

PREFACE TO THE EDITION

The present issue brings together a range of scholarly studies examining significant developments at the intersection of law, society, technology, and governance. The contributions reflect the changing nature of contemporary legal scholarship and address questions arising from established legal principles as well as emerging social and technological realities.

Among the themes explored in this issue are the relationship between customary legal systems and constitutional principles, particularly in the context of gender justice, and the legal protection of migrant workers in South Asia. These contributions draw attention to questions of equality, constitutional protection, labour rights, enforcement, and social security within diverse legal and regulatory frameworks.

The issue also engages extensively with the legal challenges arising from technological transformation. The contributions examine technology-facilitated domestic violence, cross-border data protection, blockchain-based smart contracts and international arbitration, and the regulation of mental-health telemedicine. The comparative study of the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (DPDP Act) provides particular insight into evolving approaches to data rights, cross-border transfers, regulatory accountability, and international interoperability.

Further, the issue considers the expanding role of artificial intelligence in consequential decision-making and the resulting questions of transparency, discrimination, human oversight, and legal accountability. Together, these studies demonstrate the growing need for legal frameworks to respond effectively to technological developments while maintaining appropriate safeguards for individual rights and public interests.

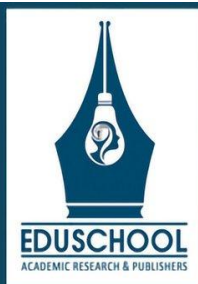
Taken together, the contributions demonstrate the breadth of contemporary legal inquiry and the importance of comparative and interdisciplinary approaches to understanding evolving legal challenges. We hope that the research presented in this issue will contribute to continued academic discussion and encourage further scholarship on the changing relationship between law, technology, and society.

We express our sincere appreciation to the authors, reviewers, and members of the editorial team for their valuable contributions and continued commitment to scholarly research.

Dakshina Saraswathy
Chief Editor

CONTENTS

SL. NO.	TITLE	AUTHOR	PAGE NO.
1	Customary Law and Constitutional Rights: Navigating Legal Pluralism for Gender Justice	Gopi C.C	1-4
2	Labor Rights and Migrant Workers: Comparative Protective Frameworks in South Asia	Varsha Palliyil	5-8
3	Legal Frameworks Protecting Domestic Violence Survivors Digitally	Adwaidh Jaimon	9-12
4	Smart Contracts in International Arbitration: Legal Challenges in the Blockchain Era	Reyona Elsa Sherin	13-15
5	Cross-Border Data Protection: Comparative Analysis of GDPR and India's DPDP Act	Sharmila	16-19
6.	Regulating Mental Health Telemedicine: Cross-Jurisdictional Challenges and Policy Responses	Amal Krishna S	20-23
7.	Artificial Intelligence and Legal Accountability: Frameworks for Algorithmic Governance	Vinothini S	24-27



INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Customary Law and Constitutional Rights: Navigating Legal Pluralism for Gender Justice

Gopi C.C

Advocate

Article information

Received: 22nd June 2026

Received in revised form: 5th July 2026

Accepted: 8th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0044>

Abstract

Legal pluralism—the coexistence of state law and customary, religious, or community-based normative orders defines the legal landscape of much of Africa and Asia. While customary law has been valorized as an expression of cultural self-determination and a counterweight to colonial legal impositions, it has also been the site of persistent gender inequality, particularly in marriage, inheritance, and guardianship. This paper examines how postcolonial constitutions in African and Asian jurisdictions mediate the tension between customary recognition and women's equality guarantees. Drawing on comparative case studies from South Africa, Kenya, Nigeria, India, Bangladesh, and Indonesia, and engaging with the recent critical analysis of Taak (2025), the paper analyzes four constitutional strategies: supremacy clauses, repugnancy tests, integrative harmonization, and pluralist parity. The analysis argues that supremacy-with-harmonization, in which constitutional equality prevails but through a dialogic reform process that enlists customary institutions, offers the most durable path to gender justice. The paper closes with recommendations for statutory codification, judicial training, and community-based reform dialogues.

Keywords:- Customary law, legal pluralism, constitutional reform, gender justice, women's rights, Africa, Asia, equality

I. INTRODUCTION

The relationship between customary law and women's rights is among the most contested issues in postcolonial legal theory. Customary law governs substantial areas of marriage, inheritance, land tenure, and family relations for hundreds of millions of women across Africa and Asia. It is simultaneously a living tradition and a zone of structural disadvantage. The tension is visible in successive waves of constitutional reform, statutory codification, and judicial intervention that have sought to reconcile respect for cultural pluralism with non-discrimination guarantees.

The scholarly literature has traced multiple positions. Cultural-relativist accounts emphasize the epistemic legitimacy of customary systems and warn against imposing universal standards derived from liberal constitutionalism (An-Na'im, 1990). Liberal-universalist accounts prioritize the non-derogable character of gender equality and insist on constitutional supremacy (Okin, 1999). Recent scholarship has moved toward dialogic or integrative models that preserve the plural character of legal orders while insisting on minimum substantive protections (Merry, 2006; Banda, 2005).

This paper engages these debates through comparative analysis of six jurisdictions: South Africa, Kenya, and Nigeria in Africa; India, Bangladesh, and Indonesia in Asia. The jurisdictions share histories of colonial codification, postcolonial constitutional drafting, and ongoing contestation over the status of customary law. Drawing on Taak (2025), who provides a systematic critical analysis of legal pluralism and constitutional reform in these regions, the paper develops a typology of constitutional strategies and assesses their comparative performance on gender justice.

II. LEGAL PLURALISM: THEORETICAL FRAMEWORK

Legal pluralism, as articulated by Merry (1988) and Griffiths (1986), refers to the presence within a single polity of multiple legal orders with overlapping and sometimes competing claims to authority. In postcolonial African and Asian

jurisdictions, the typical configuration includes state statutory law, colonial-era codifications of 'native custom,' religious or personal laws, and the living customary practices of particular communities. The pluralist condition is thus both a historical legacy and a contemporary reality.

Gender emerges as a focal point of pluralist tension because customary systems across these regions have historically privileged male authority in household governance, inheritance, marital dissolution, and child custody. Feminist legal scholars have distinguished between official customary law recorded, textualized, often distorted through colonial administration and living customary law, which evolves in community practice and may or may not reflect official texts (Oyèwùmí, 1997; Himonga, 2011). Progressive approaches to reform have sought to mobilize living customary law's adaptive capacity against the rigidities of the official text.

Four constitutional strategies recur in the comparative record. First, the supremacy strategy, exemplified by South Africa's 1996 Constitution, declares the supremacy of constitutional rights over conflicting customary rules. Second, the repugnancy strategy, rooted in British colonial administration, validates customary law subject to a judicial test of repugnance to natural justice or public policy. Third, the integrative-harmonization strategy, adopted in Kenya's 2010 Constitution, recognizes customary law as a source while authorizing parliamentary harmonization to conform with equality guarantees. Fourth, the pluralist-parity strategy treats customary and statutory law as coordinate orders, with limited override. Each strategy has particular implications for women's rights outcomes.

III. CUSTOMARY LAW AND WOMEN'S RIGHTS IN AFRICA

South Africa's post-apartheid constitutional settlement provides the clearest example of the supremacy strategy. Section 211 of the 1996 Constitution recognizes traditional leadership and customary law, but section 39(2) subjects all law to the Bill of Rights. The Constitutional Court's decision in *Bhe v. Magistrate, Khayelitsha* (2005) struck down the rule of male primogeniture in African customary succession as inconsistent with the equality guarantee. Subsequent legislation the Reform of Customary Law of Succession and Regulation of Related Matters Act 2009 codified gender-neutral succession. The supremacy strategy has produced significant doctrinal gains but has been criticized for imposing statutory solutions on living community practices (Mnisi Weeks, 2015).

Kenya's 2010 Constitution articulates the integrative-harmonization strategy. Article 2(4) declares any law, including customary law, that is inconsistent with the Constitution void; article 60 requires land-tenure reform to eliminate gender discrimination in customary land holdings. The Matrimonial Property Act 2013 codifies spousal property rights in a manner informed by customary expectations but subject to constitutional equality. Implementation has been uneven, particularly in pastoralist regions, where customary councils retain practical adjudicative authority (Nyamu-Musembi, 2013).

Nigeria retains a repugnancy regime inherited from colonial administration, reiterated in section 18(3) of the Evidence Act 2011. Customary law is valid unless repugnant to natural justice, equity, and good conscience, or incompatible with any law in force. Nigerian courts have invalidated discriminatory inheritance practices in cases such as *Mojekwu v. Mojekwu* (1997) and *Ukeje v. Ukeje* (2014), the latter holding that the Igbo custom denying daughters' inheritance rights violated section 42 of the Constitution. Yet enforcement varies across the federation's thirty-six states and between statutory and customary courts, and practical access depends heavily on urban proximity and educational resources.

Across the three African jurisdictions, Taak (2025) observes a recurrent pattern: doctrinal advances at the constitutional and apex-court level have not fully translated into community-level change. Judicial pronouncements bind parties in the litigated cases but diffuse slowly through customary councils and household practice. This diffusion gap is the central implementation challenge.

IV. ASIAN JURISDICTIONS: INDIA, BANGLADESH, AND INDONESIA

India operates a hybrid regime in which personal laws Hindu, Muslim, Christian, Parsi, and secular civil-marriage regimes govern marriage, inheritance, and related matters, alongside customary law that persists in tribal communities under the Fifth and Sixth Schedules of the Constitution. Article 14's equality guarantee and article 15's prohibition on sex discrimination have been applied to personal laws with notable inconsistency. The Hindu Succession (Amendment) Act 2005 granted daughters equal coparcenary rights; the *Shayara Bano v. Union of India* (2017) decision invalidated instantaneous triple talaq; and the Muslim Women (Protection of Rights on Marriage) Act 2019 criminalized the practice. Yet the directive principle of a Uniform Civil Code (article 44) remains unrealized, leaving a patchwork of protections.

The tribal customary law situation in India presents an additional dimension. The *Nagaland Tuluni v. Naga Mothers' Association* case (1994) and subsequent litigation have tested the boundary between community self-governance under article 371A and gender equality. The tension resembles the South African supremacy question but is mediated by India's additional commitment to cultural autonomy of scheduled tribes.

Bangladesh recognizes personal laws for Muslim, Hindu, Christian, and Buddhist communities. The Constitution's article 28 prohibits sex discrimination, but article 28(4) permits special provision for women; the interaction with personal laws has been uneven. Muslim women access divorce through the Dissolution of Muslim Marriages Act 1939; Hindu women continue to face restrictive inheritance rules, with the Hindu Women's Rights to Property Act 1937 still governing despite reform proposals (Pereira, 2002).

Indonesia's legal pluralism comprises adat (customary) law, Islamic law administered through the Religious Courts for Muslim matters, and national civil law. The 1999 amendments to the Marriage Law and the Compilation of Islamic Law (*Kompilasi Hukum Islam*) represent codifying efforts. The Constitutional Court has held, in a series of decisions from 2005 onward, that statutory interpretations infringing on women's equality violate article 28B of the 1945 Constitution. Progress has been substantial in some areas, notably divorce and child custody, while remaining uneven in inheritance and land tenure (Bowen, 2003).

V. CONSTITUTIONAL REFORM STRATEGIES: A COMPARATIVE ASSESSMENT

Comparing the six jurisdictions suggests several observations. First, the supremacy strategy of South Africa has produced the most doctrinally sharp results but has generated sustained legitimacy challenges from traditional leadership institutions. Second, the integrative-harmonization strategy of Kenya has achieved broader community acceptance at the cost of slower implementation. Third, the repugnancy strategy of Nigeria is open-ended and depends heavily on judicial composition. Fourth, the pluralist-parity features of India, Bangladesh, and Indonesia produce protections that vary by community membership rather than by citizenship, creating uneven access to equality guarantees.

A pattern emerging across all six is that purely top-down reform, whether by constitutional supremacy or statutory override, encounters implementation limits. Where reform has consolidated, it has done so through combined mechanisms: constitutional doctrine, statutory codification, judicial training, community dialogue, and civil-society mobilization. Taak (2025) describes this as the 'harmonization-with-dialogue' model and argues that it offers the most durable path to gender justice because it engages rather than displaces customary institutions.

Three further observations deserve note. First, land-tenure reform is the most consequential and the most contested site of gender equality intervention, given the centrality of land to rural livelihoods. Second, women traditional leaders have emerged as pivotal agents of internal customary reform, particularly in South African chieftaincies and Kenyan pastoralist councils. Third, international human-rights instruments CEDAW, the Maputo Protocol, the African Charter on Human and Peoples' Rights have provided normative anchors that reform-minded domestic actors invoke strategically.

VI. RECOMMENDATIONS

Five reforms would strengthen gender equality within pluralist frameworks. *First*, jurisdictions should codify core minimum protections equal succession rights, equal marital property rights, freedom from coerced marriage, and equal guardianship through dedicated statutes binding across statutory and customary forums. The Kenyan Matrimonial Property Act model demonstrates feasibility.

