In these countries, widespread poverty, limited access to education, and inadequate digital infrastructure create an environment where the majority of the population remains disconnected from ongoing debates on AI ethics, data privacy, and technological regulation. This lack of awareness, combined with socioeconomic inequality, exacerbates the vulnerability of individuals to AI-driven harms, such as privacy violations, surveillance, and algorithmic discrimination. First, the digital divide in developing nations means that many citizens do not have access to the internet, smartphones, or computers, which severely limits their ability to engage with or even understand digital technologies. Even among those who do have access, internet speeds, hardware limitations, and inconsistent service make it difficult for large sections of the population to navigate or benefit from the opportunities AI offers. This digital exclusion prevents marginalized communities from accessing information on data protection rights, AI's potential implications, and avenues for redress (Khan et al., 2020).

Second, low levels of digital literacy across much of the population contribute to a fundamental misunderstanding of how personal data is collected, processed, and utilized by AI systems. Without basic knowledge of privacy risks or an understanding of the mechanics of AI algorithms, many individuals unknowingly accept terms and conditions that expose them to extensive data harvesting or surveillance. For instance, in several developing nations, users routinely consent to data collection practices embedded within AI-powered social media platforms or mobile apps without fully understanding the long-term implications for their privacy. The low level of awareness among the public means that individuals often lack the ability to challenge data misuse, hold companies accountable, or demand transparent practices from AI developers. Furthermore, socioeconomic disparities create an environment where the most vulnerable groups—such as the poor, rural populations, or those from marginalized social groups—are disproportionately affected by the rapid adoption of AI technologies. These groups are more likely to be subjected to algorithmic biases in areas such as credit scoring, job recruitment, and law enforcement, where AI systems may inadvertently reinforce existing social inequalities. For instance, AI-driven hiring algorithms may prioritize candidates from certain educational backgrounds or geographic regions, inadvertently excluding those who may not have had access to the same opportunities due to socioeconomic factors. Similarly, AI-powered surveillance tools used for law enforcement may disproportionately target low-income neighborhoods, leading to heightened racial or economic profiling (Kahn & Wu, 2020).

Moreover, because AI technologies are often developed and implemented by foreign corporations, local knowledge and cultural sensitivity are frequently overlooked. AI systems may fail to understand local contexts, languages, and cultural nuances, leading to discriminatory or ineffective outcomes that exacerbate existing inequalities. For instance, facial

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

recognition software may be less accurate for individuals from certain racial or ethnic groups, leading to false positives or discriminatory outcomes, particularly in developing countries where AI models are trained primarily on data from the Global North. The lack of comprehensive public engagement further compounds these issues. Governments and regulators in developing nations often fail to engage with civil society, technology experts, and affected communities when crafting AI laws or data protection regulations. This lack of inclusivity in the policy-making process results in regulations that do not address the needs or concerns of the most affected populations. It also hinders the development of legal frameworks that are well-suited to local contexts and realities (Faisal & Gul, 2025).

To bridge these gaps, it is essential to prioritize digital literacy and awareness campaigns that educate the public about the risks and benefits of AI. By investing in digital education, governments can empower individuals to make informed decisions about their data and technological interactions. Additionally, fostering inclusive policy-making processes, where vulnerable communities are given a platform to voice their concerns, is crucial for creating equitable AI regulations. Efforts to narrow the socioeconomic divide must also include improving access to technology, ensuring that marginalized groups are not left behind in the digital age. In conclusion, socioeconomic disparities and low public awareness must be tackled in tandem with regulatory reforms to ensure that AI technologies are implemented responsibly, ethically, and equitably. Without addressing these foundational issues, the risks of data exploitation, surveillance, and inequality will continue to grow, leaving developing nations vulnerable to the unchecked rise of AI. Public understanding of data rights and AI risks is limited, and marginalized communities are disproportionately affected. This creates asymmetries in both awareness and the ability to seek redress (Ahmed et al., 2025).

