



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 20

The Friction of Transparency: Reconciling the Digital Personal Data Protection (DPDP) Act, 2023 with the Public Disclosure Mandates of the FCRA

Ashutosh Srivastava
*LLB Student,
2nd Year, ILS Law College, Pune*

Recommended Citation

Ashutosh Srivastava, *The Friction of Transparency: Reconciling the Digital Personal Data Protection (DPDP) Act, 2023 with the Public Disclosure Mandates of the FCRA*, 5 IJHRLR 219-230 (2026).

Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

The Friction of Transparency: Reconciling the Digital Personal Data Protection (DPDP) Act, 2023 with the Public Disclosure Mandates of the FCRA

ABSTRACT

*The enforcement of the Digital Personal Data Protection (DPDP) Act, 2023 marked the beginning of India's landmark privacy-first data framework, with stringent compliance with data minimization and consent standards. Simultaneously, civil society is subjected to a high-surveillance public transparency regime under the Foreign Contribution (Regulation) Act, 2010 (FCRA). A severe statutory clash is highlighted in this article: the FCRA mandates non-profit organizations to upload granular, un-anonymised personal data including names, passport numbers, home addresses and bank accounts of trustees and donors on the public Ministry of Home Affairs (MHA) portal to trace foreign funding. Such mandatory disclosure takes place without the revocable consent of the data principal and thus, directly contravenes the data minimization and security safeguards under the DPDP Act. This article evaluates this conflict through the lens of doctrinal legal analysis and under the comparative constitution framework of the judicial 'proportionality test' in *K.S. Puttaswamy v. Union of India* (2017). The study found that tracking foreign financial flows was a legitimate state interest, but publicizing sensitive personal details failed the "necessity" and "least restrictive means" prongs of the privacy test. A constitutionally viable, less intrusive alternative is secure, closed-loop governmental audits. Thus, this article advocates for a shift to a "bifurcated registry" model that confines sensitive personal data to authorized bodies for auditing purposes, and releases only anonymized or aggregated metadata on public portals, thereby successfully balancing national security and digital privacy.*

KEYWORDS

Anonymization, Civil Society Organizations, Data Minimization, DPDP Act, 2023, Foreign Contribution Regulation Act.

1. INTRODUCTION

A stark paradox in the contemporary Indian regulatory landscape is: The

state has, on one hand, promoted a progressive, rights-based architecture for digital privacy through the Digital Personal Data Protection (DPDP) Act, 2023¹, under Article 21 of the Constitution,² and in contrast, an increasingly high surveillance and centralized financial oversight apparatus through the Foreign Contribution (Regulation) Act, 2010 (FCRA) ³and the pending FCRA (Amendment) Bill, 2026. ⁴The DPDP Act, while safeguarding individuals from unwarranted exposure of data, is based on an administrative philosophy of complete transparency to the public in the FCRA. This statutory collision course has largely passed unnoticed by academics leaving civil society organizations (CSOs) stranded in a stubborn legal vacuum. The conflict has now reached a critical point. The DPDP Act classifies all NGOs as “Data Fiduciaries” who are legally required to process personal data for a lawful purpose only, and with revocable consent. At the same time, under Section 18 of the FCRA, associations are required to upload the granular personal data of ultimate foreign donors, trustees and key office-bearers, including names, passport numbers, home addresses and bank accounts, on the MHA’s public portal. This public indexing leaves people vulnerable to doxing, identity theft and physical threats, in clear violation of the DPDP Act’s Section 8 data-security obligations.

This statutory friction has enormous constitutional and legal significance, as it impinges upon the right to privacy (Article 21) and freedom of association (Article 19(1)(c)). In *K.S. Puttaswamy v. Union of India*, the Supreme Court held that any infringement on the right to privacy has to pass a four-fold test of proportionality: legitimacy of state interest, suitability, necessity (“least restrictive means”) and proportionality *stricto sensu*. ⁵There is a legitimate security interest in tracing foreign funding⁶. But the open-access public disclosure mechanism fails the necessity test, as the same administrative end could be achieved by secure, closed-loop regulatory audits, without public exposure.