Second, judicial training on living customary law should be institutionalized. Judges interpreting customary law should have access to expert evidence from community members, anthropological records, and women's-voice submissions to prevent reliance on stale colonial-era codifications.

Third, community-level reform dialogues should be supported and funded. South Africa's National House of Traditional Leaders, Kenya's Council of Elders initiatives, and Indonesia's *musyawarah* (consultative) forums provide infrastructure that can be harnessed for deliberative reform on gender-sensitive customary rules.

Fourth, land-tenure registration systems should be redesigned to eliminate gender discrimination at the point of titling. Women's names should appear on household titles; joint titling should be the default in marital property registrations.

Fifth, monitoring and data infrastructure should be developed. Gender-disaggregated data on succession disputes, marital dissolution outcomes, and land-tenure registrations would reveal implementation gaps that doctrinal reform alone cannot address. CEDAW reporting cycles can serve as a coordinating mechanism.

VII. CONCLUSION

Legal pluralism is not an obstacle to gender justice; it is the terrain on which gender justice must be pursued in the majority of African and Asian jurisdictions. Constitutional supremacy clauses, when applied without engagement with living customary institutions, risk producing doctrinal victories without community uptake. Conversely, unqualified deference to customary authority can perpetuate deeply rooted inequalities. The comparative evidence reviewed in this paper suggests that the most durable path lies between these extremes, in a supremacy-with-harmonization approach that insists on equality while engaging the customary institutions that deliver law on the ground.

The contribution of Taak (2025) lies in articulating this middle path with doctrinal precision and in mapping its operation across jurisdictions of significant demographic weight. The present paper has developed that framework comparatively and proposed reform avenues. Gender justice within pluralist legal orders is achievable; it requires sustained coordination between constitutional, statutory, judicial, and community mechanisms.

REFERENCES

- An-Na'im, A. A. (1990). *Toward an Islamic reformation: Civil liberties, human rights, and international law*. Syracuse University Press.
- Banda, F. (2005). *Women, law and human rights: An African perspective*. Hart Publishing.
- Bhe v. Magistrate, Khayelitsha*, 2005 (1) BCLR 1 (CC) (South Africa).
- Bowen, J. R. (2003). *Islam, law, and equality in Indonesia: An anthropology of public reasoning*. Cambridge University Press.
- Compilation of Islamic Law (Kompilasi Hukum Islam), Presidential Instruction No. 1 of 1991 (Indonesia).
- Constitution of Kenya. (2010).
- Constitution of the Republic of South Africa. (1996).
- Dissolution of Muslim Marriages Act, No. 8 of 1939 (India, applied in Bangladesh).
- Evidence Act, No. 18 of 2011 (Nigeria).
- Griffiths, J. (1986). What is legal pluralism? *Journal of Legal Pluralism and Unofficial Law*, 18(24), 1–55.
- Himonga, C. (2011). The future of living customary law in African legal systems in the twenty-first century and beyond. In J. Fenrich, P. Galizzi, & T. Higgins (Eds.), *The future of African customary law* (pp. 31–57). Cambridge University Press.
- Hindu Succession (Amendment) Act, No. 39 of 2005 (India).
- Matrimonial Property Act, No. 49 of 2013 (Kenya).
- Merry, S. E. (1988). Legal pluralism. *Law & Society Review*, 22(5), 869–896.
- Merry, S. E. (2006). *Human rights and gender violence: Translating international law into local justice*. University of Chicago Press.
- Mnisi Weeks, S. (2015). *Take your mat and go!: Rural Zulu women's strategies for secure tenure*. Rutgers University Press.
- Mojeckwu v. Mojeckwu*, (1997) 7 NWLR (Pt. 512) 283 (Nigeria).

- Muslim Women (Protection of Rights on Marriage) Act, No. 20 of 2019 (India).
- Nyamu-Musembi, C. (2013). Ruling out gender equality? The post-Cold War rule of law agenda in sub-Saharan Africa. *Third World Quarterly*, 34(5), 878–895.
- Okin, S. M. (1999). Is multiculturalism bad for women? In S. M. Okin, J. Cohen, M. Howard, & M. C. Nussbaum (Eds.), *Is multiculturalism bad for women?* (pp. 7–24). Princeton University Press.
- Oyěwùmí, O. (1997). *The invention of women: Making an African sense of Western gender discourses*. University of Minnesota Press.
- Pereira, F. (2002). *The fractured scales: The search for a uniform personal code*. STREE.
- Reform of Customary Law of Succession and Regulation of Related Matters Act, No. 11 of 2009 (South Africa).
- Shayara Bano v. Union of India*, (2017) 9 SCC 1.
- Taak, S. (2025). The intersection of customary law and women's rights in developing jurisdictions: A critical analysis of legal pluralism and constitutional reform in Africa and Asia. *International Journal of Judicial Science Research Studies*, 56–60. <https://doi.org/10.63090/ijjsrs/3049.0618.0023>
- Ukeje v. Ukeje*, (2014) 11 NWLR (Pt. 1418) 384 (Nigeria).

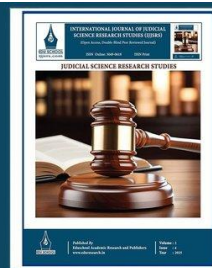


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Labor Rights and Migrant Workers: Comparative Protective Frameworks in South Asia

Varsha Palliyil

Research Scholar, School of Law, VELS University of Science and Technology, Chennai, India.

Article Information

Received: 16th June 2026

Received in revised form: 4th July 2026

Accepted: 9th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0046>

Abstract

Migrant workers constitute one of the most economically productive yet legally under-protected populations in South Asia. India alone hosts an estimated 139 million internal migrants, with cross-border corridors to Bangladesh, Nepal, and Sri Lanka generating further regulatory complexity. This paper offers a doctrinal and comparative analysis of the statutory and constitutional frameworks governing migrant labor rights across these jurisdictions. Drawing on the Indian Inter-State Migrant Workmen Act 1979, the consolidated labor codes of 2019–2020, Bangladesh's Overseas Employment and Migrants Act 2013, Nepal's Foreign Employment Act 2007, and Sri Lanka's Bureau of Foreign Employment Act 1985, the study identifies convergences, divergences, and enforcement gaps that were exposed dramatically by the COVID-19 lockdowns. The paper argues that formal statutory protection remains undermined by weak registration systems, informal subcontracting chains, and the absence of portable social security. It proposes a rights-based regional framework anchored in ILO Conventions 97 and 143, bilateral labor agreements, and digital portability of entitlements. The findings contribute to ongoing debates on labor justice, informal-sector regulation, and the constitutionalization of socio-economic rights in developing jurisdictions.

Keywords:- Migrant workers, labor rights, South Asia, legal pluralism, constitutional protection, social security, informal labor

I. INTRODUCTION

The movement of labor, whether internal or cross-border, is a structural feature of the South Asian political economy. Migration from agrarian peripheries to urban construction sites, brick kilns, textile factories, and plantation economies has accelerated since the liberalization reforms of the early 1990s. According to the Economic Survey of India (2017), approximately one-fifth of the Indian workforce is mobile, with construction, domestic work, and manufacturing absorbing the largest inflows. In Nepal, remittances from migrant workers account for nearly 22 percent of gross domestic product, while Sri Lanka and Bangladesh sustain comparable dependencies on overseas labor earnings.

Yet the legal condition of the migrant worker remains paradoxical. While migration is constitutive of national economies, legal frameworks continue to treat migrant labor as peripheral, temporary, or anomalous. The catastrophic reverse-migration of the March–May 2020 lockdowns, during which an estimated ten million Indian workers walked or rode home under conditions of acute distress, revealed the chronic failure of state registration, welfare delivery, and grievance redress mechanisms (Srivastava, 2020). Similar vulnerabilities surfaced in the Gulf corridors, where returnee workers from Nepal and Bangladesh faced delayed wages, arbitrary contract termination, and quarantine costs shifted onto them.

This paper examines the protective frameworks governing migrant labor in four South Asian jurisdictions: India, Bangladesh, Nepal, and Sri Lanka. It pursues three objectives. First, it maps the statutory and constitutional architecture in each jurisdiction. Second, it analyzes the enforcement gaps that diminish formal protection. Third, it proposes reforms that draw on regional harmonization, digital portability of entitlements, and the substantive realization of constitutional socio-economic rights. The analysis integrates the recent scholarly intervention of Palliyil (2024), whose examination of labor rights regulating migrant workers in India provides doctrinal orientation for the present comparative inquiry.

II. CONCEPTUAL FOUNDATIONS OF MIGRANT LABOR RIGHTS

The conceptualization of migrant labor rights draws on overlapping registers: international human rights law, labor standards jurisprudence, and constitutional socio-economic rights doctrine. At the international level, the International Labour Organization (ILO) Migration for Employment Convention 97 (1949) and the Migrant Workers (Supplementary Provisions) Convention 143 (1975) establish the core principles of equal treatment, non-discrimination, and protection against abusive conditions. The United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (1990) extends protections to undocumented migrants, though ratification among destination states remains limited.

At the domestic level, migrant workers intersect multiple legal categories: industrial workers under wage legislation, informal workers under social-security schemes, and citizens claiming fundamental rights. The difficulty of sorting migrants into stable legal categories is itself a source of protective failure. As Breman (2013) observed in the Indian context, the migrant is frequently rendered invisible by the very statutes intended to govern industrial labor because of the informal, subcontracted, and spatially dispersed character of the employment relationship.

The conceptual literature identifies three modalities of protection. First, the registration-based model conditions entitlements on formal enrollment with a designated agency. Second, the rights-based model derives protection from constitutional guarantees of life, dignity, and equality, as in the Indian Supreme Court's expansive reading of Article 21. Third, the contractualist model relies on bilateral agreements between sending and receiving states, common in the Gulf corridor. Each modality carries weaknesses: registration models exclude the unregistered, rights-based models depend on litigation capacity, and contractualist models privilege diplomatic over legal remedies.

Palliyil (2024) contends that in the Indian case, the effective enjoyment of labor rights by migrants has been undermined by the bifurcation between formal statutory entitlements and the ground-level realities of informal subcontracting, placement agencies, and seasonal relocation. The present analysis extends this critique comparatively.

III. INDIAN STATUTORY AND CONSTITUTIONAL FRAMEWORK

India's regulatory architecture for migrant labor rests on a combination of specialized legislation and consolidated labor codes. The Inter-State Migrant Workmen (Regulation of Employment and Conditions of Service) Act 1979 requires principal employers and contractors to register workers moving across state boundaries, provide displacement allowances, and ensure equal wages. In practice, registration rates have remained below ten percent in most destination states, and the Act's penalties are trivial relative to the economic incentives to evade compliance (Srivastava, 2020).

The consolidated codes adopted between 2019 and 2020 the Code on Wages 2019, the Industrial Relations Code 2020, the Occupational Safety, Health and Working Conditions Code 2020 (OSH Code), and the Code on Social Security 2020 collectively replace twenty-nine prior statutes. The OSH Code subsumes the 1979 Act and extends coverage to 'inter-State migrant workers' employed directly by principal employers or through contractors, defining the category with a monthly wage ceiling. The Code on Social Security establishes a national database for unorganized, gig, and migrant workers, with entitlements to health insurance, old-age protection, and disability benefits. Despite these advances, scholars have observed that the codes retain the registration model's structural limitations, delegate critical rule-making to state governments, and lack robust enforcement machinery (Sundar, 2020).

Constitutionally, the Supreme Court has elaborated a rich jurisprudence on migrant labor dignity. In *Peoples Union for Democratic Rights v. Union of India* (1982), the Court held that non-payment of minimum wages to migrant construction workers constituted forced labor under Article 23. In *Bandhua Mukti Morcha v. Union of India* (1984), it recognized the right to rehabilitation of bonded migrant laborers. More recently, the suo motu proceedings initiated during the 2020 lockdown (*In re: Problems and Miseries of Migrant Labourers*, 2020) resulted in directions for free transportation, food distribution, and the operation of a National Database of Unorganized Workers.

Palliyil (2024) argues that this constitutional jurisprudence, though doctrinally generous, has depended on activist litigation and has not translated into administrative routinization of protection. The gap between declared right and delivered remedy remains the central puzzle of the Indian framework.

IV. COMPARATIVE PERSPECTIVE: BANGLADESH, NEPAL, AND SRI LANKA

Bangladesh operates a distinct regulatory model focused on overseas labor migration. The Overseas Employment and Migrants Act 2013 establishes a grievance redress mechanism, mandates recruitment licensing, and creates a Wage Earners Welfare Board financed by pre-departure contributions. Critics note that the Act is oriented toward regulating private recruiters rather than empowering workers; complaints procedures are cumbersome, and the Welfare Board's benefits have been described as symbolic in scope (Siddiqui, 2016).

Nepal's Foreign Employment Act 2007, together with its 2008 Regulations, institutes a Foreign Employment Promotion Board, mandatory pre-departure orientation, and insurance cover for overseas workers. The Act prohibits discrimination based on gender, though informal bans on female domestic-worker migration have periodically reappeared in executive policy. Nepali migrant workers primarily transit to India under the Treaty of Peace and Friendship 1950, which grants reciprocal rights of residence and employment, creating one of the world's most open cross-border labor regimes. Despite the treaty's formal generosity, Nepali migrants in India rarely access welfare entitlements because of identification, language, and administrative barriers (Thieme, 2012).

