International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 14 Issue 4, July-August, 2026

Digital Rights and Data Privacy of Diaspora Communities: Legal Challenges in the Digital Age

Dr. Gizala Hashmi

Assistant Professor, Sarvadharm Law College Gwalior, Todi Bazaar, Near Ganesh Mandir Sheopur, Madhya Pradesh

ABSTRACT

This review article aims to examine the legal dimensions of digital rights and data privacy affecting diaspora communities by analyzing international human rights instruments, regional data protection regulations, and selected national legal frameworks. The study also seeks to identify emerging legal challenges arising from artificial intelligence, biometric technologies, digital identity systems, and transnational data governance while proposing policy measures to strengthen privacy protection in the digital age. The study adopts a qualitative review methodology based on an extensive analysis of peer-reviewed journal articles, books, international conventions, policy reports, legislative documents, and publications from organizations such as the United Nations, the Organisation for Economic Co-operation and Development (OECD), UNESCO, and the European Union. The literature is synthesized thematically to evaluate existing legal frameworks, identify recurring issues, and highlight gaps in current scholarship. The review finds that although instruments such as the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection Act, 2023 provide important safeguards, significant legal inconsistencies remain in regulating cross-border data flows, digital surveillance, and platform accountability. Existing scholarship has paid limited attention to the specific vulnerabilities of diaspora communities within digital governance frameworks. The article argues for stronger international cooperation, harmonization of privacy standards, enhanced transparency in artificial intelligence governance, and diaspora-inclusive policy frameworks to ensure that digital rights are effectively protected across jurisdictions.

Keywords: Digital Rights; Data Privacy; Diaspora Communities; Cross-border Data Governance; Digital Personal Data Protection; GDPR; Artificial Intelligence.

INTRODUCTION

Background

The twenty-first century has witnessed an unprecedented increase in global migration, resulting in the formation of diverse and interconnected diaspora communities across the world. According to international migration estimates, hundreds of millions of people now reside outside their countries of birth, maintaining strong social, economic, cultural, and political ties with their homelands through digital technologies. The rapid expansion of the internet, cloud computing, artificial intelligence (AI), mobile communication, and social media platforms has transformed the ways in which diaspora populations communicate, participate in civic life, conduct financial transactions, and preserve their cultural identities. These technological advancements have enabled individuals to transcend geographical boundaries, fostering continuous interaction between migrants and their countries of origin[1].The digital transformation of societies has also contributed to the emergence of **digital citizenship**, a concept that recognizes individuals' ability to participate in economic, political, and social activities through digital platforms irrespective of geographical location. Digital citizenship extends beyond access to technology and encompasses digital rights, online participation, digital literacy, privacy protection, and responsible use of information and communication technologies. For diaspora communities, digital citizenship provides opportunities to engage in transnational governance, online education, entrepreneurship, political advocacy, and cultural exchange while strengthening their sense of belonging across multiple jurisdictions[2-3].

Alongside digital citizenship, **online identity** has become an essential component of personal and social existence. Digital identities now include social media profiles, biometric information, financial records, health data, communication histories, geolocation information, and government-issued digital credentials. These digital identities facilitate access to banking services, immigration procedures, employment opportunities, healthcare, education, and public services. However, the increasing dependence on digital identity systems has also expanded the collection,

storage, and processing of personal information by governments, multinational corporations, financial institutions, and technology companies. Consequently, protecting digital rights and ensuring effective data privacy have become critical concerns for individuals whose lives span multiple legal jurisdictions[4].

Research Problem

A significant concern is the absence of comprehensive international mechanisms specifically addressing the protection of migrant and diaspora data. Existing human rights instruments recognize the right to privacy, yet they provide limited guidance on digital governance in an increasingly interconnected world. Government surveillance programs, extensive data collection by digital platforms, algorithmic profiling, and commercial exploitation of personal information further complicate the protection of digital rights. Technology companies often process vast amounts of user data across multiple countries without ensuring consistent transparency or accountability. Consequently, the intersection of migration, digital technology, and international data governance remains an important but underexplored area of legal scholarship[5].

Research Objectives

a) To examine the concept and scope of digital rights and data privacy in relation to diaspora communities.
b) To review international human rights instruments, regional regulations, and national legal frameworks governing digital privacy.
c) To analyze the legal challenges associated with cross-border data governance, digital surveillance, identity theft, artificial intelligence, and platform accountability.
d) To identify gaps in existing legal and policy frameworks affecting diaspora populations.
e) To propose policy recommendations for strengthening international cooperation and enhancing the protection of digital rights in the digital age.

CONCEPTUAL FRAMEWORK

Digital Rights

One of the most fundamental digital rights is the right to privacy, which protects individuals from unlawful or arbitrary interference with their personal information, communications, and online activities. In the digital age, privacy encompasses the collection, storage, processing, and transfer of personal data by governments, private corporations, and digital platforms. Effective privacy protection enables individuals to maintain control over their personal information while reducing risks associated with surveillance, identity theft, and unauthorized data sharing[6].