The current academic literature is not integrated and is limited to either DPDP compliance or FCRA cancelations. To date, there is no literature that analyzes the direct legal clash where compliance with the public disclosure mandates of the FCRA makes it impossible for an NGO to comply with its data protection duties under the DPDP Act, exposing it

¹ Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

² The Constitution of India, art. 21.

³ Foreign Contribution (Regulation) Act, 2010 (Act 42 of 2010).

⁴ The Foreign Contribution (Regulation) Amendment Bill, 2026 (Bill 81 of 2026).

⁵ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, para 310.

⁶ Chandan Kallaiah, "THE FCRA (AMENDMENT) BILL, 2026: HISTORY, KEY CHANGES, AND THE ROAD TO A MORE ROBUST LAW", (2026) VIII Indian Journal of Law and Legal Research IV, 1.

to civil penalties of up to ₹250 crore or the cancelation of its license and vesting of its assets under the 2026 Bill. In this article, we (1) examine structural tensions between the DPDP Act and FCRA, (2) analyze MHA portal⁷ disclosures through the Puttaswamy proportionality lens, and (3) propose a pragmatic “bifurcated registry” model.

2. LITERATURE REVIEW

There is a fierce contestation over the intersection of digital privacy, state security and the regulation of CSOs. But the scholarship is split between two parallel, non-communicating streams: constitutional critiques of the FCRA and regulatory analyzes of the DPDP Act.

2.1. Privacy and National Security Scholarship: Financial Surveillance and State Interest

The state supervision of cross-border flows of financial resources is a compromise between individual freedom and national security. National security experts say sovereign states have the right to monitor and trace foreign capital to protect domestic democratic processes and national sovereignty⁸. In contrast, privacy advocates and human rights scholars argue that financial surveillance is an overreach that curtails the space available for civil society to function.⁹ They argue the FCRA’s public release of private financial and identity data is an unfair penalty for legitimate voluntary associations, even while tracking illicit funds is a legitimate activity.¹⁰

2.2. Criticism of the amendments to the FCRA and administrative consolidation (by the Academy)

The legislative developments of the FCRA have moved from simple surveillance to a centralized administrative control. Scholars critically analyzed the Foreign Contribution (Regulation) Amendment Act, 2020¹¹ which banned sub-granting, reduced the administrative expenditure caps to 20% and mandated a single SBI designated account.¹² The

⁷ Ministry of Home Affairs, "Foreign Contribution Regulation Act Online Services", available at: <https://fcraonline.nic.in> (Last visited on 4 September 2026).

⁸ Doc2026722929001.pdf, "Transparency and Disclosure Regime: The Foundational Principles of FCRA", 12.

⁹ Upendra Baxi, "Human Rights and Constitutionalism", (2021) 63 Journal of the Indian Law Institute 245.

¹⁰ Doc2026722929001.pdf, "Transparency and Disclosure Regime: The Foundational Principles of FCRA", 15.

¹¹ The Foreign Contribution (Regulation) Amendment Act, 2020 (Act 33 of 2020).

¹² Chandan Kallaiaah, "THE FCRA (AMENDMENT) BILL, 2026: HISTORY, KEY CHANGES, AND THE ROAD TO A MORE ROBUST LAW", (2026) VIII Indian

pending FCRA (Amendment) Bill, 2026 ¹³takes this from regulation of cash flows to regulation of physical assets. FCRA License Cancellation/Suspension: Section 16A states that if the FCRA license is canceled, voluntarily surrendered or not renewed, then “provisional vesting” of assets like schools and hospitals happens in a Designated Authority, resulting in permanent forfeitures.