Sri Lanka's Bureau of Foreign Employment Act 1985 similarly regulates private recruiters, mandates pre-departure training, and operates a Welfare Fund. Sri Lanka's 2008 National Labour Migration Policy is one of the most comprehensive in the region, embedding a rights-based approach, gender mainstreaming, and return-and-reintegration programming.

Implementation, however, has been uneven, and the Gulf corridor continues to generate recurring reports of wage theft, contract substitution, and confinement.

Three patterns emerge from comparison. First, all four jurisdictions rely on registration-based frameworks that struggle to penetrate the informal recruitment pipelines dominating migrant placement. Second, destination-state cooperation is weak across the region, with bilateral labor agreements frequently lacking enforceable dispute-resolution clauses. Third, women migrants face heightened vulnerabilities, particularly in domestic work, which all four states have attempted to regulate through pre-departure restrictions that often displace rather than reduce risk.

V. ENFORCEMENT GAPS AND THE COVID-19 CRISIS

The COVID-19 pandemic functioned as a stress test for South Asian migrant-labor frameworks. In India, the 21-day national lockdown announced on 24 March 2020 created immediate income collapse for migrant construction, domestic, and informal workers. With inter-state transport suspended and urban shelters inaccessible, millions began journeys on foot that exposed the absence of real-time identification, welfare portability, and grievance redress. The Supreme Court, acting on public-interest litigation, directed states to provide food, water, and transport; the Ministry of Labour subsequently activated the e-Shram portal for unorganized-worker registration in August 2021.

Bangladesh, Nepal, and Sri Lanka each faced returnee surges from the Gulf. Quarantine costs, repatriation logistics, and the reabsorption of unemployed returnees into rural economies strained administrative capacity. In Nepal, the Foreign Employment Welfare Fund extended limited financial assistance, though coverage reached a minority of returnees. Sri Lanka's Bureau of Foreign Employment coordinated repatriation flights, but testing and isolation infrastructure remained overwhelmed. The pandemic revealed four systemic enforcement gaps common across jurisdictions:

- absence of a unique, portable identification that links a worker to entitlements across districts or states
- dependence on employer-initiated registration that chronically under-counts the migrant workforce
- weak administrative sanctions for non-compliance with wage, housing, and safety standards
- limited institutional capacity for rapid welfare delivery during crises. Palliyil (2024) links these gaps to the deeper political-economy failure to treat migrant labor as a site of constitutional entitlement rather than administrative tolerance.

VI. RECOMMENDATIONS

Reform of the South Asian migrant-labor framework should proceed along five axes. First, jurisdictions should institute a portable, biometric-linked worker identification that travels with the worker and automatically updates entitlement status. India's e-Shram platform and Aadhaar interface constitute a foundation, but the platform's extension to cross-border migrants requires bilateral interoperability arrangements.

Second, destination-state liability must be strengthened. Principal employers, not merely contractors, should bear primary liability for wage, safety, and social-security compliance under a statutory chain-of-responsibility doctrine. India's OSH Code moves tentatively in this direction; Bangladesh, Nepal, and Sri Lanka should adopt equivalent provisions for outbound and returning workers.

Third, the region should negotiate a South Asian Framework Agreement on Labor Migration, modeled on the ASEAN Consensus on the Protection and Promotion of the Rights of Migrant Workers (2017), to harmonize recruitment standards, wage protection, and grievance redress. SAARC has the institutional mandate; political will has been the limiting factor.

Fourth, gender-specific protections should be embedded rather than substituted by prohibitionist restrictions on female migration. Restricting women's outward migration displaces rather than reduces risk, pushing women into unregulated channels. Regulation of domestic-work recruitment, standardized contracts, and consular inspection provide more durable protection.

Fifth, constitutional review mechanisms should be strengthened. In India, the Supreme Court's *suo motu* jurisprudence could be institutionalized through a statutory Migrant Welfare Commission with investigative powers. In Nepal and Sri Lanka, constitutional socio-economic rights clauses should be read with directive force on the executive.

VII. CONCLUSION

The South Asian migrant-labor framework exhibits a consistent pattern: formal statutory protection undermined by weak registration, informal recruitment, and limited administrative capacity. The COVID-19 crisis exposed the operational fragility of these regimes and prompted incremental reforms, notably India's labor codes and e-Shram platform. Yet the structural gap between constitutional entitlement and administrative delivery persists across all four jurisdictions examined.

This paper has argued that effective protection requires three shifts. It requires a shift from registration-based to rights-based frameworks, in which entitlements attach to the worker rather than the job. It requires a shift from national-silo regulation to regional harmonization, given the cross-border character of South Asian labor flows. And it requires a shift from episodic judicial intervention to routinized administrative delivery. Palliyil's (2024) intervention offers a starting doctrinal map; the comparative analysis developed here points to a regional reform agenda. The migrant worker is neither marginal nor anomalous to the South Asian economy; the legal framework must finally reflect that centrality.

REFERENCES

- Breman, J. (2013). *At work in the informal economy of India: A perspective from the bottom up*. Oxford University Press.
- Bandhua Mukti Morcha v. Union of India*, AIR 1984 SC 802.
- Code on Social Security, No. 36 of 2020, Acts of Parliament, India.
- Code on Wages, No. 29 of 2019, Acts of Parliament, India.

Foreign Employment Act, 2007 (Nepal).
 Industrial Relations Code, No. 35 of 2020, Acts of Parliament, India.
In re: Problems and Miseries of Migrant Labourers, (2020) SCC OnLine SC 567.
 Inter-State Migrant Workmen (Regulation of Employment and Conditions of Service) Act, No. 30 of 1979, Acts of Parliament, India.
 International Labour Organization. (1949). *Migration for employment convention (revised)*, No. 97.
 International Labour Organization. (1975). *Migrant workers (supplementary provisions) convention*, No. 143.
 Ministry of Finance, Government of India. (2017). *Economic survey 2016–17*. Government of India.
 Occupational Safety, Health and Working Conditions Code, No. 37 of 2020, Acts of Parliament, India.
 Overseas Employment and Migrants Act, 2013 (Bangladesh).
 Palliyil, V. (2024). Labor rights regulating migrant workers in India. *International Journal of Judicial Science Research Studies (IJJSRS)*, 18–21. <https://doi.org/10.63090/ijjsrs/3049.0618.0005>
Peoples Union for Democratic Rights v. Union of India, AIR 1982 SC 1473.
 Siddiqui, T. (2016). *International labour migration and remittance management in Bangladesh*. Refugee and Migratory Movements Research Unit.
 Srivastava, R. (2020). *Understanding circular migration in India: Its nature and dimensions, the crisis under lockdown, and the response of the state*. Centre for Employment Studies Working Paper Series.
 Sundar, K. R. S. (2020). Critiquing the Indian labour codes 2019–2020. *Economic and Political Weekly*, 55(38), 47–52.
 Thieme, S. (2012). Coming home? Patterns and characteristics of return migration in Nepal. *International Migration*, 50(4), 106–124.
 United Nations. (1990). *International convention on the protection of the rights of all migrant workers and members of their families*.

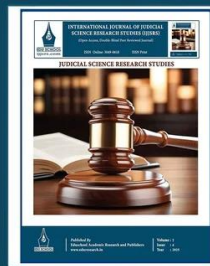


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Legal Frameworks Protecting Domestic Violence Survivors Digitally

Adwaidh Jaimon

4th year Student, BBA LL.B. (Hons), Cooperative School of Law, Thodupuzha, India

Article information

Received: 4th June 2026

Received in revised form: 2nd July 2026

Accepted: 10th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0047>

Abstract

The digital age has fundamentally transformed the landscape of domestic violence, creating new avenues for abuse while simultaneously challenging traditional legal frameworks designed to protect survivors. This paper examines the evolution of legal protections for domestic violence survivors confronting technology-facilitated abuse, analyzing recent legislative developments including the Violence Against Women Act Reauthorization of 2022, the federal Take It Down Act of 2025, and state-level coercive control legislation. Through critical analysis of international conventions, federal statutes, and emerging case law, this study reveals persistent gaps in legal frameworks despite progressive reforms. The paper argues that effective protection requires interdisciplinary approaches integrating criminal law, civil remedies, platform accountability, and survivor-centered policies. By examining the intersection of technology, law, and gendered violence, this research contributes to ongoing debates about digital safety, privacy rights, and the modernization of domestic violence law to address 21st-century threats.

Keywords:- Domestic violence, cyberstalking, coercive control, survivors, Take It Down Act, digital abuse

I. INTRODUCTION

Domestic violence, historically understood as physical and sexual abuse within intimate relationships, has undergone a profound transformation in the digital age. Technology-facilitated domestic abuse (TFDA) now encompasses cyberstalking, non-consensual intimate image distribution, GPS tracking, account hacking, and digital coercive control--tactics that extend an abuser's reach beyond physical proximity (Harris & Woodlock, 2019). The ubiquity of smartphones, social media platforms, and Internet of Things devices has created unprecedented opportunities for surveillance, harassment, and manipulation, fundamentally altering the dynamics of intimate partner violence.

Legal frameworks designed to protect domestic violence survivors have struggled to keep pace with technological evolution. Traditional restraining orders and assault statutes, crafted in an era of localized physical violence, prove inadequate when confronting digital abuse that transcends geographic boundaries and operates continuously through networked devices. As intimate partner violence affects over 10 million individuals annually in the United States alone (Centers for Disease Control and Prevention, 2024), the imperative to modernize legal protections has never been more urgent.

This paper critically examines the legal frameworks emerging to address digital-age domestic violence. It analyzes international conventions, federal legislation, and state-level reforms while interrogating their efficacy in protecting survivors from technology-facilitated abuse. Through this analysis, the paper illuminates both the progress achieved and the persistent gaps requiring further legislative attention.

II. THEORETICAL FRAMEWORK

Understanding legal responses to digital domestic violence requires engagement with multiple theoretical frameworks. The *power and control model*, developed by domestic violence advocates and articulated through the Duluth Model's Power and Control Wheel, provides foundational understanding of how abusers maintain dominance through systematic tactics including intimidation, isolation, economic abuse, and emotional manipulation (Pence & Paymar, 1993). Technology amplifies

each spoke of this wheel: digital surveillance enables constant monitoring, social media facilitates public humiliation, financial apps provide tools for economic control, and smart home devices create new mechanisms for intimidation.

Feminist legal theory illuminates how digital domestic violence perpetuates gendered power structures. Though anyone can experience technology-facilitated abuse, women disproportionately suffer from non-consensual intimate image distribution, cyberstalking, and digital sexual harassment (Powell & Henry, 2019). Legal frameworks failing to recognize technology-facilitated abuse as serious violence effectively perpetuate patriarchal systems that minimize women's experiences and maintain male dominance through fear and control.

The concept of *coercive control* provides crucial theoretical grounding. Developed by Evan Stark, coercive control describes domestic violence as a pattern of strategic behaviors designed to dominate another person through intimidation, isolation, and deprivation rather than discrete physical assaults (Stark, 2007). Digital technologies enhance coercive control by enabling continuous surveillance, instantaneous communication of threats, and inescapable monitoring that follows survivors into every aspect of their lives. This theoretical framework has proven particularly influential in recent legislative reforms recognizing non-physical abuse as actionable domestic violence.

III. THE EVOLUTION OF LEGAL FRAMEWORKS: FROM PHYSICAL VIOLENCE TO DIGITAL ABUSE

Modern domestic violence law emerged from feminist activism in the 1970s that challenged law enforcement's reluctance to intervene in family matters and courts' failure to protect battered women. The Violence Against Women Act of 1994 marked a watershed moment, establishing federal leadership in addressing gender-based violence and authorizing over \$1.6 billion for investigation, prosecution, and victim services (Violence Against Women Act, 1994). VAWA's original focus centered on physical violence, sexual assault, and stalking understood primarily through pre-digital paradigms.

The 2000 reauthorization began addressing technology's role by including dating violence and stalking provisions. The 2005 reauthorization represented the first explicit recognition of cyberstalking, expanding federal stalking definitions to encompass electronic communications and surveillance (Violence Against Women and Department of Justice Reauthorization Act, 2005). The 2013 reauthorization strengthened tribal jurisdiction and explicitly addressed cyberstalking using any interactive computer service or electronic communication service (Violence Against Women Reauthorization Act, 2013).

Most significantly, the 2022 VAWA Reauthorization Act introduced comprehensive definitions of technological abuse as acts or patterns of behavior intended to harm, threaten, intimidate, control, stalk, harass, impersonate, exploit, extort, or monitor another person using technology (Violence Against Women Act Reauthorization Act, 2022). This definitional expansion acknowledged that technology-facilitated abuse constitutes a distinct form of violence requiring specialized legal responses. The 2022 reauthorization also authorized grant programs specifically targeting cybercrimes against individuals and established a National Resource Center on Cybercrimes to provide training for law enforcement and judicial personnel.