Another essential component of digital rights is freedom of expression, which guarantees the ability to seek, receive, and disseminate information through digital media without undue censorship or intimidation. Social networking platforms, online forums, and digital communication tools enable diaspora communities to participate in political discussions, maintain cultural identities, and engage in democratic processes across national borders[7]. However, online censorship, misinformation, and algorithmic content moderation may restrict this freedom.

Access to the internet has increasingly been recognized as a prerequisite for exercising numerous economic, educational, and social rights. Reliable internet connectivity enables individuals to access government services, educational resources, healthcare information, employment opportunities, financial services, and digital communication. For diaspora communities, internet access is essential for maintaining relationships with families, participating in transnational business activities, and preserving cultural and linguistic identities[8].

Diaspora Communities

The term migrants generally refers to individuals who voluntarily relocate across national borders for purposes such as employment, education, family reunification, or improved living conditions. Migrants often rely extensively on digital platforms for communication, remittances, legal documentation, and employment opportunities.

Refugees are individuals who have been compelled to leave their home countries because of armed conflict, persecution, violence, or serious human rights violations. Digital technologies play a critical role in facilitating access to humanitarian assistance, legal protection, identity verification, and communication with family members. At the same time, refugees face heightened risks of surveillance, data misuse, and digital exclusion[9].

Overseas citizens are nationals who permanently or temporarily reside outside their country while retaining legal or constitutional ties with their homeland. Many countries provide overseas citizens with voting rights, consular assistance, digital identity services, and access to government portals that require the processing of sensitive personal information across jurisdictions[10].

Transnational communities comprise networks of individuals, families, organizations, and institutions whose social and economic activities extend beyond national boundaries. Through digital technologies, these communities participate in

cross-border entrepreneurship, education, philanthropy, political advocacy, and cultural exchange, creating continuous flows of personal information across multiple legal systems.

Data Privacy
Personal data includes any information capable of identifying an individual directly or indirectly, such as names, addresses, identification numbers, email addresses, telephone numbers, online identifiers, location data, and internet protocol (IP) addresses. As digital interactions expand, the volume and diversity of personal data generated by individuals continue to increase[11].

A subset of personal data comprises sensitive information, including biometric identifiers, genetic information, health records, financial information, religious beliefs, political opinions, racial or ethnic origin, and sexual orientation. Because misuse of such information may result in discrimination, financial harm, or violations of fundamental rights, many legal systems impose stricter safeguards for its processing.

A fundamental principle of modern privacy law is consent, which requires organizations to obtain informed, specific, freely given, and unambiguous permission before collecting or processing personal information. Consent mechanisms strengthen individual autonomy and promote transparency in digital transactions[12].

Data processing encompasses all operations performed on personal information, including collection, recording, storage, organization, retrieval, analysis, sharing, transfer, and deletion. Effective regulation requires organizations to process data lawfully, fairly, and only for legitimate and specified purposes.

Collectively, these concepts form the analytical foundation for examining how legal frameworks can better protect the digital rights and data privacy of diaspora communities in an increasingly interconnected and data-driven world.

THEORETICAL FRAMEWORK

The protection of digital rights and data privacy for diaspora communities is an interdisciplinary issue situated at the intersection of human rights law, information governance, migration studies, and digital technology. Understanding the legal and ethical implications of cross-border data flows requires a theoretical framework that explains how individual rights, state authority, technological advancement, and global digital networks interact. This review adopts four complementary theoretical perspectives—Human Rights Theory, Information Privacy Theory, Surveillance Theory, and Network Society Theory—to examine the challenges and opportunities associated with digital governance in the digital age[13].

Human Rights Theory
Human Rights Theory provides the primary normative foundation for understanding digital rights as an extension of universally recognized human rights. Rooted in the principles of human dignity, equality, liberty, and justice, the theory maintains that every individual possesses inherent rights that must be respected and protected irrespective of nationality, residence, or legal status. The Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966) recognize the rights to privacy, freedom of expression, access to information, and protection from arbitrary interference in personal life. These rights remain equally applicable within digital environments.

Information Privacy Theory
Information Privacy Theory focuses on the individual's ability to control the collection, use, storage, and dissemination of personal information. The theory argues that privacy is fundamentally linked to autonomy, dignity, and informed decision-making. Rather than viewing privacy merely as secrecy, it emphasizes that individuals should have meaningful control over how their personal data are processed by governments, corporations, and digital platforms[14].
In contemporary digital ecosystems, enormous volumes of personal information are generated through social media interactions, financial transactions, online communication, biometric authentication, and cloud-based services. Diaspora communities routinely exchange personal data across multiple jurisdictions while accessing immigration services, remittance systems, digital banking, healthcare, education, and government portals. Consequently, maintaining effective control over personal information has become increasingly difficult.