2.3. The Paradox of Compliance: The Data Privacy-Surveillance Discrepancy

What is missing and critical in current legal scholarship is an analysis of the compliance paradox that arises when the DPDP Act, 2023 and the public disclosure obligations under the FCRA are enforced simultaneously. According to section 6 of the DPDP Act ¹⁴states that the personal data can only be processed if the consent is “free, specific, informed, unconditional and unambiguous” and the consent must be “clear” with a right to revoke. Section 8 mandates Data Fiduciaries to put in place strong safety safeguards which, if not followed, can attract civil penalties up to ₹250 crore. Conversely, the MHA’s FCRA rules¹⁵ impose a regime of high surveillance and public disclosure¹⁶. NGOs will have to upload detailed, un-anonymised personal information of their ultimate foreign donors, trustees and office-bearers (including passport numbers, home addresses, phone numbers and bank account details) on the publicly accessible online MHA portal.

The direct confrontation of legislation is missed. The DPDP Act recognizes the fundamental right of an individual to withdraw consent. If a trustee or a donor withdraws their consent, the NGO is not legally allowed to process or publish their data. But, in case of the NGO’s compliance and the redaction of the personal details in its MHA submissions, it will directly violate Section 18 of the FCRA¹⁷, and its license will be immediately canceled and its entire asset infrastructure will vest in the State under the 2026 Bill.¹⁸

Journal of Law and Legal Research IV, 5.

¹³ The Foreign Contribution (Regulation) Amendment Bill, 2026 (Bill 81 of 2026), s. 16A.

¹⁴ Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 6.

¹⁵ Ministry of Home Affairs, "Foreign Contribution Regulation Act Online Services", available at: <https://fcraonline.nic.in> (Last visited on 4 September 2026)

¹⁶ Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 8

¹⁷ Foreign Contribution (Regulation) Amendment Rules, 2026, S.O. 3272(E), Ministry of Home Affairs, June 22, 2026

¹⁸ Nivedita Krishna and Naman Khatwani, "FCRA Amendment Bill, 2026: How does it affect nonprofits?", India Development Review, April 17, 2026, available at: <https://idronline.org/article/board-governance/fcra-amendment-bill-2026-how-does-it-affect-nonprofits/> (Last visited on 4 September 2026)]****[20: Sanskriti University, "Government Power vs. Property Rights: The FCRA Bill 2026 Debate

3. RESEARCH METHODOLOGY

The research design used in this study is doctrinal, analytical and comparative. The black-letter law statutes, rules and notifications are doctrinally analyzed for compliance gaps. The comparative approach is adopted to benchmark India against the EU's GDPR¹⁹ and the US's FARA²⁰. Data is collected from primary sources (legislative texts and binding Supreme Court precedents like *K.S. Puttaswamy (2017)*²¹ and Noel Harper (2022))²² and secondary sources (MHA statistical dashboards, PRS Legislative Research reports and legal journals).²³

The central analytical framework is the four-pronged proportionality test laid down in *K.S. Puttaswamy v. Union of India (2017)*. Any state action or law which violates the fundamental right to privacy under Article 21 has to satisfy four cumulative conditions: (1) Legitimacy of the State goal; (2) Suitability of the measure; (3) Necessity ("least restrictive means"); and (4) Proportionality stricto sensu (balanced impact).

4. DISCUSSION AND ANALYSIS

The intersection of the DPDP Act, 2023 and the FCRA, 2010 represents a critical conflict in Indian public law.

4.1 The crash course you can't avoid: Consent, data minimization and full disclosure

That legislative friction is a product of two clashing administrative philosophies. The DPDP Act is a rights-based privacy-first model whereas the FCRA is an executive-centric high-surveillance regime that demands absolute public-facing transparency.