International Law and Soft Law Instruments

in addressing the regulatory challenges of AI and data protection in developing nations, international law and soft law instruments play a pivotal role in shaping the regulatory landscape. While binding international treaties or conventions directly addressing AI are still in their nascent stages, soft law instruments, such as guidelines, principles, and recommendations, have emerged as crucial tools in guiding the development of national laws and frameworks. For developing nations, international legal frameworks and soft law instruments offer both a source of inspiration and a means to foster international cooperation on AI governance, while also promoting human rights and ethical standards (Malik & Gul, 2024).

The Role of International Law

International law, though slow to catch up with the rapid evolution of AI technologies, is gradually addressing the need for global norms and standards in the digital age. Instruments such as the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990) and the OECD Principles on Artificial Intelligence (2019) provide a foundational basis for integrating human rights into AI governance. These international frameworks, while non-binding, help shape the discourse around AI ethics and data protection, serving as blueprints for national legislations. The UN Declaration on Human Rights and its subsequent covenants underscore the importance of privacy, freedom of expression, and non-discrimination, principles which must be safeguarded as AI technologies proliferate. These international legal principles provide the backbone for developing nations to assert their regulatory authority over AI and data protection, ensuring that AI deployment does not infringe on fundamental human rights (Gul & Malik, 2024).

In the absence of a comprehensive international treaty on AI, regional initiatives are also becoming increasingly important. For example, the European Union's GDPR has set a high standard for data protection and serves as a de facto model for countries around the world, including those in the Global South. While it is a binding legal instrument for EU member states, its extraterritorial reach has led to its adoption as a benchmark for data protection in

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

non-EU countries. Countries like Brazil, which have adopted the LGPD, have drawn heavily from the GDPR to inform their own legal frameworks, signaling the growing influence of international law in shaping domestic AI and data protection policies (Ishii, 2019).

Soft Law Instruments and Their Impact

Soft law instruments, such as the OECD's AI Principles, the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, and the GAC's Beijing AI Principles, play a critical role in providing guidance on ethical AI development and deployment. These non-binding documents are crucial in establishing a shared understanding of what constitutes ethical AI and offer developing nations a framework to align their national regulations with international best practices. For example, the OECD's AI Principles emphasize transparency, accountability, and fairness, which are key concerns for developing countries that may lack the technical expertise or infrastructure to monitor AI systems effectively. These principles encourage member countries, including those in the Global South, to adopt regulatory frameworks that promote the responsible development of AI technologies while safeguarding human rights. Soft law instruments can also facilitate international collaboration, allowing countries to share best practices, research, and regulatory experiences in the fast-evolving AI landscape. Initiatives such as the Global Partnership on AI (GPAI), which brings together governments, academia, and industry to promote responsible AI development, provide a platform for developing nations to collaborate with more technologically advanced countries and ensure that their voices are heard in the formulation of global AI standards (Alemany & Gurumurthy, 2019).

Challenges and Limitations

While international law and soft law instruments are instrumental in fostering global norms and best practices, they face significant limitations in ensuring enforcement and addressing the specific needs of developing nations. Unlike binding treaties, soft law lacks the force of law and may be ignored or poorly implemented by states. Furthermore, the emphasis of international norms on human rights and privacy protection may not always align with the economic or political priorities of developing nations, which may face pressure to prioritize technological development or economic growth over regulatory concerns. Moreover, developing nations often lack the political will or resources to fully implement international standards or to negotiate treaties that protect their digital sovereignty. The asymmetry in technological power between the Global North and Global South means that developing countries may struggle to assert their interests in global forums or may find themselves bound by agreements that do not adequately address their unique regulatory challenges (Alic, 2021).

To bridge the gap between international and domestic AI regulation, developing countries must actively engage with international legal and normative frameworks while also tailoring them to their local context. International law can serve as a guide, but it should not be viewed as a one-size-fits-all solution. Instead, developing nations should advocate for greater inclusivity in international negotiations, ensuring that the voices of underrepresented countries are heard and that their specific challenges—such as technological asymmetry and limited regulatory capacity—are addressed in global AI governance. By harmonizing international norms with domestic legal frameworks, developing nations can create more robust and rights-respecting AI regulations. This approach would foster greater cooperation, improve the enforcement of ethical standards, and ensure that AI technologies contribute to sustainable and inclusive development. Global initiatives such as the OECD AI Principles, UNESCO's Recommendation on the Ethics of AI, and the Council of Europe's Convention 108+ provide guiding frameworks. However, their non-binding nature limits enforcement. Developing countries must navigate these frameworks while asserting their regulatory autonomy and prioritizing contextual needs (Ijaiya & Odumuwagun, 2021).