INTERNATIONAL LEGAL FRAMEWORK

The rapid digitalization of global society has fundamentally transformed the protection of privacy and personal data, particularly for diaspora communities whose digital interactions routinely transcend national borders. While technological advancements have enhanced communication, mobility, and economic participation, they have also intensified concerns regarding cross-border data transfers, digital surveillance, identity theft, and unauthorized processing of personal information. In response, several international legal instruments and policy frameworks have established principles governing privacy, data protection, and digital rights. Although these frameworks differ in their legal status and enforcement mechanisms, collectively they provide the normative foundation for protecting individuals

in the digital age[15]. This section reviews the principal international legal instruments relevant to the digital rights and data privacy of diaspora communities.

Universal Declaration of Human Rights (1948)
The **Universal Declaration of Human Rights (UDHR)**, adopted by the United Nations General Assembly in 1948, remains the cornerstone of the international human rights framework. Although drafted before the emergence of the internet and digital technologies, its principles continue to guide contemporary interpretations of digital rights and data protection.

Article 12 of the UDHR provides that:
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

This provision establishes privacy as a universal human right applicable to all individuals regardless of nationality or residence. In the digital era, the concept of "correspondence" has been broadly interpreted to include electronic communications such as emails, instant messaging, social media interactions, cloud-based communication, and digital records[16].

For diaspora communities, Article 12 has particular significance because cross-border communication often involves the exchange of sensitive personal information through digital platforms. Protecting these communications against unlawful interception, unauthorized surveillance, and arbitrary government interference remains essential for safeguarding individual autonomy, family life, and freedom of association. Although the UDHR itself is not legally binding, it has profoundly influenced subsequent international treaties and domestic constitutional protections relating to digital privacy.

International Covenant on Civil and Political Rights (ICCPR)
The **International Covenant on Civil and Political Rights (ICCPR)**, adopted in 1966 and entering into force in 1976, transformed many principles contained in the UDHR into legally binding obligations for State Parties. The Covenant is widely regarded as one of the most important international human rights treaties governing civil liberties in both physical and digital environments.

Article 17 of the ICCPR provides that:
"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."

Unlike the UDHR, the ICCPR imposes legally enforceable obligations requiring States to prevent unlawful or arbitrary interference with individual privacy. Governments are expected to enact legislation, establish judicial remedies, and provide effective oversight mechanisms to ensure compliance with privacy protections.

European Union General Data Protection Regulation (GDPR)
The **General Data Protection Regulation (GDPR)**, which became applicable in 2018, represents the world's most comprehensive and influential legal framework governing personal data protection. Although enacted by the European Union, its extraterritorial application extends to organizations processing the personal data of individuals located within the European Economic Area, making it highly relevant for multinational corporations and cross-border digital services. The GDPR is founded upon principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles significantly influence contemporary privacy legislation across the world.

One of the Regulation's most important provisions concerns **informed consent**. Organizations must obtain freely given, specific, informed, and unambiguous consent before collecting or processing personal information, except where another lawful basis applies. Individuals must also retain the right to withdraw consent at any time.

Another significant safeguard is the **Right to Erasure**, commonly referred to as the "Right to be Forgotten." Under specified circumstances, individuals may request the deletion of personal information that is no longer necessary, has been unlawfully processed, or infringes their privacy rights. This provision allows individuals greater control over their digital footprint and online reputation.

The GDPR also establishes the **Right to Data Portability**, enabling individuals to receive their personal data in a structured, commonly used, and machine-readable format and transfer those data to another service provider without unnecessary obstacles. This right promotes user autonomy, competition, and interoperability among digital platforms.

United Nations Digital Cooperation Reports

Recognizing the transformative impact of digital technologies, the United Nations established the **High-level Panel on Digital Cooperation**, which produced a series of reports advocating inclusive, secure, and human rights-based approaches to global digital governance[17].

These reports emphasize that digital technologies should promote sustainable development, reduce digital inequalities, strengthen international cooperation, and protect fundamental human rights. Key recommendations include expanding universal internet access, improving digital inclusion, strengthening cybersecurity, promoting trustworthy artificial intelligence, and ensuring effective governance of cross-border data flows.

The reports further stress that governments, international organizations, civil society, academia, and the private sector must collaborate to develop interoperable regulatory frameworks capable of addressing emerging challenges associated with digital transformation. For diaspora communities, these recommendations highlight the necessity of protecting digital participation while ensuring equitable access to digital services across national boundaries.