I. The Consent Paradox (Section 6 of DPDP Act vs. Section 18 of FCRA)

The processing would be based on 'unconditional, specific, informed and revocable consent' of the Data Principal who can withdraw consent and ask for erasure, the Section 6 of the DPDP Act²⁴ states. But the FCRA

Every Law Student Should Understand", August 6, 2026, available at: <https://www.sanskriti.edu.in/blog/fcra-bill-2026-law-student-guide.php> (Last visited on 4 September 2026)

¹⁹ Regulation (EU) 2016/679 (General Data Protection Regulation)

²⁰ Foreign Agents Registration Act of 1938, 22 U.S.C. §§ 611–621 (2018)

²¹ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1

²² Noel Harper v. Union of India, (2022) SCC OnLine SC 434

²³ PRS Legislative Research, "The Foreign Contribution (Regulation) Amendment Bill, 2026", available at: <https://prsindia.org/billtrack/the-foreign-contribution-regulation-amendment-bill-2026> (Last visited on 4 September 2026)

²⁴ Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 6.

requires public filing in section 18. NGOs need to upload personal information of trustees, office-bearers and donors (names, passport numbers, home addresses, and bank accounts) without anonymization for getting registration or filing annual returns (Form FC-4). This disparity creates an unavoidable compliance dilemma:

1. The NGO is not allowed to process or publish the data of the trustee or donor if they revoke their consent under Section 6 of the DPDP Act.²⁵
2. In case the NGO complies and deletes the personal data from the submissions made on the MHA portal, the NGO would be in violation of Section 18 of the FCRA.
3. The lapse leads to immediate suspension, non-renewal or cancelation of the NGO's registration and provisional and permanent vesting of the entire asset infrastructure of the NGO in the State under the pending 2026 Bill.²⁶

II. The Gap in Data Minimization

The DPDP Act requires minimization of data, and stipulates that a Data Fiduciary shall process personal data only to the extent strictly "necessary" for a particular lawful purpose. But the MHA's FCRA portal follows the 'absolute disclosure' model. There is no operational reason why monitoring foreign funding should require the sensitive personal identifiers such as home addresses and passport numbers of domestic trustees to be available on the open searchable internet. Without data minimization protections, people are vulnerable to serious security threats such as doxing, profiling and targeted harassment. This is a clear breach of security obligations under Section 8 of DPDP Act²⁷.

4.2. Judicial developments and constitutional scrutiny: Noel Harper in the aftermath of the DPDP Act

In *Noel Harper v. Union of India* (2022), the Supreme Court of India upheld the restrictive 2020 amendments to the FCRA,²⁸ which it said made the receipt of foreign contributions a highly regulated statutory right, not a fundamental right. There was a legitimate state interest in preventing foreign influence and requiring key office-bearers to provide Aadhaar or passport details was an appropriate mechanism for verification, the court

²⁵ 3: Foreign Contribution (Regulation) Act, 2010 (Act 42 of 2010).

²⁶ The Foreign Contribution (Regulation) Amendment Bill, 2026 (Bill 81 of 2026), s. 16A

²⁷ Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 8.

²⁸ The Foreign Contribution (Regulation) Amendment Act, 2020 (Act 33 of 2020).

held.²⁹

However, the constitutional validity of Noel Harper has to be seen in the light of the later DPDP Act, 2023. The Noel Harper decision was given in 2022, prior to the statutory data protection regime. The DPDP Act, 2023 has therefore put data protection under a specific statutory framework.

The state has an interest in verification but the tools used must comply with statutory data protection standards. The Puttaswamy test shows that the disclosure of sensitive personal data to the public does not pass the test of constitutional scrutiny:

1. **Legal rate of interest.** There is nothing wrong with keeping an eye on foreign funding.³⁰
2. **Admissibility** The public display of personal identifiers on an open portal bears no rational relation to tracking financial flows. The audits can be private.³¹
3. **Necessity:** The model fails this prong. There is a clear and very effective alternative, which is much less intrusive for the state, which is a closed loop auditing mechanism.³² NGO bank flows should be audited by MHA, RBI and FIU-IND using secure non-public government databases.
4. **Proportionality in the strict sense:** The public indexing is a disproportionate interference with the fundamental rights under article 21 as trustees are exposed to identity theft and doxing by malicious third parties.

4.3 Comparative Study: India and International Regimes of Transparency

This constitutional critique is buttressed by comparative international law-

I. The European Union Model: GDPR and ECJ Beneficial-Ownership

²⁹ Noel Harper v. Union of India, (2022) SCC OnLine SC 434.