IV. TECHNOLOGY-FACILITATED DOMESTIC ABUSE: MANIFESTATIONS AND MECHANISMS

Technology-facilitated domestic abuse encompasses diverse tactics that exploit digital infrastructure to perpetuate control and harm. *Surveillance and monitoring* include GPS tracking through phone applications, spyware installation, keylogging software, unauthorized access to email and social media accounts, and exploitation of smart home devices to monitor survivors' movements and communications (Freed et al., 2018). Such pervasive surveillance creates a psychological state of constant monitoring that survivors describe as inescapable, extending abusers' reach into spaces traditionally considered safe.

Image-based sexual abuse, commonly termed revenge porn, involves non-consensual distribution of intimate images to humiliate, intimidate, or coerce survivors. With the advent of artificial intelligence, deepfake pornography--digitally fabricated explicit images appearing to depict real individuals--has emerged as a particularly pernicious form of technological abuse (McGlynn et al., 2017). The threat of image distribution functions as a powerful tool for coercion, forcing survivors to comply with abusers' demands under threat of public humiliation and professional destruction.

Cyberstalking encompasses repeated unwanted communications through email, text messages, social media, and online forums that cause substantial emotional distress or fear. The persistent, boundary-crossing nature of digital communications means survivors cannot escape their abusers by changing physical locations; harassment follows them into every digital space they inhabit. Additionally, *identity theft and impersonation* enable abusers to create fake accounts in survivors' names, post defamatory content, damage professional reputations, and manipulate survivors' social networks (Douglas et al., 2019).

Research indicates that technology-facilitated abuse rarely occurs in isolation but typically accompanies or escalates into physical violence. Survivors experiencing digital coercive control report higher rates of physical assault, sexual violence, and fear for their safety (Dragiewicz et al., 2018). This interconnection underscores the necessity of legal frameworks that recognize technology-facilitated abuse not as a separate category but as integral to contemporary domestic violence patterns.

V. RECENT LEGISLATIVE DEVELOPMENTS: FEDERAL AND STATE RESPONSES

The landscape of legal protections for survivors of digital domestic violence has transformed dramatically between 2022 and 2025. At the federal level, the Take It Down Act, signed into law in May 2025, represents the first comprehensive federal criminalization of non-consensual intimate image distribution (Take It Down Act, 2025). The legislation establishes criminal penalties for knowingly publishing or threatening to share intimate images without consent, including AI-generated deepfake pornography depicting identifiable individuals. Significantly, the Act imposes differential penalties based on victim age: violators face up to two years imprisonment for adult victims and three years for minor victims.

The Take It Down Act also establishes platform accountability requirements, mandating that social media companies, hosting services, and online forums remove non-consensual intimate imagery within 48 hours of notification and implement reasonable measures preventing reposting. This provision addresses the viral nature of digital abuse, where images circulate rapidly across platforms, causing ongoing harm. However, critics note that 48-hour removal timeframes may prove insufficient given the speed of digital distribution and the psychological trauma inflicted even by brief exposure (Franks, 2023).

State-level reforms have demonstrated particular innovation in recognizing coercive control as actionable domestic violence. Massachusetts's Act to Prevent Abuse and Exploitation, enacted in June 2024, criminalized non-consensual intimate image distribution while expanding the definition of abuse under protective order statutes to include coercive control (Commonwealth of Massachusetts, 2024). The legislation defines coercive control as a pattern of behavior intended to threaten, intimidate, harass, isolate, control, coerce or compel compliance of a family or household member that causes fear or a reduced sense of physical safety or autonomy. This definition explicitly encompasses threatening to share explicit images, regulating communications and access to services, and isolating victims from support networks.

By September 2024, Massachusetts became one of the first states to operationalize coercive control provisions, enabling survivors to obtain restraining orders based solely on patterns of non-physical abuse including digital harassment and technological control (Domestic Violence Services Network, 2024). As of mid-2025, all 50 states have enacted criminal statutes addressing non-consensual intimate image distribution, representing remarkable legislative progress achieved through sustained advocacy by survivors, anti-violence organizations, and legal scholars.

VI. IMPLEMENTATION CHALLENGES AND PERSISTENT GAPS

Despite progressive legislative reforms, significant challenges impede effective protection of survivors confronting technology-facilitated abuse. *Enforcement gaps* remain pronounced. Law enforcement officers frequently lack training to recognize and investigate digital domestic violence, viewing online harassment as less serious than physical assault (Bond & Tyrrell, 2021). Police responses to image-based sexual abuse reveal limited understanding of relevant legal frameworks and insufficient confidence investigating cases or supporting survivors.

Jurisdictional complexities compound enforcement challenges. Digital abuse transcends geographic boundaries, with abusers potentially located in different states or countries from their victims. Cross-border cooperation remains inadequate, and international legal frameworks provide minimal recourse for survivors whose abusers operate from jurisdictions with weak or non-existent digital abuse legislation. Even within the United States, variations in state laws create patchwork protections dependent on survivors' locations rather than consistent federal standards.

Platform accountability presents ongoing challenges. While the Take It Down Act mandates content removal within 48 hours, enforcement mechanisms remain unclear. Questions persist regarding liability for platforms failing to comply, procedures for survivors to request removals, and verification processes preventing misuse. Section 230 of the Communications Decency Act, which shields internet platforms from liability for user-generated content, complicates efforts to hold technology companies accountable for facilitating abuse through inadequate moderation policies.

Evidence collection poses particular difficulties in technology-facilitated abuse cases. Digital evidence is easily deleted, devices may be shared or controlled by abusers, and survivors often lack technical knowledge to preserve evidence effectively. Forensic analysis requires specialized expertise and resources that many jurisdictions cannot provide. Furthermore, privacy protections--though essential--can complicate evidence gathering when abusers exploit encrypted communications and privacy-protective technologies to evade detection.

Victim-blaming narratives persist, particularly regarding image-based abuse. Legal proceedings and public discourse frequently focus on survivors' decisions to create intimate images rather than perpetrators' violations of consent and privacy. This victim-blaming approach, evident in questions about why survivors allowed images to be taken, reflects broader rape culture dismissing women's autonomy and excusing male violence. Such attitudes deter survivors from seeking legal remedies and perpetuate shame undermining recovery.

VII. IMPLICATIONS FOR LEGAL PRACTICE AND POLICY DEVELOPMENT

Addressing technology-facilitated domestic abuse requires comprehensive approaches integrating multiple legal and social interventions. First, *specialized training programs* must educate law enforcement, prosecutors, judges, and victim advocates about digital abuse manifestations, investigation techniques, and trauma-informed responses. The 2022 VAWA reauthorization authorized funding for such training, but implementation remains inconsistent across jurisdictions. Investment in continuing education ensuring criminal justice professionals understand technology-facilitated abuse as serious violence meriting robust responses is essential.

Second, *platform regulation* must expand beyond content removal mandates to address design features enabling abuse. Technology companies should implement safety-by-design principles, conducting impact assessments evaluating how platform features might facilitate abuse and developing interventions preventing misuse. Transparency requirements compelling platforms to report abuse prevalence, response times, and mitigation strategies would enhance accountability and enable data-driven policy improvements.

Third, *survivor-centered legal remedies* must prioritize victims' needs and safety. This includes expedited protective order processes addressing digital harassment, civil damages enabling survivors to sue perpetrators for economic and emotional harm, and support services providing technical assistance, mental health counseling, and legal advocacy. Massachusetts's diversion programs for youth who share explicit images represent innovative approaches balancing accountability with education, recognizing that criminal prosecution may prove counterproductive for adolescents requiring guidance rather than incarceration.

Fourth, international cooperation frameworks must develop to address cross-border digital abuse. The Council of Europe's Istanbul Convention provides a model for international domestic violence standards, but technological provisions

require strengthening and broader ratification. Bilateral agreements facilitating evidence sharing, extradition for digital abuse offenses, and coordinated platform regulation would enhance survivors' access to justice when perpetrators exploit jurisdictional gaps.

VIII. CONCLUSION

Legal frameworks protecting survivors of domestic violence in the digital age have undergone remarkable evolution, transitioning from laws designed for pre-internet violence to comprehensive statutes addressing technology-facilitated abuse. The 2022 VAWA Reauthorization Act's definition of technological abuse, the 2025 Take It Down Act's criminalization of non-consensual intimate image distribution, and state-level coercive control legislation represent significant progress toward recognizing digital violence as serious harm requiring legal intervention.

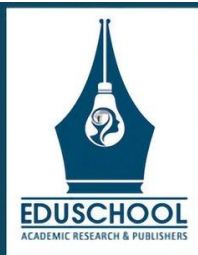
However, persistent implementation challenges—including law enforcement training deficits, jurisdictional complexities, platform accountability gaps, and victim-blaming narratives—demonstrate that legislative reform alone proves insufficient. Effective protection requires sustained investment in specialized training, platform regulation addressing design features enabling abuse, survivor-centered legal remedies prioritizing victims' safety and autonomy, and international cooperation frameworks managing cross-border digital violence.

As technology continues evolving, legal frameworks must remain adaptive, anticipating emerging forms of abuse rather than reacting after harm occurs. The rise of artificial intelligence, virtual reality, and increasingly sophisticated surveillance technologies portends new mechanisms for control and harassment. Policymakers must engage technologists, survivors, advocates, and legal scholars in ongoing dialogue ensuring that laws protect fundamental rights to safety, privacy, and dignity in digital spaces.

Ultimately, addressing technology-facilitated domestic violence requires recognizing that digital and physical abuse constitute interconnected manifestations of gendered violence rooted in patriarchal power structures. Legal frameworks protecting survivors must therefore integrate technical solutions with broader efforts challenging cultural norms normalizing violence against women, promoting digital literacy and safety education, and fostering social conditions where all individuals can live free from fear, control, and harassment—whether experienced through physical force or digital technologies.

REFERENCES

- Bond, E., & Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence*, 36(5–6), 2166–2181. <https://doi.org/10.1177/0886260518760011>
- Centers for Disease Control and Prevention. (2024). *Intimate partner violence*. U.S. Department of Health and Human Services.
- Commonwealth of Massachusetts. (2024). *An Act to prevent abuse and exploitation* (H.4744). Massachusetts Legislature.
- Domestic Violence Services Network. (2024). October 2024: A legal leap forward—MA's new coercive control law. *DVSN News and Updates*. <https://www.dvsn.org/october-2024-a-legal-leap-forward-mas-new-coercive-control-law/>
- Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, 59(3), 551–570.
- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 18(4), 609–625.
- Franks, M. A. (2023). *The cult of the Constitution: Our deadly devotion to guns and free speech*. Stanford University Press.
- Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2018). A stalker's paradise: How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). Association for Computing Machinery.
- Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, 59(3), 530–550.
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, 25(1), 25–46.
- Pence, E., & Paymar, M. (1993). *Education groups for men who batter: The Duluth model*. Springer Publishing Company.
- Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, 34(17), 3637–3665.
- Stark, E. (2007). *Coercive control: How men entrap women in personal life*. Oxford University Press.
- Take It Down Act, S. 146, 119th Cong. (2025).
- Violence Against Women Act of 1994, Pub. L. No. 103-322, tit. IV, 108 Stat. 1902 (1994).
- Violence Against Women Act Reauthorization Act of 2022, Pub. L. No. 117-103, div. W, 136 Stat. 49 (2022).
- Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2006).
- Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, 127 Stat. 54 (2013).

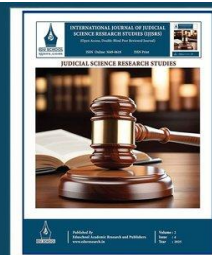


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Smart Contracts in International Arbitration: Legal Challenges in the Blockchain Era

Reyona Elsa Sherin

Student, Department of Law, Kristu Jayanthi University, Bengaluru, Karnataka, India

Article information

Received: 30th May 2026

Received in revised form: 10th June 2026

Accepted: 15th July 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0048>

Abstract

The diffusion of blockchain-based smart contracts is reshaping the landscape of international commercial dispute resolution. Self-executing code that performs contractual obligations without human intervention challenges foundational arbitration doctrines concerning consent, arbitrability, seat, enforceability, and the role of the arbitrator. This paper offers a doctrinal analysis of the intersection between smart contracts and the arbitration frameworks established by the UNCITRAL Model Law on International Commercial Arbitration, the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards 1958, and the institutional rules of the ICC, LCIA, HKIAC, SIAC, and JAMS. The analysis distinguishes automated contracts from purely on-chain blockchain-native agreements and evaluates decentralized dispute-resolution platforms such as Kleros and Aragon Court. Drawing on Niriella's (2024) critical review, the paper identifies four doctrinal pressure points: the form requirements of the arbitration agreement, the seat and *lex arbitri* of code-based transactions, the enforcement of awards against autonomous wallets, and the interaction between decentralized adjudication and the New York Convention. The paper concludes that hybrid human–algorithmic arbitration, supported by explicit choice-of-law and seat provisions, is the most coherent path for reconciling smart contracts with existing arbitration architecture.