UNESCO Recommendations

The **United Nations Educational, Scientific and Cultural Organization (UNESCO)** has increasingly recognized the ethical, social, and legal implications of emerging digital technologies. Its recommendations emphasize that technological innovation must remain firmly grounded in human rights, transparency, inclusiveness, and accountability. UNESCO has played a leading role in promoting ethical governance of artificial intelligence, digital literacy, open knowledge, and universal access to information. Its **Recommendation on the Ethics of Artificial Intelligence (2021)** encourages governments to ensure that AI systems respect privacy, protect personal data, prevent discrimination, and remain subject to meaningful human oversight[18].

UNESCO also advocates strengthening digital literacy and public awareness regarding privacy rights, responsible data management, cybersecurity, and ethical technology use. These initiatives are particularly valuable for diaspora communities, who frequently navigate multiple legal systems while relying extensively on digital platforms for communication, education, employment, and civic participation(Table 1-3, Fig 1-3).

Table 1: Global International Migrant Population

Year	International Migrants (Million)
2000	173
2005	191
2010	221
2015	248
2020	281
2024	304

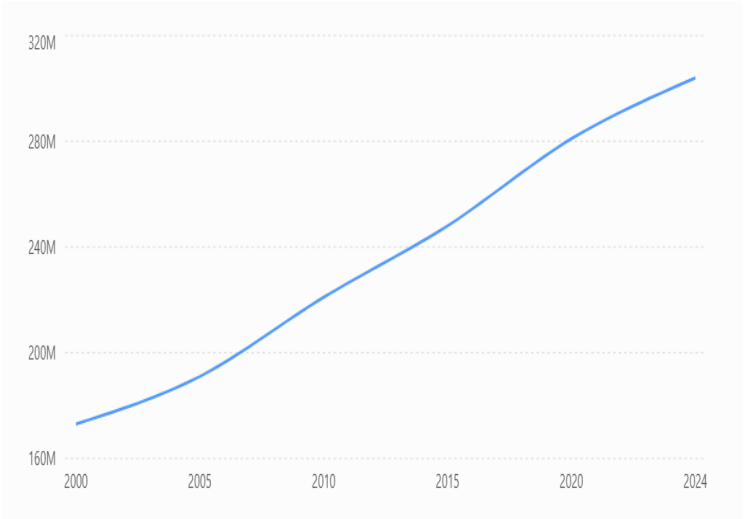


Fig 1: Global International Migrant Population

Table 2: Global Status of Data Protection Legislation

Legislation Status	Number of Countries	Percentage (%)
Comprehensive Data Protection Laws	144	73.8
Partial/Sectoral Data Protection Laws	26	13.3
Draft Data Protection Legislation	16	8.2
No Data Protection Legislation	9	4.6
Total	**195**	**100.0**

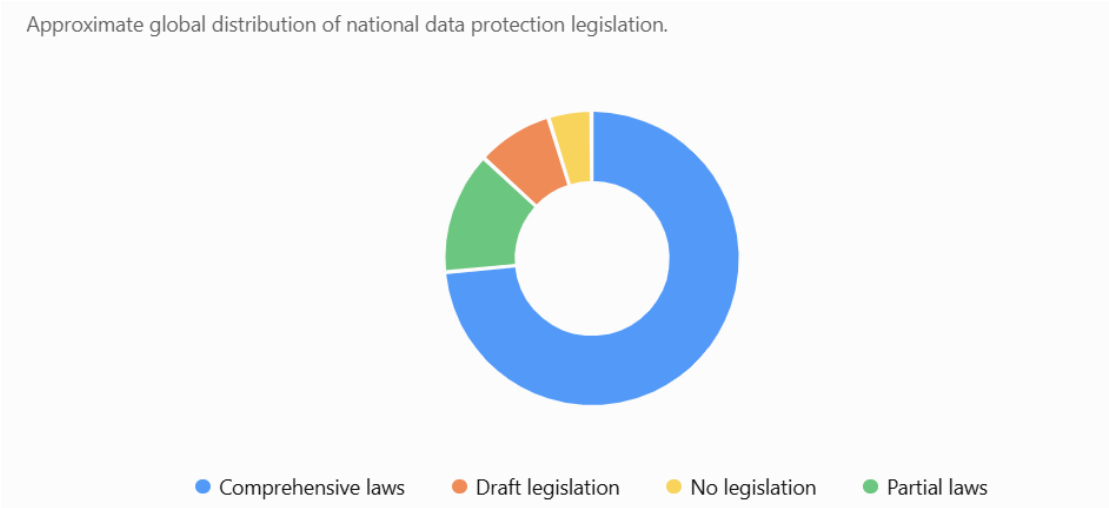


Fig. 2: Countries by Data Protection Legislation Status

Table 3: Reported Global Data Breaches by Sector

Sector	Reported Data Breaches (Approx.)	Share (%)
Healthcare	890	24.2
Finance	760	20.7
Government	620	16.8
Technology	540	14.7
Retail	470	12.8
Education	390	10.6
Total	**3,670**	**100.0**