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

Toward a Rights-Based and Contextual Framework

Establishing Robust Data Protection Laws

To effectively regulate AI and safeguard data privacy, developing nations must prioritize the establishment of comprehensive and robust data protection laws. These laws should be designed to address the unique challenges posed by AI technologies, including data mining, algorithmic transparency, and the risks of automated decision-making. By adopting frameworks similar to the GDPR, countries can set clear standards for data collection, consent, storage, and processing, ensuring that individuals' privacy rights are protected while enabling responsible AI innovation. Additionally, these laws should mandate strong enforcement mechanisms, independent oversight bodies, and mechanisms for redress, empowering citizens to challenge violations and hold organizations accountable. Implementing data protection laws that reflect local realities while aligning with international best practices will not only strengthen privacy rights but also foster public trust in AI systems, enabling these nations to navigate the digital age with greater security and confidence. A foundational step involves enacting and updating data protection laws to cover AI-specific risks. These should include provisions on algorithmic transparency, data subject rights, and impact assessments (Alazzam & Aldrou, 2025).

Building Regulatory and Technical Capacity

Building regulatory and technical capacity is crucial for developing nations to effectively manage AI technologies and enforce data protection laws. This requires investment in training and upskilling government regulators, legal professionals, and technical experts to understand the complexities of AI systems and data privacy issues. Establishing specialized AI regulatory bodies and fostering collaboration between governments, academia, and the private sector can help ensure that AI innovations are effectively monitored and assessed for ethical compliance. Additionally, governments should invest in the development of local AI expertise, promoting research and development initiatives that allow for the creation of context-specific solutions that reflect national priorities and values. Strengthening these regulatory and technical capacities not only ensures that AI deployment is responsible but also enhances the ability of developing nations to engage in global AI governance and safeguard their digital sovereignty. Governments should invest in capacity-building for regulatory bodies, establish independent data protection authorities, and foster cooperation with civil society and academia (Sharma, 2024).

Ensuring Algorithmic Transparency and Accountability

Ensuring algorithmic transparency and accountability is essential for mitigating the risks associated with AI in developing nations. Governments must implement regulations that require AI systems, especially those used in critical sectors like healthcare, finance, and law enforcement, to be transparent in their decision-making processes. This includes mandating that AI developers provide clear documentation about the underlying algorithms, data used, and the rationale behind automated decisions. Additionally, it is crucial to establish mechanisms for accountability, such as independent audits and public reporting, to ensure that AI systems are not only effective but also fair, non-discriminatory, and aligned with human rights principles. By prioritizing transparency and accountability, developing nations can build public trust in AI technologies while reducing the risk of harm from biased or opaque decision-making processes. Mandating explainability, fairness audits, and redress mechanisms is essential. Developing countries can learn from the EU's AI Act while tailoring obligations to local capacities (De Almeida et al., 2021).

Promoting Inclusive and Participatory Policymaking

Promoting inclusive and participatory policymaking is vital for creating AI regulations that are equitable and reflect the needs of diverse populations in developing nations. To ensure that AI technologies benefit all sectors of society, policymakers must actively involve a wide range of stakeholders—such as civil society organizations, local communities, technology experts, and marginalized groups—in the decision-making process. This approach fosters a more holistic

Vol. 3 No. 5 (2025)

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

understanding of the potential impacts of AI on different segments of the population and ensures that the voices of those most affected, particularly vulnerable or underserved communities, are heard. By incorporating diverse perspectives, developing nations can create more effective and context-specific AI policies that not only protect individuals' rights but also drive innovation in ways that promote social and economic inclusion. Inclusive policymaking also helps build public trust, ensuring that AI systems are deployed responsibly and in a manner that aligns with the values and priorities of society as a whole. Law-making should involve public consultations, especially with affected communities, to ensure that AI governance frameworks reflect diverse perspectives and uphold digital rights (Mbah, 2024).