Keywords:- Smart contracts, blockchain, international arbitration, UNCITRAL Model Law, New York Convention, decentralized dispute resolution, *lex arbitri*

I. INTRODUCTION

The idea of a self-executing agreement traces at least to Szabo's (1997) formulation of smart contracts as computerized protocols that enforce contractual performance. The emergence of public blockchains, beginning with Bitcoin in 2009 and expanding through Ethereum's programmable virtual machine in 2015, converted that idea from a theoretical device into operational infrastructure (De Filippi & Wright, 2018). Smart contracts now underpin decentralized finance, supply-chain attestation, parametric insurance, intellectual-property licensing, and a growing share of cross-border commercial activity.

The rise of smart contracts disrupts fundamental assumptions of contract law and dispute resolution. Classical doctrine presupposes a contract authored by the parties, interpreted by a tribunal, and enforced by state organs through post-hoc coercion. Smart contracts invert this sequence: enforcement is *ex ante*, embedded in code, and self-executing upon the satisfaction of cryptographically verified conditions. Where disputes arise, the traditional arbitration framework must absorb a transactional object that is partially or wholly machine-authored and whose performance cannot be stopped by judicial injunction without blockchain-level intervention.

International commercial arbitration, the dominant mechanism for resolving cross-border disputes, is presently adapting to this shift. This paper examines four doctrinal pressure points: the form requirements of the arbitration agreement, the seat and *lex arbitri* of code-mediated transactions, the enforcement of awards against wallets and smart contracts, and the status of decentralized dispute-resolution platforms under the New York Convention. The analysis builds on the recent critical examination of Niriella (2024), who treats the role of the smart contract in arbitration with particular attention to the asymmetry between procedural expectations and technological architecture.

II. SMART CONTRACTS: TECHNICAL AND LEGAL ARCHITECTURE

A smart contract, as deployed on contemporary blockchains such as Ethereum, Solana, and Polkadot, is executable code stored at a specific address on a distributed ledger. Its functions are triggered by transactions that meet defined input conditions; upon triggering, the contract modifies state variables and, where relevant, transfers digital assets. The salient technical features for legal analysis are determinism, immutability, transparency, and trustlessness the last referring to the property that performance does not require the parties to trust one another or a central intermediary.

Legal scholarship distinguishes three models of smart-contractual arrangement. The first is the external or ancillary model, in which the smart contract automates performance of a traditional natural-language agreement that remains the legally binding instrument. The second is the hybrid or 'Ricardian' contract, which pairs human-readable prose with machine-executable logic, each referencing the other (Grigg, 2004). The third is the fully code-native agreement, where the code is intended to constitute the agreement itself, with no privileged natural-language text.

Each model raises distinct questions for arbitration. In the external model, standard arbitration clauses embedded in the natural-language document govern. In the hybrid model, divergence between the natural-language and code components generates interpretive conflicts about which version controls. In the fully code-native model, the very existence and content of the arbitration agreement may be contested. Niriella (2024) argues that the hybrid model is likely to dominate near-term commercial practice and that arbitral institutions must develop interpretive protocols for resolving natural-language/code divergence.

III. ARBITRATION FRAMEWORKS AND SMART CONTRACT INTEGRATION

The international arbitration framework rests on three pillars: the UNCITRAL Model Law on International Commercial Arbitration (1985, revised 2006), the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958), and the procedural rules of arbitral institutions. Article 7 of the UNCITRAL Model Law requires that an arbitration agreement be in writing; the 2006 amendments expanded 'writing' to include electronic communications. The New York Convention similarly requires an 'agreement in writing,' defined under Article II(2) to include signed contracts or exchanges of letters and telegrams. The literal text predates blockchain by decades; however, the UNCITRAL Recommendation of 2006 endorses an inclusive interpretation that accommodates digital formats.

A smart contract carrying an embedded arbitration clause, whether expressed in code or in a referenced natural-language document, satisfies the writing requirement under a purposive reading because the agreement is recorded on a persistent, verifiable ledger. The more difficult question is whether the code itself can constitute the arbitration agreement absent any natural-language expression. The prevailing scholarly position is that a pure code clause, without an expression of the parties' intent in a form capable of judicial interpretation, fails the purposive test because it does not communicate the substance of the arbitration undertaking to the enforcing court (Ortolani, 2019; Mik, 2017).

Institutional rules have begun to address these questions. The ICC Arbitration Rules (2021) permit the electronic submission of pleadings; the HKIAC issued guidelines in 2022 on the use of technology in arbitration; JAMS launched a Blockchain Dispute Resolution track; and the Silicon Valley Arbitration and Mediation Center published its Guidelines on the Use of Artificial Intelligence in Arbitration (2024). These developments position institutional arbitration to host smart-contract disputes while preserving doctrinal coherence. Niriella (2024) observes that the cumulative effect is the emergence of a hybrid procedural template in which the automated performance layer coexists with a human tribunal invested with interpretive authority.

IV. JURISDICTIONAL AND ENFORCEMENT CHALLENGES

The *lex arbitri* of a smart-contract transaction is notoriously difficult to determine in the absence of an express choice. A smart contract is deployed to an address that exists on a globally distributed ledger; the nodes validating the contract are located in multiple jurisdictions; the parties may be pseudonymous. Classical connecting factors place of contracting, place of performance, habitual residence become indeterminate or artificial. The most workable solution, adopted in the practice of the HKIAC and SIAC, is to require parties to specify a seat and governing law in the arbitration clause, whether embedded in the code or a paired natural-language document. Where no seat is specified, tribunals have tended to default to the jurisdiction with the closest connection to the parties' off-chain identity, typically their principal place of business.

Enforcement against blockchain-held assets presents distinct challenges. A New York Convention award, once obtained, is enforceable in the 172 contracting states. However, the practical execution of a monetary award denominated in cryptocurrency requires cooperation from exchanges, wallet providers, or in extremis the parties themselves. Decentralized wallets, governed solely by private keys, cannot be compelled through traditional garnishment. Jurisdictions such as Singapore, through the High Court's decision in *CLM v. CLN* (2022), and the United Kingdom, in *AA v. Persons Unknown* (2019), have recognized cryptocurrency as property susceptible to proprietary injunctions, thereby offering a doctrinal bridge between the Convention's enforcement architecture and blockchain-resident assets.

A further layer of complexity arises in the interaction between automated performance and award enforcement. If a smart contract has already executed a disputed transfer by the time an arbitral award issues, the tribunal's remedy is reduced to restitution, which again depends on cooperation or jurisdictional reach. This asymmetry between *ex ante* code execution and *ex post* tribunal authority is the most pronounced conceptual challenge identified by Niriella (2024).

V. DECENTRALIZED DISPUTE RESOLUTION AND THE NEW YORK CONVENTION

Alongside institutional arbitration, a class of decentralized dispute-resolution platforms has emerged on public blockchains. Kleros, launched in 2018, uses a token-weighted juror selection model in which stakeholders are drawn from a

pool, commit staked tokens to a decision, and are rewarded or penalized based on consensus. Aragon Court operates on similar principles, and the Openlaw and Jur platforms offer related services.

The legal status of decisions rendered by these platforms under the New York Convention is contested. An award qualifying under Article I must be made by arbitrators or an arbitral institution in a contracting state. Where the juror pool is globally distributed and the platform lacks a juridical seat, the awards do not readily satisfy the Convention's seat requirement. Ast (2018) has argued that Kleros decisions are more appropriately characterized as contractual determinations or expert decisions than as arbitral awards. If so, enforcement would depend on contractual incorporation into a follow-on arbitration or litigation rather than direct Convention recognition.

A practical compromise is the 'anchor arbitration' model, in which parties incorporate a decentralized-platform determination into a subsequent institutional arbitration clause, thereby preserving Convention enforcement while retaining the efficiency benefits of on-chain adjudication. The HKIAC and JAMS have signaled openness to this hybrid approach, and pilot programs are underway.

VI. RECOMMENDATIONS

Four reforms would substantially clarify the treatment of smart contracts in international arbitration. First, arbitral institutions should issue model smart-contract arbitration clauses that specify the seat, governing law, language, and tribunal composition in machine-readable and human-readable form. The HKIAC's 2022 model clause for technology disputes offers a starting point; parallel initiatives at ICC, SIAC, and LCIA would harmonize practice.

Second, tribunals should develop interpretive protocols for natural-language/code divergence. A presumption in favor of the human-readable document where the code fails to capture the parties' commercial intent accommodates ordinary interpretive expectations while preserving the automation benefits of code.

Third, enforcement-side reforms are required at the national level. Jurisdictions hosting significant cryptocurrency activity should legislate explicit recognition of digital assets as property, standardize the form of proprietary injunctions against on-chain holdings, and establish judicial cooperation channels for wallet identification. Singapore's Payment Services Act 2019 and the UK Law Commission's 2023 Report on Digital Assets provide comparative benchmarks.

Fourth, the UNCITRAL Working Group II on Dispute Settlement should consider a soft-law instrument addressing blockchain-era arbitration agreements. A Model Protocol, without amending the Convention itself, could clarify the writing requirement, the seat, and the interaction with decentralized platforms. Niriella (2024) supports such a calibrated soft-law response as preferable to premature treaty revision.

VII. CONCLUSION

Smart contracts are not replacing arbitration; they are reshaping the transactional substrate on which arbitration operates. The doctrinal challenges are real but manageable within existing frameworks, provided that institutional rules, national enforcement laws, and interpretive protocols evolve in tandem. The paper has argued that a hybrid human–algorithmic model code executing performance, tribunals resolving contested questions, national courts enforcing monetary awards offers the most coherent path.

Two conclusions warrant emphasis. First, the pure code-native model, though theoretically elegant, generates enforcement vulnerabilities that make it unsuitable for high-value cross-border commerce absent a paired natural-language expression. Second, decentralized dispute-resolution platforms are best understood as contractual adjunct mechanisms rather than substitutes for New York Convention arbitration. Building on Niriella's (2024) critical analysis, this paper suggests that the future of smart-contract arbitration lies in structured hybridity: preserving the commercial efficiencies of automation while retaining the interpretive and enforcement guarantees of the existing international framework.

REFERENCES

- Ast, F. (2018). Kleros: A decentralized justice protocol. *Stanford Journal of Blockchain Law and Policy*, 1(1), 1–14.
- CLM v. CLN, [2022] SGHC 46.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Grigg, I. (2004). The Ricardian contract. In *Proceedings of the First IEEE International Workshop on Electronic Contracting* (pp. 25–31). IEEE.
- HKIAC. (2022). *Guidelines on the use of technology in arbitration*. Hong Kong International Arbitration Centre.
- International Chamber of Commerce. (2021). *ICC arbitration rules*.
- Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 9(2), 269–300.
- Niriella, M. A. D. S. J. S. (2024). Role of smart contract in arbitration: A critical analysis. *International Journal of Judicial Science Research Studies*, 43–48. <https://doi.org/10.63090/ijjsrs/3049.0618.0010>
- Ortolani, P. (2019). The impact of blockchain technologies and smart contracts on dispute resolution: Arbitration and court litigation at the crossroads. *Uniform Law Review*, 24(2), 430–448.
- Silicon Valley Arbitration and Mediation Center. (2024). *Guidelines on the use of artificial intelligence in arbitration*.
- Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9).
- UK Law Commission. (2023). *Digital assets: Final report (Law Com No 412)*. The Stationery Office.
- United Nations Commission on International Trade Law. (2006). *UNCITRAL Model Law on International Commercial Arbitration (1985 with amendments as adopted in 2006)*.
- United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, 330 U.N.T.S. 38 (1958).
- Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
- AA v. Persons Unknown, [2019] EWHC 3556 (Comm).



INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Cross-Border Data Protection: Comparative Analysis of GDPR and India's DPDP Act

Sharmila

Indian Institute of Management, Rohtak, India.

Article information

Received: 5th June 2026

Received in revised form: 20th June 2026

Accepted: 12th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0049>

Abstract

The General Data Protection Regulation 2016 and India's Digital Personal Data Protection Act 2023 represent two of the most consequential data-protection instruments globally. They share structural commitments to individual rights, principles-based processing, and accountability-based compliance, while differing in material respects on cross-border transfer mechanisms, sensitive-data classification, public-authority exemptions, regulator independence, and enforcement architecture. This paper offers a comparative doctrinal analysis of the two regimes with particular attention to cross-border data transfers, a site of sustained regulatory innovation since the 2020 Schrems II decision invalidated the EU-US Privacy Shield. It examines the GDPR's Chapter V mechanisms adequacy decisions, standard contractual clauses, binding corporate rules, and derogations—and the DPDP Act's section 16 notified-jurisdictions framework. The paper argues that India's post-2023 position is converging with European practice but retains structural differences in the public-authority and government-access domains that complicate the prospect of a reciprocal adequacy arrangement. It proposes calibrated reforms to support interoperability.

Keywords:- Data protection, GDPR, DPDP Act, cross-border transfers, adequacy, Schrems II, Puttaswamy, digital rights

I. INTRODUCTION

Data protection has become a defining field of twenty-first-century law. The European Union's General Data Protection Regulation (GDPR), in force since May 2018, established a horizontal framework with global influence. India's Digital Personal Data Protection Act 2023 (DPDP Act), enacted in August 2023 and commencing through staged notification, represents the culmination of more than a decade of legislative effort following the Supreme Court's recognition of privacy as a fundamental right in Puttaswamy (2017). The two frameworks jointly govern the personal data of more than 1.8 billion individuals and influence data-protection practice across numerous jurisdictions.