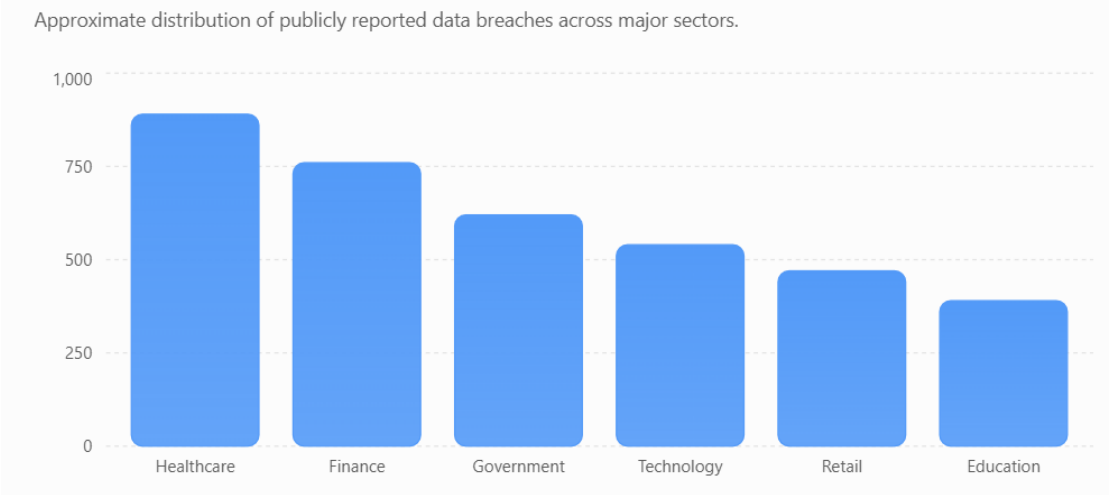


Figure 3: Reported Global Data Breaches by Sector

NATIONAL LEGAL FRAMEWORKS

European Union: General Data Protection Regulation (GDPR)
The **General Data Protection Regulation (GDPR)**, which came into force on 25 May 2018, is widely regarded as the global benchmark for data protection legislation. It applies to both public and private organizations that process the personal data of individuals located within the European Economic Area (EEA), irrespective of where the organization is established. This extraterritorial application makes the GDPR particularly relevant in regulating multinational technology companies and cross-border data processing.

The GDPR is based on several fundamental principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. It grants individuals a comprehensive set of rights, including the right to access personal data, rectify inaccurate information, erase data under specified conditions, restrict processing, object to processing, and transfer personal data between service providers.

United States: California Consumer Privacy Act (CCPA) and Sectoral Privacy Laws
Unlike the European Union, the United States does not have a single comprehensive federal data protection law. Instead, the American privacy framework consists of sector-specific legislation combined with state-level privacy laws that regulate different categories of personal information.

Among these, the **California Consumer Privacy Act (CCPA)**, as amended by the California Privacy Rights Act (CPRA), represents the most comprehensive state privacy legislation. The CCPA grants California residents several important rights, including the right to know what personal information businesses collect, the right to request deletion of personal data, the right to correct inaccurate information, the right to opt out of the sale or sharing of personal data, and protection against discrimination for exercising privacy rights.

At the federal level, privacy regulation remains fragmented. Various statutes govern specific sectors, including the Health Insurance Portability and Accountability Act (HIPAA) for health information, the Gramm-Leach-Bliley Act (GLBA) for financial institutions, the Children's Online Privacy Protection Act (COPPA) for children's data, and the Fair Credit Reporting Act (FCRA) for consumer credit information.

India: Digital Personal Data Protection Act, 2023 and Information Technology Act, 2000
India has undergone significant legal reforms to strengthen its data protection framework. The **Digital Personal Data Protection (DPDP) Act, 2023** establishes a comprehensive legal regime governing the processing of digital personal data while balancing individual privacy with legitimate governmental and business interests[19].

The DPDP Act introduces several important rights for individuals, referred to as Data Principals. These include the right to access information regarding personal data processing, the right to correction and erasure of personal data, the right to grievance redressal, and the right to nominate another person to exercise rights in specified circumstances. The Act requires Data Fiduciaries to process personal data lawfully, for specified purposes, and based on informed consent or other legally recognized grounds.

The legislation also establishes obligations relating to data security, breach notification, accountability, and penalties for non-compliance. While the Act permits cross-border data transfers, the Central Government retains authority to restrict transfers to specific jurisdictions where necessary for national interests.

Before the enactment of the DPDP Act, privacy regulation primarily relied upon the **Information Technology Act, 2000**, particularly Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These provisions imposed obligations upon organizations handling sensitive personal information and required implementation of reasonable security practices.