³⁰ Chandan Kallaiah, "THE FCRA (AMENDMENT) BILL, 2026: HISTORY, KEY CHANGES, AND THE ROAD TO A MORE ROBUST LAW", (2026) VIII Indian Journal of Law and Legal Research IV, 1.

³¹ doc2026722929001.pdf, "Transparency and Disclosure Regime: The Foundational Principles of FCRA", 12.

³² doc2026722929001.pdf, "Transparency and Disclosure Regime: The Foundational Principles of FCRA", 15.

Precedent

In consolidated cases *WM v Luxembourg Business Registers* (2022) the Court of Justice of the European Union (CJEU) invalidated open-public access to beneficial-ownership registries established under EU anti-money laundering directives, holding that it infringed Articles 7 and 8 of the EU Charter of Fundamental Rights.³³ The CJEU ruled that although the fight against money laundering is in the public interest, the public-facing registries are not strictly necessary. The state's auditing interest is fully met if the competent administrative authorities have secure access. A broad public access is beyond what is strictly necessary.

II. The U.S. Model: FARA

The United States has a law that regulates foreign influence, the Foreign Agents Registration Act of 1938 (FARA). Foreign Principal Registration Entities acting on behalf of a foreign principal must register with the Department of Justice (DOJ) under the Foreign Agents Registration Act (FARA).³⁴ Notably, although FARA mandates public disclosure of informational materials, sensitive personal information (such as personal bank accounts, home addresses, and passport numbers) is maintained in confidential DOJ databases available only to authorized law enforcement and national security personnel. The dual design achieves security goals without compromising data privacy.

4.4. Empirical Trends & Policy Developments: The 2026 Bill and Rules in Practice

The compliance burden and administrative risks for Indian NGOs have increased immensely on account of pending legislative changes under the FCRA (Amendment) Bill, 2026 and the notified FCRA Rules, 2026.

I. The Vesting of Assets Trap under Section 16A of the 2026 Bill

Section 16A of the 2026 Bill proposes a Designated Authority to administer civil society assets. "Provisionally vest" in this Authority, raising critical issues: In case of cancelation, surrender or expiry of registration all assets created out of foreign contributions-

1. **The Perpetuity Trap:** NGOs can continue to hold physical assets (like schools, hospitals) only if they keep renewing their FCRA

³³ Joined Cases C-37/20 and C-601/20, *WM v. Luxembourg Business Registers*, ECR I-845 (CJEU).

³⁴ Foreign Agents Registration Act of 1938, 22 U.S.C. §§ 611–621 (2018).

certificate in perpetuity, even if they stop using foreign funds. Forfeiture through lapse or surrender.³⁵

2. **The Mixed-Funding Crisis:** Seizures apply to assets funded “wholly or partly” by foreign contributions. Mixed funds cannot be technically allocated in indivisible physical infrastructure, risking arbitrary domestic capital takeovers.³⁶
3. **Operational Takeover:** The Designated Authority may take over the operational management at the provisional stage and may deprive of autonomy without any prior judicial review.

II. The Restrictive Effects of the FCRA Rules, 2026

The FCRA (Amendment) Rules, 2026 (enforced 22 June 2026) make it worse:

- **₹10-Lakh Utilization Threshold (Rule 12):** NGOs need to have utilized at least ₹10 lakh of foreign contributions received during the last two financial years to renew registration.³⁷ This harms small local entities (e.g., a rural clinic constructed with foreign grants but operated on local donations for which the certificate automatically expires, risking asset confiscation).
- **Administrative Silos:** Registrations are required to state specific purposes and geographic regions of operation under a rigid Schedule.
- **Aggressive Reporting:** Forces CSOs to collect more personal data and increases their liability under the DPDP Act by requiring details on project utilization, social media handles and identification of ultimate donor.