Cross-border data transfers are central to the digital economy and constitute a particular site of regulatory innovation. Cloud services, software-as-a-service, global payment processing, cross-border healthcare, and multinational employee management all depend on the routine movement of personal data across jurisdictional boundaries. Regulatory regimes must reconcile this reality with protective standards that may differ substantially between origin and destination jurisdictions.

This paper offers a comparative doctrinal analysis of the GDPR and the DPDP Act, with particular attention to cross-border transfer mechanisms. It proceeds in six steps: foundational context (Puttaswamy and the GDPR adoption); GDPR core architecture; DPDP Act structure and scope; cross-border transfer mechanisms under each regime; gaps, convergences, and interoperability prospects; and recommendations. The paper argues that Indian law is broadly converging with European practice, with residual differences concentrated in public-authority exemptions and government-access frameworks that may complicate the prospect of reciprocal adequacy.

II. PRIVACY AS A FUNDAMENTAL RIGHT: PUTTASWAMY'S LEGACY

The Indian Supreme Court's unanimous Nine-Judge Bench decision in *K. S. Puttaswamy v. Union of India* (2017) held that the right to privacy is a fundamental right under Part III of the Constitution, protected under articles 14, 19, and 21. The judgment articulated a tripartite test for legitimate interference:

- legality, requiring a basis in validly enacted law;
- necessity, meaning a legitimate state aim; and
- proportionality, requiring that the measure be the least restrictive means to achieve the aim.

The decision grounded subsequent privacy jurisprudence, including *Puttaswamy II* (2018) on Aadhaar and subsequent data-protection developments.

The Puttaswamy framework mirrors the Charter of Fundamental Rights of the European Union's Article 8 on personal data protection and the European Court of Human Rights' Article 8 jurisprudence on private life. The GDPR gives effect to Charter Article 8 and ECHR Article 8 through comprehensive statutory implementation, including the appointment of independent supervisory authorities, codification of data-subject rights, and robust enforcement mechanisms with administrative fines up to EUR 20 million or 4 percent of global annual turnover.

The trajectory from Puttaswamy to the DPDP Act was lengthy. The Srikrishna Committee's 2018 draft, the Personal Data Protection Bill 2019, and iterative revisions preceded the DPDP Bill 2022 and the enacted DPDP Act 2023. The final text diverges in material respects from the Srikrishna draft, including on data-localization, public-authority exemptions, and regulator appointment mechanisms.

III. GDPR: CORE ARCHITECTURE

The GDPR applies to the processing of personal data by controllers and processors either established in the European Union or targeting data subjects in the European Union (Articles 2 and 3). It articulates six processing principles in Article 5: lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality, with accountability as an overarching principle.

Lawful bases for processing (Article 6) include consent, contractual necessity, legal obligation, vital interests, public task, and legitimate interests. Special categories of data (Article 9) racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometric data, health, and sexual orientation are subject to heightened protection with an additional set of narrow permissions.

Data-subject rights (Articles 12–22) include the rights to information, access, rectification, erasure, restriction, data portability, objection, and protection against solely automated decision-making with legal or similarly significant effects. These rights are individually actionable and supported by the supervisory authorities' investigatory and enforcement powers under Chapter VI and VII.

Cross-border transfers are governed by Chapter V. A transfer to a third country or international organization requires either:

- an adequacy decision by the Commission;
- appropriate safeguards such as standard contractual clauses, binding corporate rules, approved codes of conduct, or certification schemes; or
- derogation for specific situations under Article 49. \

The Court of Justice's *Schrems II* decision (2020) invalidated the EU-US Privacy Shield adequacy decision and conditioned SCC use on case-by-case assessment of third-country law, with supplementary measures as needed. The EU-US Data Privacy Framework adopted in July 2023 restored an adequacy decision for certified US organizations, subject to ongoing legal challenge.

IV. DPDP ACT 2023: STRUCTURE AND SCOPE

The DPDP Act applies to the processing of digital personal data within India and to processing outside India in connection with offering goods or services to data principals in India (section 3). The Act is notably concise relative to the GDPR twenty-five numbered sections plus definitions and schedules reflecting a principles-based design with significant implementation to be specified in subordinate rules.

Core provisions include consent as the default lawful basis (section 6), with 'legitimate uses' serving as a limited additional basis (section 7) covering specified situations such as government services, medical emergencies, and employment contexts. Data fiduciaries (equivalent to GDPR controllers) owe duties of accurate processing, data minimization, security safeguards, breach notification to the Data Protection Board and affected data principals, and limited retention (section 8).

Data-principal rights (Chapter III) include rights to information, correction and erasure, grievance redress, and nomination. The Act does not include a right to data portability or a specific right analogous to GDPR Article 22 on automated decision-making, gaps that have attracted scholarly criticism.

The enforcement architecture centers on the Data Protection Board of India (sections 18–27). The Board may impose penalties up to INR 2.5 billion (approximately EUR 25 million) per violation. Critics note that the Board's appointment by the Central Government, absence of judicial-power recognition, and limited procedural safeguards create concerns about regulator independence. The Act provides substantial exemptions for government processing, including where the Central Government notifies an instrumentality as exempted under section 17(2).

Significantly, the DPDP Act's treatment of cross-border transfers (section 16) shifts away from the localization models of earlier drafts. The Central Government may restrict transfers to specified jurisdictions by notification; in the absence of

such restriction, transfers are permitted. This 'blacklist' approach contrasts with the GDPR's 'whitelist' adequacy model and with the localization requirements of some other jurisdictions.

V. CROSS-BORDER TRANSFER MECHANISMS AND ADEQUACY PROSPECTS

The GDPR and DPDP Act adopt structurally different approaches to cross-border transfers. The GDPR restricts transfers to third countries absent adequacy, appropriate safeguards, or derogations, reflecting a precautionary logic that places the burden of protection on the exporter. The DPDP Act permits transfers except to notified restricted jurisdictions, reflecting a permissive default with discretionary governmental restriction.

The practical implications differ. Under the GDPR, an Indian data importer handling EU personal data must rely on the EU-Indian adequacy decision (not currently in place), SCCs supplemented by case-by-case assessment under Schrems II, binding corporate rules, or Article 49 derogations. The EU has not issued an adequacy decision for India; the Schrems II assessment burden is non-trivial, particularly in view of Indian government-access frameworks such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 and the Telecommunications (Temporary Suspension of Services) Rules 2017.

Under the DPDP Act, an EU data importer handling Indian personal data need only comply with the Act's general obligations, subject to restriction notifications under section 16. This asymmetry—stricter EU restrictions on outbound transfers to India, combined with more permissive Indian restrictions on outbound transfers to the EU creates a de facto imbalance in cross-border flows.

The prospects for an EU-India adequacy decision depend on three factors. First, the extent to which the DPDP Act's rule-specified operational details provide protections comparable to the GDPR, particularly on data-principal rights, regulator independence, and enforcement. Second, the treatment of government-access requests under Indian law, including the interaction with the Information Technology Act 2000's section 69 and recent decisions on surveillance-law constitutionality. Third, institutional trust between the Commission and the Indian authorities. Recent negotiations on EU-India trade and digital-economy cooperation have created some momentum, but the adequacy-specific dialogue remains at an early stage.

Bilateral corporate mechanisms offer a more immediate path. SCCs may be adapted for EU-India transfers; emerging Indian SCCs, if promulgated under DPDP Act rules, could be reciprocally recognized. The ASEAN Model Contractual Clauses and APEC Cross-Border Privacy Rules provide potential templates for regional harmonization.

VI. CONVERGENCES, DIVERGENCES, AND GAPS

Four convergences are notable. First, both regimes enshrine consent as the presumptive lawful basis for processing. Second, both regulate data-controller/fiduciary accountability through obligations of purpose limitation, minimization, security, and breach notification. Third, both provide individual rights of access, correction, and erasure. Fourth, both adopt an extraterritorial scope that captures processing outside the regulating jurisdiction where directed at data subjects within.

Four divergences are significant. First, the DPDP Act lacks an Article 22 equivalent on solely automated decision-making, leaving Indian individuals without an explicit right to contest algorithmic decisions. Second, the DPDP Act does not classify data categories with the GDPR's specificity; all personal data is subject to uniform protection, though sensitive-data designation may emerge through rules. Third, the DPDP Act's public-authority exemptions are broader than the GDPR's, particularly under section 17(2). Fourth, regulator independence and procedural safeguards in enforcement differ, with the Data Protection Board more closely tied to executive appointment than the typical GDPR supervisory authority.

Beyond these structural differences, implementation gaps are significant. The DPDP Act's commencement is staged through rule notification; at the time of writing, key rules on data-fiduciary classifications, cross-border restrictions, children's data, and grievance mechanisms are at varying stages of consultation. Effective protection depends heavily on rule-level specification and on the eventual operational capacity of the Data Protection Board.

VII. RECOMMENDATIONS AND CONCLUSION

Five reforms would strengthen interoperability between the GDPR and DPDP Act frameworks. First, the DPDP Act rules should specify categories of sensitive data subject to heightened protection, drawing on the GDPR Article 9 taxonomy adapted for Indian context. Second, provisions analogous to GDPR Article 22 on automated decision-making should be introduced, either in the DPDP Act or through a successor Digital India Act. Third, regulator independence should be strengthened through staggered appointments, judicial involvement in selection, and enhanced procedural protections.

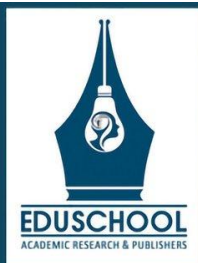
Fourth, cross-border transfer mechanisms should be specified with clarity. The DPDP Act's section 16 notification framework should be complemented by Indian standard contractual clauses and a pathway for EU-India adequacy dialogue. Reciprocal recognition of binding corporate rules, building on EU practice, would support multinational compliance.

Fifth, government-access frameworks should be reformed to meet the proportionality and accountability standards implied by Puttaswamy. Modernization of surveillance laws, judicial authorization requirements, and transparency reporting would align Indian practice with international standards and support adequacy dialogues.

This paper has argued that the GDPR and DPDP Act represent convergent but distinct approaches to data protection. Convergence is substantial on principles and individual rights; divergence persists on public-authority exemption, regulator independence, and government-access architecture. Closing these gaps would strengthen both frameworks, support cross-border data flows, and ensure that the Puttaswamy promise of privacy as a fundamental right is operationalized in the digital economy. Data protection is no longer a technical specialism; it is a foundational layer of twenty-first-century law.

REFERENCES

- Asia-Pacific Economic Cooperation. (2011). *APEC cross-border privacy rules system*.
- Association of Southeast Asian Nations. (2021). *ASEAN model contractual clauses for cross-border data flows*.
- Charter of Fundamental Rights of the European Union. (2012). *Official Journal of the European Union*, C 326, 391.
- Court of Justice of the European Union. (2020). *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II)*, Case C-311/18, EU:C:2020:559.
- Court of Justice of the European Union. (2023). *SCHUFA Holding AG v. OQ*, Case C-634/21, EU:C:2023:957.
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India.
- European Commission. (2023). *Commission implementing decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final.
- European Data Protection Board. (2021). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*.
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. (2016). *Official Journal of the European Union*, L 119, 1.
- Greenleaf, G. (2023). India's data protection act 2023: Rules await to fill in many gaps. *Privacy Laws & Business International Report*, 183, 1–9.
- Information Technology Act, No. 21 of 2000, Acts of Parliament, India.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. (2021). India.
- Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.
- Puttaswamy v. Union of India (Puttaswamy I), (2017) 10 SCC 1 (India).
- Puttaswamy v. Union of India (Puttaswamy II – Aadhaar), (2019) 1 SCC 1 (India).
- Srikrishna, B. N. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna.

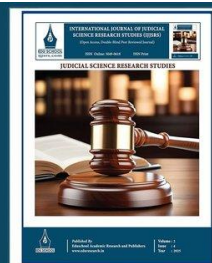


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Regulating Mental Health Telemedicine: Cross-Jurisdictional Challenges and Policy Responses

Amal Krishna S

Student, Department of Law, Christ Academy Institute of Law, Bangalore, Karnataka, India

Article information

Received: 21st May 2026

Received in revised form: 17th June 2026

Accepted: 18th July 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0050>

Abstract

Mental health telemedicine has expanded at unprecedented scale since 2020, transforming psychiatric and psychological services from predominantly in-person to hybrid digital delivery. This transformation has exposed the inadequacy of regulatory frameworks originally designed for face-to-face clinical encounters. This paper offers a comparative analysis of the regulation of mental-health telemedicine in India, the United States, and the United Kingdom. It examines licensing, standard of care, informed consent, data protection, cross-border practice, and emergency-protocol requirements, drawing on India's Telemedicine Practice Guidelines 2020 and Mental Healthcare Act 2017, the US Ryan Haight Online Pharmacy Consumer Protection Act 2008 and state telehealth statutes, and the UK's General Medical Council Remote Prescribing Guidance 2020 and Data Protection Act 2018. The analysis engages the recent contribution of P and Venkateswarlu (2025) and identifies three convergent trends—standard-of-care equivalence, data-minimization mandates, and suicide-risk protocols and three areas of persistent divergence—licensing portability, controlled-substance prescribing, and cross-border provider accountability. The paper proposes a tiered international framework to reconcile patient mobility with regulatory coherence.