United Kingdom: UK GDPR
Following its withdrawal from the European Union, the United Kingdom retained much of the GDPR framework through the **UK General Data Protection Regulation (UK GDPR)**, supplemented by the Data Protection Act 2018. The UK GDPR continues to provide comprehensive protection for personal information while adapting certain provisions to the post-Brexit legal environment. The UK GDPR preserves key rights available under the EU GDPR, including the rights of access, rectification, erasure, restriction of processing, objection, and data portability. Organizations must process personal information lawfully, transparently, and only for specified purposes while implementing appropriate technical and organizational security measures[20].

Cross-border transfers of personal data remain subject to safeguards ensuring an adequate level of protection. The Information Commissioner's Office (ICO) serves as the independent supervisory authority responsible for monitoring compliance, investigating complaints, and imposing administrative sanctions where necessary.

Comparative Analysis of National Legal Frameworks

Although all five jurisdictions recognize privacy as an important legal right, they differ significantly in regulatory philosophy, enforcement mechanisms, and approaches to international data governance.(Table 1)

The **European Union** and the **United Kingdom** adopt comprehensive rights-based approaches, emphasizing informed consent, strong regulatory oversight, accountability, and extensive individual rights. The GDPR framework remains the most influential international standard for protecting personal data.

The **United States** follows a decentralized, sector-specific regulatory model in which privacy protections vary according to industry and state legislation. While laws such as the CCPA provide significant consumer rights, the absence of a comprehensive federal privacy statute creates regulatory fragmentation.

India's Digital Personal Data Protection Act, 2023 represents an important step toward comprehensive privacy regulation. However, its implementation and interpretation continue to evolve, particularly regarding government access, cross-border transfers, and institutional oversight.

Canada's PIPEDA adopts a principles-based regulatory approach emphasizing organizational accountability, meaningful consent, and responsible international data transfers. Its flexible framework has influenced privacy legislation in several other jurisdictions.

Table 1: Comparative Analysis of National Data Protection Frameworks

Feature	European Union (GDPR)	United States	India (DPDP Act, 2023)	United Kingdom (UK GDPR)	Canada (PIPEDA)
Consent	Explicit, informed, freely given	Varies by sector and state	Consent-based with specified exceptions	Explicit and informed	Meaningful consent required
Cross-border Data Transfer	Permitted with adequacy decisions or approved safeguards	Limited federal restrictions	Permitted subject to government restrictions	Similar to EU GDPR safeguards	Permitted with organizational accountability
Data Localization	Generally not mandatory	No general federal requirement	Selective restrictions may apply	No mandatory localization	No mandatory localization
Enforcement Authority	Independent Data Protection Authorities	Federal and state agencies	Data Protection Board of India	Information Commissioner's Office	Office of the Privacy Commissioner
Penalties for Non-compliance	Very high administrative fines	Vary by law and jurisdiction	Monetary penalties under the DPDP Act	Significant administrative penalties	Regulatory investigations and compliance measures

The comparative analysis demonstrates that while considerable progress has been made in national privacy legislation, divergent legal standards continue to create challenges for protecting the digital rights of diaspora communities. Greater interoperability among national legal systems and stronger international cooperation are essential for ensuring effective cross-border data protection in the digital age.

LEGAL CHALLENGES FOR DIASPORA COMMUNITIES

Cross-border Data Transfer

Cross-border data transfer represents one of the most significant legal challenges facing diaspora communities. Personal information—including immigration records, financial transactions, biometric identifiers, healthcare records, educational credentials, and communication data—is frequently transferred across multiple jurisdictions through cloud services and multinational digital platforms. Since countries maintain different data protection standards, individuals may lose legal protection once their data are processed outside their country of residence.

Jurisdictional conflicts often arise concerning which country's laws govern data processing, dispute resolution, and enforcement. While regulations such as the European Union's GDPR impose strict safeguards for international transfers, many jurisdictions lack equivalent protections. Consequently, diaspora communities may experience inconsistent privacy standards and limited access to legal remedies.

Digital Surveillance

Digital surveillance has expanded considerably due to advances in artificial intelligence, facial recognition, biometric authentication, and predictive analytics. Governments increasingly justify surveillance for national security, immigration control, and law enforcement purposes. Nevertheless, excessive monitoring may undermine privacy, freedom of expression, and democratic participation.

Diaspora communities are particularly vulnerable because surveillance may originate from multiple sources. Host-country authorities may monitor immigration status, financial transactions, or online activities. Simultaneously, governments in countries of origin may monitor political activists, journalists, and dissidents residing abroad. In addition, private technology companies continuously collect user information for commercial profiling, personalized advertising, and behavioral analytics. The combination of state and corporate surveillance creates complex legal questions regarding transparency, accountability, proportionality, and judicial oversight.

Identity Theft and Biometric Data Misuse

Identity theft remains one of the fastest-growing cyber threats affecting migrants and overseas communities. Personal information submitted during immigration procedures, employment verification, banking transactions, and online registration can be exploited by cybercriminals for financial fraud or unauthorized access to digital services.