Conclusion

The regulation of AI in developing nations is a complex and urgent issue that intersects with data protection, privacy rights, and socio-economic development. As AI technologies continue to evolve rapidly, these countries face significant challenges in ensuring that the benefits of AI are realized while minimizing the risks to privacy, equality, and human rights. Through the establishment of robust legal frameworks, the strengthening of technical and regulatory capacities, and the promotion of transparent, accountable AI systems, developing nations can navigate these challenges and harness the potential of AI for inclusive development. Key findings suggest that international cooperation, as well as the integration of local needs and cultural contexts into regulatory frameworks, are essential for ensuring the ethical deployment of AI. Moreover, it is critical to address the digital divide, raise public awareness, and empower citizens with the knowledge to navigate the AI landscape responsibly. As this research highlights, the path forward for developing nations requires a multi-pronged approach: from improving legal structures to investing in education and fostering public-private collaboration.

Looking ahead, future research should focus on exploring the impact of AI on marginalized groups, the development of AI models tailored to local contexts, and the challenges of enforcing data protection laws in the face of globalized, cross-border data flows. Additionally, further studies could examine the role of international institutions in shaping AI regulations and promoting digital sovereignty in the Global South. Ultimately, the way developing nations approach AI regulation will have profound implications for the future of global governance, digital rights, and sustainable development. It is crucial that these nations remain proactive and collaborative in shaping the future of AI in a way that protects human dignity and ensures equitable growth for all. AI offers transformative potential for developing nations, but without robust legal safeguards, it risks entrenching inequalities and violating fundamental rights. By adopting a rights-based, locally adapted approach to AI governance, developing nations can ensure that technological advancement does not come at the cost of privacy and human dignity. Regional cooperation, capacity-building, and the harmonization of standards will be key to fostering ethical AI ecosystems in the Global South.

References

Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital Economy Barriers to Trade Regulation Status, Challenges, and China's Response. *International Journal of Social Sciences Perspectives*, *8*(2), 41-49.

Ahmed, F. A., Zafar, S., & Gul, S. (2025). Analyzing PECA Amendments: Press Freedom, Democratic Values, and Digital Regulation in Pakistan. *Traditional Journal of Law and Social Sciences*, *4*(01), 41-51.

Alazzam, F. A. F., & Aldrou, K. K. A. R. (2025). Artificial intelligence and data privacy in international trade law. *Multidisciplinary Science Journal*, *7*(8), 2025379-2025379.

Alemany, C., & Gurumurthy, A. (2019). Governance of data and artificial intelligence. *Reshaping*, 86.

Alic, D. (2021). The Role of Data Protection and Cybersecurity Regulations in Artificial Intelligence Global Governance: A Comparative Analysis of the European Union, the

United States, and China Regulatory Framework. *Central European University Thesis Repository*.

De Almeida, P. G. R., dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: a framework for governance. *Ethics and Information Technology*, *23*(3), 505-525.

Faisal, S. M., & Gul, S. (2025). From Margins to the Mainstream: Evaluating the Impact of the 26th Amendment on Democratic Governance in Pakistan. *The Journal of Research Review*, *2*(02), 95-102.

Gul, S., & Malik, W. (2024). Cyber Conflict and International Security: Legal Challenges and Strategic Solutions in Cyberspace. *The Journal of Research Review*, *1*(04), 305-314.

Hasan, M. (2024). Regulating artificial intelligence: A study in the comparison between South Asia and other countries. *Legal Issues in the digital Age*, (1), 122-149.

Ijaiya, H., & Odumuwagun, O. O. (2021). Advancing Artificial Intelligence and Safeguarding Data Privacy: A Comparative Study of EU and US Regulatory Frameworks Amid Emerging Cyber Threats.

Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI & society*, *34*, 509-533.

Kahn, A., & Wu, X. (2020). Impact of digital economy on intellectual property law. *J. Pol. & L.*, *13*, 117.

Khan, A. (2022). E-commerce Regulations in Emerging Era: The Role of WTO for Resolving the Complexities of Electronic Trade. *ASR Chiang Mai University Journal Of Social Sciences And Humanities*.