5. FINDINGS AND RECOMMENDATIONS

5.1. Experiment Results

³⁵ Sanskriti University, "Government Power vs. Property Rights: The FCRA Bill 2026 Debate Every Law Student Should Understand", August 6, 2026, available at: <https://www.sanskriti.edu.in/blog/fcra-bill-2026-law-student-guide.php> (Last visited on 4 September 2026).

³⁶ Nivedita Krishna and Naman Khatwani, "FCRA Amendment Bill, 2026: How does it affect nonprofits?", India Development Review, April 17, 2026, available at: <https://idronline.org/article/board-governance/fcra-amendment-bill-2026-how-does-it-affect-nonprofits/> (Last visited on 4 September 2026).

³⁷ Foreign Contribution (Regulation) Amendment Rules, 2026, S.O. 3272(E), Ministry of Home Affairs, June 22, 2026, Rule 12.

1. **The Compliance Paradox:** The MHA's disclosure rules under the FCRA create a legal double bind for NGOs, as compliance with these rules directly contradicts DPDP mandates on data sharing and data minimization, leading to huge civil liabilities of up to ₹250 crore.
2. **Proportionality Deficit:** The public disclosure of personal data on MHA portals does not pass the "necessity" and "proportionality" tests. Funds can be tracked through closed-loop governmental audits without exposing sensitive data on the public internet.
3. **The Never-Ending Compliance Trap:** Section 16A of the 2026 Bill states that any non-renewal or surrender of registration will result in the immediate vesting of mixed-funded, indivisible public-service assets, provisionally and permanently, in a Designated-Authority.
4. **Strategic Philanthropic Reorientation:** The threat of asset takeover is causing donors and NGOs to walk away from long-term investments in permanent physical infrastructure and gravitate toward short-term, low-risk program spending, to the detriment of sector development.

5.2 Suggestions

1. **Split Registry Model:** The Ministry of Home Affairs should amend the FCRA Rules in consultation with MeitY to create a bifurcated dual-access system. Detailed un-redacted personal data (e.g. passport numbers, bank accounts) should be submitted through a secure, encrypted database, which is only accessible to authorized regulatory bodies (MHA, RBI, FIU-IND) for auditing for national security purposes. The portal accessible by the general public will post only anonymized aggregated metadata (e.g., total foreign funds, regions of utilization) to ensure trustees' and donors' digital privacy and safety.
2. **Set up a statutory appellate body:** The FCRA (Amendment) Bill, 2026 should be amended to establish an independent **FCRA Appellate Tribunal** headed by a retired judicial officer. The statute must prescribe a hearing prior to the making of the decision. No asset shall be vested, whether provisionally or permanently, in the Designated Authority without giving the association affected thereby a reasonable opportunity of being heard in its defense. There must be clear statutory guidelines codified to mathematically apportion and protect domestic capital in mixed funded assets.

3. **MeitY Clarification on “Specified Legitimate Uses”:** MeitY should exercise its rulemaking authority under Section 7 of the DPDP Act, 2023 to issue a clear clarification that compliance with statutory filing requirements is a “specified legitimate use”, but that such compliance does not allow or protect the public-facing dissemination of sensitive personal identifiers on open-internet domains.

6. CONCLUSION

The parallel evolution of India’s legislative landscape has set two basic constitutional values in opposition to each other: the collective interest in national security and sovereign financial integrity, and the individual right to digital privacy and informational self-determination. The present regulatory architecture under the FCRA, 2010, characterized by absolute, public-facing disclosure and aggressive asset-vesting measures under the proposed 2026 Bill, systematically undermines the digital privacy protections codified in the DPDP Act, 2023.

The study shows that transparency and national security are not incompatible. The state can fully monitor, trace and control the foreign capital inflow, without throwing the private and sensitive lives of civil society members to the public internet. India can build a modern and proportionate administrative system through the adoption of a Bifurcated Registry Model, independent appellate oversight, and clear regulatory boundaries. The harmonization of these laws is essential to protect the fundamental rights of the people, the democratic autonomy of the civil society and to guaranty the constitutionality of the national security measures.