Biometric information—including fingerprints, facial recognition templates, iris scans, and voice patterns—has become increasingly important in digital identity systems. Unlike passwords, biometric identifiers cannot easily be replaced once compromised. Unauthorized collection or misuse of biometric information therefore presents serious privacy and security risks.

Diaspora populations are also exposed to passport fraud, forged travel documents, and identity impersonation during international migration processes. Strengthening legal safeguards governing biometric databases and identity verification systems has become essential for protecting migrants against identity-related crimes.

Artificial Intelligence Profiling

Artificial intelligence has transformed the processing of personal information through automated decision-making, predictive analytics, and algorithmic profiling. Governments and private organizations increasingly rely on AI systems to evaluate immigration applications, employment opportunities, financial services, healthcare eligibility, and security assessments.

Although AI enhances administrative efficiency, concerns have emerged regarding algorithmic discrimination and opaque decision-making processes. Bias within training datasets may disproportionately disadvantage migrants, refugees, and minority communities. Automated **risk-scoring** systems may incorrectly classify individuals as security risks or financial liabilities without adequate transparency or opportunities for appeal.
For diaspora communities, AI profiling raises important legal questions regarding fairness, accountability, explain ability, and human oversight in automated decision-making.

Political Targeting

Digital platforms have become important spaces for transnational political participation. Diaspora communities frequently engage in homeland politics through online campaigns, fundraising, advocacy, and social media discussions. While digital technologies strengthen democratic participation, they also increase exposure to political manipulation.

Political actors may employ targeted advertising, algorithmic profiling, misinformation campaigns, and coordinated disinformation strategies to influence diaspora voters. Online harassment, intimidation, and surveillance of political activists further threaten freedom of expression and civic participation.

The legal regulation of political advertising, cross-border election interference, and platform accountability remains inconsistent across jurisdictions, leaving diaspora communities vulnerable to digital political manipulation.

Cybercrime

The increasing reliance on digital technologies has expanded opportunities for cybercriminal activities targeting migrant populations. Common cyber threats include phishing attacks, ransom ware, identity fraud, financial scams, and fraudulent immigration services.

Diaspora communities often rely heavily on online banking, remittance platforms, visa application systems, and digital government portals. Cybercriminals exploit these dependencies by impersonating government agencies, financial institutions, or immigration authorities to obtain sensitive personal and financial information.

Combating cybercrime requires stronger international cooperation among law enforcement agencies, enhanced cybersecurity standards, and improved public awareness regarding digital security practices.

Social Media Privacy
Social media platforms have become indispensable tools for maintaining family relationships, cultural identity, and professional networks across borders. However, these platforms routinely collect extensive personal information through user interactions, location services, browsing histories, and behavioral analytics.

Unauthorized profiling enables companies to generate detailed behavioral profiles that may be used for targeted advertising, political messaging, or commercial purposes without meaningful user awareness. Location tracking further exposes diaspora communities to surveillance risks by revealing travel patterns, social relationships, and geographic movements.

Large-scale **data harvesting** by digital platforms has intensified concerns regarding informed consent, transparency, and accountability. Ensuring stronger regulation of social media companies remains essential for protecting the privacy rights of diaspora populations.

EMERGING ISSUES

i. **Artificial Intelligence (AI):** AI-driven decision-making systems increasingly influence immigration screening, employment, healthcare, policing, and financial services. Greater transparency, fairness, and accountability are required to prevent discriminatory outcomes.
ii. **Blockchain Technology:** Blockchain offers enhanced security, transparency, and tamper-resistant record keeping for digital identity and financial transactions. However, the immutability of blockchain records may conflict with privacy rights such as the right to erasure.
iii. **Digital Identity Systems:** Governments increasingly introduce digital identity platforms to improve access to public services. While these systems enhance administrative efficiency, centralized identity databases require strong legal safeguards against unauthorized access and misuse.
iv. **Facial Recognition Technology:** Facial recognition supports border management, public security, and authentication systems but raises concerns regarding mass surveillance, informed consent, and civil liberties.
v. **Deepfake Technology:** AI-generated synthetic media can facilitate identity fraud, misinformation, political manipulation, and reputational harm, particularly affecting diaspora activists and public figures.
vi. **Metaverse:** Virtual environments create new forms of social interaction, commerce, and digital identity while generating novel privacy, jurisdictional, and consumer protection challenges.
vii. **Quantum Computing:** Future quantum technologies may compromise existing encryption methods, requiring the development of quantum-resistant cybersecurity standards to protect personal information.
viii. **Cross-border Cloud Computing:** International cloud infrastructure facilitates efficient data storage but complicates jurisdiction, regulatory oversight, and legal accountability.
ix. **Digital Citizenship:** Increasing reliance on digital government services reinforces the importance of equitable internet access, digital literacy, and legal recognition of digital rights.
x. **Biometric Databases:** Large-scale biometric databases improve identity verification but require rigorous legal safeguards governing collection, retention, access, and international sharing.