Keywords:- Mental health, telemedicine, teletherapy, data protection, licensing, comparative health law, cross-border care

I. INTRODUCTION

The delivery of mental-health services has undergone a structural shift. Before 2020, telemental-health represented a small percentage of psychiatric and psychological encounters in most jurisdictions; by the end of 2022, it accounted for more than half of all outpatient psychiatric sessions in the United States and a rising share in India and the United Kingdom (American Psychiatric Association, 2022; NHS Digital, 2022). Pandemic-era emergency waivers catalyzed adoption, and substantial portions of that adoption have proved durable.

The regulatory architecture, however, was not designed for this scale or modality. Licensing regimes assume geographic practice; standard-of-care doctrines presuppose physical examination; informed-consent requirements rest on face-to-face interactions; and emergency-response protocols were developed for in-person clinic settings. Mental-health care poses particular regulatory challenges because the standard of care often hinges on non-verbal observation, because crisis situations such as acute suicidality require rapid in-person intervention, and because the therapeutic relationship depends on trust that may be mediated differently across digital channels.

This paper compares the regulatory responses of three jurisdictions that host substantial telemental-health markets: India, the United States, and the United Kingdom. Building on the comparative study of P and Venkateswarlu (2025), the analysis identifies convergences, divergences, and policy gaps, and proposes a tiered international framework to address cross-border practice.

II. THE EMERGENCE OF TELEPSYCHIATRY AND POLICY DRIVERS

Mental-health demand in all three jurisdictions exceeds the supply of licensed providers. India has approximately one psychiatrist per 100,000 population against a WHO-recommended ratio of three; the United Kingdom faces waits of weeks to months for NHS psychological therapies; the United States struggles with regional maldistribution, with acute shortages in

rural counties (World Health Organization, 2021). Telemental-health addresses the geographic mismatch between demand and supply, enables lower-friction access for populations facing stigma, and allows specialist providers to serve underserved regions without relocation.

Three policy drivers have shaped regulation. First, public-health emergencies have catalyzed provisional regulatory relaxations; most jurisdictions have subsequently converted emergency measures into permanent reforms. Second, parity movements have sought to equate telemental-health reimbursement and legal standing with in-person care. Third, digital-health innovation has introduced asynchronous modalities text-based therapy, app-mediated cognitive behavioral therapy, AI-supported triage whose regulatory status remains unsettled.

The regulatory response has broadly converged on standard-of-care equivalence, meaning that provisions must meet the same professional standard whether delivered in person or remotely. Divergence persists in licensing reciprocity, controlled-substance prescribing, and the treatment of asynchronous and AI-augmented services.

III. INDIAN REGULATORY LANDSCAPE

India's regulatory framework for mental-health telemedicine rests on three principal instruments: the Telemedicine Practice Guidelines 2020 issued by the Board of Governors in supersession of the Medical Council of India; the Mental Healthcare Act 2017; and sectoral rules issued by the National Medical Commission. The Telemedicine Practice Guidelines establish the first national framework permitting registered medical practitioners to provide teleconsultation. They distinguish first consultations, in which caution governs prescribing, from follow-up consultations where the therapeutic relationship is established. Category-specific prescription restrictions apply: medicines listed in Schedule X and most narcotic substances require in-person evaluation and cannot be prescribed via teleconsultation alone.

The Mental Healthcare Act 2017 adopts a rights-based framework for mental-health services, including the right to access, the right to community living, advance directives, and a regulatory structure of Mental Health Review Boards at state and central levels. The Act does not specifically address telemedicine, but its rights-based architecture applies equally to digital delivery. The right to confidentiality under section 23 and the right to informed consent under section 86 are particularly salient for digital encounters.

The Digital Personal Data Protection Act 2023 (DPDP Act) supplements these frameworks by regulating the processing of personal data, including health data. Consent is the default lawful basis; data fiduciaries must provide notice, secure consent, and implement reasonable safeguards. The Act does not yet designate health data as sensitive personal data with heightened protection, a gap that P and Venkateswarlu (2025) identify as requiring urgent remediation given the specific sensitivity of mental-health information.

Gaps in the Indian framework include the absence of specific protocols for psychologists and counsellors (who are not 'medical practitioners' under the Telemedicine Guidelines), the lack of standardized consent forms for digital mental-health services, and limited guidance on emergency-response protocols for acute suicidality during teleconsultations. The National Mental Health Policy 2014 is due for revision to incorporate these digital-era considerations.

IV. UNITED STATES REGULATORY APPROACH

The United States regulates telemental-health through an intersecting system of federal and state instruments. Federally, the Ryan Haight Online Pharmacy Consumer Protection Act 2008 requires at least one in-person medical evaluation before prescribing a controlled substance through telemedicine, subject to defined exceptions. The Act's applicability to buprenorphine and other medications used in mental-health treatment has been temporarily relaxed under public-health emergency declarations; the Drug Enforcement Administration has iterated through proposed rules to formalize a permanent framework.

State law governs licensing. A practitioner must generally hold a license in the state where the patient is physically located at the time of the consultation. The Interstate Medical Licensure Compact, adopted by forty states and the District of Columbia, expedites but does not eliminate state-by-state licensure. Psychology licensing is addressed through the PSYPACT compact, which permits telepsychology practice across member jurisdictions under an authorization to practice interjurisdictionally. Neither compact provides full portability.

The Health Insurance Portability and Accountability Act 1996 (HIPAA) establishes the federal privacy and security framework for protected health information. HIPAA's Privacy Rule restricts disclosure; the Security Rule mandates technical, administrative, and physical safeguards for electronic protected health information. HIPAA's applicability to app-based mental-health services has generated significant enforcement activity, particularly in 2023–2024, as the Federal Trade Commission has pursued consent decrees against apps that shared sensitive data with advertisers.

The Mental Health Parity and Addiction Equity Act 2008 requires insurance plans offering mental-health coverage to provide parity with medical and surgical benefits; the Consolidated Appropriations Act 2021 strengthened enforcement. Telemental-health reimbursement has been expanded under Medicare and most state Medicaid programs through post-pandemic legislation, though specific parity questions around asynchronous care remain unsettled.

V. UNITED KINGDOM REGULATORY APPROACH

The United Kingdom regulates telemental-health through a combination of professional-body guidance, data-protection statute, and NHS commissioning frameworks. The General Medical Council's Remote Consultations and Prescribing Guidance 2020 establishes that remote consultations must meet the same standards as in-person care, including thorough clinical assessment, safeguarding, and record-keeping. The British Association for Counselling and Psychotherapy and the Health and Care Professions Council have issued parallel guidance for psychologists, psychotherapists, and counselling professionals.

The Data Protection Act 2018 implements the UK General Data Protection Regulation (UK GDPR), with special-category protections for health data under Article 9. Controllers must identify a lawful basis under Article 6 and a condition

under Article 9, typically consent for non-clinical services or provision of health care for clinical services. The Information Commissioner's Office has issued specific guidance on telehealth applications, emphasizing data-minimization, purpose-limitation, and controller accountability.

NHS England's Digital Mental Health Service Assessment provides an accreditation framework for digital tools commissioned into NHS mental-health pathways. The Improving Access to Psychological Therapies (IAPT) program, since renamed NHS Talking Therapies, has incorporated substantial digital components including internet-enabled cognitive behavioral therapy (iCBT).

The UK framework is notable for its integration of professional-body, statutory, and service-commissioning standards. Gaps include the unclear regulatory status of direct-to-consumer mental-health apps operating outside NHS pathways, cross-border practice issues following Brexit's effect on European health professional recognition, and emergency-response coordination for acute presentations.

VI. DATA PROTECTION, LICENSING, AND CROSS-BORDER CHALLENGES

Three issues dominate the comparative landscape. First, data protection for mental-health information. All three jurisdictions afford heightened protection, but the architecture differs. The US HIPAA framework is sectoral and applies only to covered entities; the UK GDPR framework is horizontal and treats health data as a special category across all controllers; the Indian DPDP Act 2023 currently treats all personal data uniformly, pending sector-specific rules. Convergence on data minimization, purpose limitation, and breach notification is substantial; divergence on the scope of 'covered' activities and the applicability to direct-to-consumer apps is significant.

Second, licensing portability. The US is moving toward compact-based interstate practice for physicians and psychologists, but portability remains limited. The UK recognizes health professionals registered with the General Medical Council, Nursing and Midwifery Council, and Health and Care Professions Council, with restricted post-Brexit arrangements for European Economic Area qualifications. India operates a state-registration system under the National Medical Commission Act 2019 with limited interstate reciprocity. Cross-border telehealth between the three jurisdictions is legally precarious.

Third, emergency-response protocols. Acute mental-health crises during teleconsultation suicide ideation, acute psychosis, imminent risk of harm require rapid in-person intervention, which in turn depends on local emergency services and verification of the patient's physical location. Protocols in all three jurisdictions require the practitioner to verify the patient's location at the outset of the session and to maintain local emergency-contact information. The UK's IAPT program includes the most developed risk-stratification protocols; US and Indian frameworks rely on individual-practitioner discretion within broad guidance. P and Venkateswarlu (2025) emphasize the urgency of harmonizing emergency-response standards, particularly for cross-border care.

VII. RECOMMENDATIONS AND CONCLUSION

Reform should advance along four axes. First, jurisdictions should codify data-protection provisions specific to mental-health information, including restrictions on secondary uses, retention limits for session recordings, and required disclosures at the point of service. India's DPDP Act framework requires sector-specific rules that elevate mental-health data to a sensitive category.

Second, licensing portability should be expanded. Bilateral recognition agreements, modeled on the IMLC and PSYPACT compacts, could extend portability for mental-health practice between jurisdictions with comparable training and ethical standards. The World Health Organization's 2018 Global Strategy on Digital Health provides a coordinating framework.

Third, emergency-response protocols should be standardized. A minimum set of requirements location verification, documented emergency-contact person, local crisis-line integration, risk-assessment documentation should be adopted across jurisdictions as a condition of teleconsultation practice.

Fourth, specific frameworks for non-physician mental-health providers (psychologists, counsellors, social workers) and for asynchronous and AI-augmented services should be developed. India's Telemedicine Practice Guidelines, currently limited to registered medical practitioners, should be expanded; the FDA's Software-as-a-Medical-Device framework and the MHRA's 2023 guidance on digital mental-health tools provide reference models.

Building on P and Venkateswarlu's (2025) comparative analysis, this paper concludes that regulatory convergence has progressed substantially but that meaningful cross-border practice requires bilateral coordination on data flows, licensing, and emergency response. Mental-health telemedicine has demonstrated its clinical and social value; regulatory infrastructure should be brought into alignment with that demonstrated value.

REFERENCES

- American Psychiatric Association. (2022). *Telepsychiatry toolkit: Practice guidance*. American Psychiatric Association Publishing.
- Consolidated Appropriations Act, Pub. L. No. 116–260, 134 Stat. 1182 (2021).
- Data Protection Act 2018, c. 12 (UK).
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India.
- General Medical Council. (2020). *Remote consultations and prescribing: Good practice guidance*. GMC.
- Health and Care Professions Council. (2021). *Guidance on the use of technology*.
- Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (U.S.).
- Information Commissioner's Office. (2023). *Guidance on data protection in telehealth*. ICO.
- Mental Health Parity and Addiction Equity Act of 2008, Pub. L. No. 110–343, 122 Stat. 3765 (U.S.).
- Mental Healthcare Act, No. 10 of 2017, Acts of Parliament, India.
- National Medical Commission. (2020). *Telemedicine practice guidelines*. Government of India.
- NHS Digital. (2022). *Mental health services monthly statistics*. NHS Digital.

- P, V., & Venkateswarlu, C. (2025). Digital minds, analog laws: A comparative study of regulatory frameworks governing mental health telemedicine in India, the US, and the UK. *International Journal of Judicial Science Research Studies (IJJSRS)*, 2(4), 122. <https://doi.org/10.63090/ijjsrs/3049.0618.0038>
- Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub. L. No. 110–425, 122 Stat. 4820 (U.S.).
- UK General Data Protection Regulation (retained EU law as amended).
- World Health Organization. (2018). *Global strategy on digital health 2020–2025*. WHO.
- World Health Organization. (2021). *Mental health atlas 2020*. WHO.