Khan, A. (2023). Rules on Digital Trade in the Light of WTO Agreements. *PhD Law Dissertation, School of Law, Zhengzhou University China*.

Khan, A. (2024). The Emergence of the Fourth Industrial Revolution and its Impact on International Trade. *ASR: CMU Journal of Social Sciences and Humanities (2024) Vol*, *11*.

Khan, A. (2024). The Intersection Of Artificial Intelligence And International Trade Laws: Challenges And Opportunities. *IIUMLJ*, *32*, 103.

Khan, A., & Jiliani, M. A. H. S. (2023). Expanding The Boundaries Of Jurisprudence In The Era Of Technological Advancements. *IIUMLJ*, *31*, 393.

Khan, A., & Ullah, M. (2024). The Pakistan-China FTA: legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, *11*, 1478669.

Khan, A., & Usman, M. (2023). The Effectiveness of International Law: A Comparative Analysis. *International Journal of Contemporary Issues in Social Sciences*, *2*(3), 780-786.

Khan, A., & Wu, X. (2021). Bridging the Digital Divide in the Digital Economy with Reference to Intellectual Property. *Journal of Law and Political Sciences*, *28*(03), 256-263.

Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do Information Communication and Technology (ICT) and economic complexity matter?. *International journal of environmental research and public health*, *19*(19), 12301.

Khan, A., Amjad, S., & Usman, M. (2020). The Role of Customary International Law in Contemporary International Relations. *International Review of Social Sciences*, *8*(08), 259-265.

Khan, A., Jillani, M. A. H. S., Abdelrehim Hammad, A. A., & Soomro, N. E. H. (2021). Plurilateral negotiation of WTO E-commerce in the context of digital economy: Recent issues and developments. *Journal of Law and Political Sciences*.

Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, *28*(2), 408-423.

Khan, A., Usman, M., & Amjad, S. (2020). Enforcing Economic, Social, and Cultural Rights: A Global Imperative. *International Review of Social Sciences (IRSS)*, *8*(09).

Journal of Social Signs Review

Online ISSN 3006-4651

Print ISSN 3006-466X

Khan, A., Usman, M., & Amjad, S. (2023). The digital age legal revolution: taped's trailblazing influence. *International journal of contemporary issues in social sciences*, *2*(4), 524-535.

KHAN, M. I., Usman, M., KANWEL, S., & Khan, A. (2022). Digital Renaissance: Navigating the Intersection of the Digital Economy and WTO in the 21st Century Global Trade Landscape. *Asian Social Studies and Applied Research (ASSAR)*, *3*(2), 496-505.

Lin, S., & Khan, A. (2021). The Concept of E-sports in Digital Era: A Case Study of China.

Lin, S., & Song, Y. (2024). Upholding human rights in mega sports: A study of governance practices within the IOC and FIFA through the lens of the Ruggie Principle. *Heliyon*, *10*(16).

Liu, X., Khan, M., & Khan, A. (2023). The Law and Practice of Global ICT Standardization by Olia Kanevskaia [CUP, Cambridge, 2023, xxvi+ 361pp, ISBN: 978-1-0093-00575,£ 95.00 (h/bk)]. *International & Comparative Law Quarterly*, *72*(4), 1094-1097.

Malik, W., & Gul, S. (2024). Bridging the Gap: Exploring the Intersection of Cybersecurity and Human Security in the Digital Age. *Competitive Research Journal Archive*, *2*(04), 195-202.

Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses.

Puertas-Bravo, L., Pineda, L. O., & Piedra, N. (2024). Regulation of Artificial Intelligence: Challenges and Perspectives in the Andean Community. *Knowledge Management and Artificial Intelligence for Growth: Cases from Emerging and Developed Economies*, 221-244.

Sharma, A. K. (2024). Comparative Analysis of Data Protection Laws and.

Sharma, A. K., & Sharma, R. (2024). Comparative Analysis of Data Protection Laws and ai Privacy Risks in brics Nations: A Comprehensive Examination. *Global Journal of Comparative Law*, *13*(1), 56-85.

Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in data protection and artificial intelligence: Trends and challenges. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 294-319.