FUTURE RESEARCH DIRECTIONS

Despite significant advances in digital governance research, several important areas require further scholarly attention. Future studies should investigate the implications of **artificial intelligence** for diaspora privacy, particularly concerning algorithmic bias, automated decision-making, and AI-based immigration management systems. Research is also needed on **children's digital rights within migrant families**, including online education, parental consent, and protection from digital exploitation.

Another emerging area concerns the governance of **cross-border biometric databases**, especially their implications for identity verification, refugee protection, border management, and international information sharing. Scholars should further explore legal models for **digital identity governance**, examining issues such as interoperability, cybersecurity, data ownership, and accountability across jurisdictions.

Finally, greater emphasis should be placed on **comparative research between Global North and Global South countries** to understand how differing legal systems, technological capacities, and institutional frameworks influence

the protection of digital rights. Such comparative studies would contribute to the development of more inclusive and globally harmonized approaches to data privacy and digital governance for diaspora communities.

CONCLUSION

Digital technologies have fundamentally transformed the lives of diaspora communities by enabling continuous communication, economic participation, cultural preservation, and political engagement across national borders. At the same time, these technological developments have introduced complex legal challenges associated with cross-border data transfers, digital surveillance, identity theft, artificial intelligence, cybercrime, and the expanding influence of global technology companies. The fragmented nature of national privacy laws further complicates the effective protection of personal information, leaving diaspora populations vulnerable to inconsistent legal standards and limited enforcement mechanisms.

This review demonstrates that international instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the General Data Protection Regulation, Convention 108+, the OECD Privacy Guidelines, and UNESCO's ethical recommendations collectively provide a strong normative foundation for digital rights protection. Nevertheless, significant gaps remain in implementation, cross-border cooperation, and global governance.

Protecting the digital rights of diaspora communities requires stronger international collaboration, harmonized privacy standards, transparent regulation of artificial intelligence, effective oversight of digital platforms, and enhanced cybersecurity measures. Governments, international organizations, technology companies, and civil society must work collaboratively to ensure that technological innovation advances human welfare without compromising privacy, equality, and fundamental freedoms.

REFERENCES

1. Balkin, J. M. (2021). *The path of robotics law*. California Law Review, 109(1), 45–82.
2. European Commission. (2024). *Data protection rules in the European Union (GDPR).* https://commission.europa.eu/law/law-topic/data-protection_en
3. European Parliament & Council of the European Union. (2024). *Artificial Intelligence Act (AI Act).* Official Journal of the European Union.
4. Government of India. (2023). *Digital Personal Data Protection Act, 2023.* Ministry of Electronics and Information Technology.
5. Government of India. (2025). *Draft Digital Personal Data Protection Rules, 2025.* Ministry of Electronics and Information Technology.
6. Organisation for Economic Co-operation and Development. (2021). *Going Digital Toolkit 2021*. OECD Publishing.
7. Organisation for Economic Co-operation and Development. (2023). *OECD Digital Economy Outlook 2023.* OECD Publishing.
8. Pandit, H. J., Esteves, B., Krog, G. P., Ryan, P., Golpayegani, D., & Flake, J. (2024). *Data Privacy Vocabulary (DPV) Version 2.* Semantic Web Journal.
9. United Nations. (2021). *Our Common Agenda: Report of the Secretary-General.* United Nations.
10. United Nations. (2023). *Global Digital Compact: Zero Draft.* United Nations.
11. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence.* UNESCO.
12. UNESCO. (2023). *Guidance for the Governance of Digital Platforms.* UNESCO.
13. UNESCO. (2024). *Ethics of Artificial Intelligence: Implementation Readiness Assessment Methodology.* UNESCO.
14. World Bank. (2021). *World Development Report 2021: Data for Better Lives.* World Bank.
15. Zuboff, S. (2021). *The age of surveillance capitalism* (Updated ed.). PublicAffairs.
16. Athar, S., Gosain, D., Feldmann, A., Kaur, M., & Dao, H. (2025). *"Nobody should control the end user": Exploring privacy perspectives of Indian Internet users in light of the Digital Personal Data Protection Act.* arXiv.
17. Sanford, M., & Yasseri, T. (2021). The kaleidoscope of privacy: Differences across French, German, UK, and US GDPR media discourse. *arXiv*.
18. Amaral, O., Abualhaija, S., Torre, D., Sabetzadeh, M., & Briand, L. (2021). AI-enabled automation for completeness checking of privacy policies under GDPR. *arXiv*.
19. Reuters. (2025, November 14). India strengthens privacy law with new data collection rules. Reuters.
20. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024.* World Economic Forum.