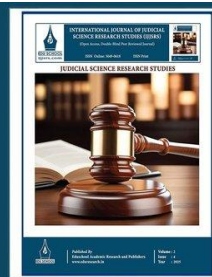


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Artificial Intelligence and Legal Accountability: Frameworks for Algorithmic Governance

Vinothini S

Sathyabama School of Law, Chennai, India

Article information

Received: 29th May 2026

Received in revised form: 13th June 2026

Accepted: 4th July 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0051>

Abstract

The accelerating deployment of artificial intelligence systems in consequential decision-making credit scoring, employment screening, welfare eligibility, criminal justice, and healthcare has outpaced the development of legal accountability frameworks. This paper offers a comparative analysis of emerging regulatory responses to algorithmic harm across three jurisdictions: the European Union's Artificial Intelligence Act 2024, the United States' sectoral and state-law approach, and India's Digital Personal Data Protection Act 2023 and proposed Digital India Act. The analysis constructs a typology of algorithmic harms discrimination, opacity, safety failures, and informational manipulation and evaluates the regulatory tools addressing each type: risk classification, conformity assessment, data-protection impact assessments, transparency obligations, human oversight, and ex post liability. The paper argues that the EU's risk-based horizontal approach and the US sectoral approach each capture different but partial dimensions of algorithmic accountability, while the Indian framework remains under-specified. It proposes a convergent framework combining horizontal transparency obligations with sectoral risk regulation and a sustainable liability regime.

Keywords:- Artificial intelligence, algorithmic accountability, EU AI Act, GDPR Article 22, risk-based regulation, automated decision-making

I. INTRODUCTION

Artificial intelligence systems are increasingly deployed in decisions that have substantial consequences for individual life chances. Credit-scoring models allocate credit; employment-screening tools shortlist candidates; predictive-policing systems influence enforcement resource allocation; automated welfare-eligibility systems determine social-assistance benefits; medical-diagnostic systems inform treatment decisions. The speed and scale at which these deployments have proceeded has produced a growing catalog of algorithmic harms: discriminatory outcomes replicated or amplified from training data, opaque decision processes that preclude meaningful review, safety failures in high-stakes applications, and informational manipulation through recommender systems and content moderation.

Legal and regulatory responses have accelerated in the 2020s. The European Union's Artificial Intelligence Act, adopted in 2024, represents the most comprehensive horizontal framework to date. The United States has pursued a mixed strategy of sectoral regulation, state-level statutes, and executive-branch initiatives, supplemented by the White House Blueprint for an AI Bill of Rights (2022) and Executive Order 14110 (2023). India's Digital Personal Data Protection Act 2023 establishes foundational data-protection rules, with a proposed Digital India Act to supersede the Information Technology Act 2000 expected to introduce AI-specific provisions.

This paper offers a comparative analysis of these three regulatory frameworks with particular attention to the doctrinal instruments they employ, the harms they address, and the gaps they leave. It argues that algorithmic accountability is best conceived as a multi-layered problem requiring horizontal transparency obligations, sectoral risk regulation, and a functional liability regime.

II. ALGORITHMIC HARMS: A TYPOLOGY

Scholarship on algorithmic harm has converged on a rough taxonomy of four categories. First, discrimination, encompassing decisions that produce unjustified disparate impact or disparate treatment against protected groups. Well-documented cases include the ProPublica investigation of the COMPAS recidivism-risk tool (Angwin et al., 2016), gender bias in Amazon's now-abandoned employment-screening system, racial bias in facial-recognition systems (Buolamwini & Gebru, 2018), and disparate mortgage-lending outcomes from automated underwriting.

Second, opacity, referring to the inability of affected persons, decision-makers, or oversight bodies to understand or audit the basis of algorithmic decisions. Pasquale (2015) described the 'black box society' produced by commercial secrecy, technical complexity, and deep-learning architectures that resist interpretation. The resulting accountability gap affects both individual redress and systemic governance.

Third, safety failures, particularly in applications where algorithmic error can cause physical or serious economic harm: medical diagnostic errors, autonomous-vehicle failures, algorithmic trading-driven financial instability. These harms raise issues of product liability, professional responsibility, and regulatory oversight that extend beyond pure algorithmic-governance doctrines.

Fourth, informational manipulation, including recommender-system amplification of misinformation, political microtargeting, and content-moderation decisions that shape public discourse. These harms raise free-speech concerns alongside algorithmic-accountability concerns, creating tensions that complicate regulatory design.

A coherent regulatory framework must address all four categories, though not necessarily with identical instruments. The typology also helps to identify blind spots: for example, most existing regulations focus on discrimination and opacity in individual decisions, with less attention to systemic informational harms and safety failures.

III. THE EU AI ACT: RISK-BASED HORIZONTAL REGULATION

The EU AI Act (Regulation 2024/1689) adopts a horizontal, risk-based framework. AI systems are classified into four risk tiers. Prohibited practices (Article 5) include social scoring by public authorities, untargeted scraping of facial images for recognition databases, emotion-recognition systems in workplaces and schools (with defined exceptions), and certain predictive-policing applications. High-risk systems (Article 6 and Annex III) include biometric identification, critical-infrastructure management, education and vocational training, employment and worker management, access to essential services, law enforcement, migration, administration of justice, and democratic processes. High-risk systems are subject to rigorous obligations: risk-management systems, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and cybersecurity. General-purpose AI models (Article 51 ff.) face transparency and documentation obligations, with systemic-risk designation triggering additional requirements. Limited-risk systems face transparency obligations (disclosure that the user is interacting with an AI system, disclosure of deep fakes). Minimal-risk systems remain largely unregulated.

The Act's strengths include its horizontal reach, its coverage of general-purpose models, and its integration with existing product-safety and conformity-assessment infrastructure. Its structural weaknesses include the list-based approach to high-risk classification, which may prove insufficiently agile as AI applications evolve; the extended implementation timeline (phased from 2025 through 2027); and the potential for forum-shopping through EU Member State designation of national competent authorities.

The Act interacts with the General Data Protection Regulation. GDPR Article 22 prohibits decisions based solely on automated processing that produce legal or similarly significant effects, subject to exceptions for contractual necessity, authorization by Union or Member State law, or explicit consent; where permitted, safeguards including human intervention, contesting, and explanation must be provided. The 2023 SCHUFA decision of the Court of Justice of the European Union clarified that credit-scoring systems fall within Article 22 even where a human formally implements the output. The AI Act and the GDPR together form the regulatory core, complemented by the Digital Services Act 2022 for online platforms and the proposed AI Liability Directive.

IV. US SECTORAL AND STATE-LEVEL APPROACH

The United States has not enacted a horizontal AI statute. Federal regulation proceeds through sectoral authorities: the Equal Employment Opportunity Commission's 2023 technical assistance on employer use of algorithmic tools; the Federal Trade Commission's unfair-or-deceptive-practices enforcement against algorithmic misrepresentation; the Consumer Financial Protection Bureau's application of the Equal Credit Opportunity Act and Fair Credit Reporting Act to algorithmic lending; the Department of Health and Human Services' Algorithmic Accountability Framework in healthcare; the Securities and Exchange Commission's 2023 proposed rule on predictive-data-analytics conflicts of interest.

Executive Order 14110 of October 2023 directed agencies to implement AI safety testing, red-teaming, critical-infrastructure protection, and immigration-adjacent AI reviews. The order was partially rescinded and replaced by Executive Order 14179 (January 2025), reflecting the administration's preference for lighter-touch regulation while preserving safety-evaluation elements.

State legislation has been active. Illinois' Artificial Intelligence Video Interview Act (2020) requires candidate disclosure of AI use in video interviews. The Colorado Artificial Intelligence Act (2024) imposes duties on developers and deployers of 'high-risk' AI systems affecting consequential decisions. New York City Local Law 144 (2023) requires bias audits of automated employment-decision tools. California's SB 1047 on frontier-model safety was passed and vetoed in 2024, with successor legislation under consideration.

The US approach's strengths include sectoral expertise and regulatory flexibility. Its weaknesses include fragmentation, enforcement gaps where sectoral coverage is thin (notably in political advertising and social-media platforms), and the patchwork burden on multijurisdictional operators. Industry preferences for preemptive federal legislation reflect this concern.

V. INDIAN REGULATORY LANDSCAPE AND THE DPDP GAP

India's current framework for AI governance rests on three instruments. First, the Information Technology Act 2000 and Rules regulate intermediary liability, data-security obligations, and digital-communications offenses, but do not directly address algorithmic accountability. Second, the Digital Personal Data Protection Act 2023 establishes a horizontal personal-data framework with consent-based processing, purpose limitation, data-minimization, and breach notification, but does not contain specific provisions on automated decision-making analogous to GDPR Article 22. Third, the Niti Aayog's Principles for Responsible AI (2021) and subsequent policy papers offer non-binding guidance. The proposed Digital India Act, expected to supersede the IT Act 2000, has been in consultation since 2023 and is anticipated to introduce high-risk AI classifications and online-platform obligations.

The absence of a GDPR-equivalent Article 22 is a particular gap. Indian consumers confronted by algorithmic credit denial, insurance-eligibility determination, or employment screening lack the GDPR's foundational right to contest and obtain human review of solely automated decisions. The Supreme Court's 2017 Puttaswamy decision established privacy as a fundamental right, providing a constitutional basis for future recognition of algorithmic-accountability rights, but statutory specification remains pending.

Additional initiatives include the Ministry of Electronics and Information Technology's 2024 Advisory on AI Platforms (requiring explicit government approval for certain under-tested AI deployments, subsequently softened following industry pushback), the Reserve Bank of India's 2024 guidelines on lending-platform liability, and the Competition Commission of India's 2024 study on algorithmic harms in digital markets. A horizontal framework integrating these developments with the DPDP Act remains the structural next step.

VI. RECOMMENDATIONS

Five reforms would strengthen algorithmic accountability across the comparative landscape. First, horizontal transparency obligations should be specified. A minimum requirement that affected persons be informed when consequential decisions are made by automated systems, together with a right to meaningful explanation and a right to human review, should be common across jurisdictions. GDPR Article 22 provides the base model; India's DPDP Act should be amended or supplemented to incorporate equivalent provisions.

Second, sectoral risk regulation should complement horizontal transparency. High-stakes sectors credit, employment, healthcare, criminal justice, education, welfare should be subject to specific obligations on data governance, testing, and monitoring, as in the EU AI Act's Annex III classification.

Third, liability regimes should be adapted. The EU's proposed AI Liability Directive and the updated Product Liability Directive (2024) extend product-liability concepts to software and AI-system damage; analogous approaches should be considered in the US and India. A 'joint and several' regime for developers and deployers, with appropriate contractual allocation, supports accountability where fault allocation among actors is complex.

Fourth, international coordination is essential to prevent regulatory arbitrage. The OECD AI Principles 2019 and the Council of Europe Framework Convention on Artificial Intelligence 2024 provide coordinating platforms. Mutual-recognition agreements for conformity assessment and shared standards development through IEEE and ISO could reduce compliance burdens while preserving protective standards.

Fifth, enforcement capacity requires investment. Regulators need technical expertise to audit algorithmic systems; affected persons need accessible remedies including class-action or representative mechanisms. Regulatory sandboxes, as provided under Article 57 of the EU AI Act, allow controlled experimentation while preserving accountability.

VII. CONCLUSION

Algorithmic accountability is no longer a theoretical concern; it is a concrete policy domain with established regulatory instruments, growing case law, and rapidly evolving practice. The EU has adopted the most comprehensive horizontal framework; the US has produced a patchwork of sectoral and state-level responses with considerable substantive depth in covered areas; India has established a foundational data-protection statute but lacks specific algorithmic-accountability provisions.

This paper has argued that effective algorithmic governance requires the combination of horizontal transparency obligations, sectoral risk regulation, and a functioning liability regime. Each element addresses distinct accountability concerns; absent any one, the overall framework leaves substantial gaps.

The immediate priority in each jurisdiction differs. In the EU, the priority is effective implementation of the AI Act. In the US, the priority is either comprehensive federal legislation or more systematic coordination of sectoral authorities. In India, the priority is to enact the Digital India Act with clear automated-decision-making provisions and to align DPDP Act rules with algorithmic-accountability requirements. The global convergence of these frameworks will shape how consequential decisions are made, audited, and challenged for decades to come.

REFERENCES

- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine bias*. ProPublica.
Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Proceedings of Machine Learning Research, 81, 77–91.
Colorado Artificial Intelligence Act, SB 24-205 (2024).

Council of Europe. (2024). *Framework Convention on Artificial Intelligence* (CM(2024)92-final).

Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India.

Digital Services Act, Regulation (EU) 2022/2065, [2022] OJ L 277/1.

Executive Order 14110, 88 Fed. Reg. 75191 (2023) (United States).

Federal Trade Commission. (2022). *Aiming for truth, fairness, and equity in your company's use of AI*.

General Data Protection Regulation, Regulation (EU) 2016/679, [2016] OJ L 119/1.

Information Technology Act, No. 21 of 2000, Acts of Parliament, India.

Justiz, SCHUFA Holding AG v. OQ, Case C-634/21, EU:C:2023:957.

K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

NITI Aayog. (2021). *Responsible AI: Approach document for India* (Parts 1 & 2).

New York City Local Law 144 of 2021 (Automated Employment Decision Tools) (effective 2023).

OECD. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449).

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Regulation (EU) 2024/1689 (Artificial Intelligence Act), [2024] OJ L 1689.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*. *International Data Privacy Law*, 7(2), 76–99.

White House Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights*.