International Journal of Contemporary Research In Multidisciplinary

Research Article

Hohfeldian Analysis of Digital Privacy Rights: Reconstructing Data Protection Frameworks under GDPR, DPDPA 2023, and Puttaswamy

Soumyadip Panda [1*], Dr. Rupak Kr. Joshi [2]
[1] Research Scholar, School of Legal Studies, The Neotia University, West Bengal, India
[2] Assistant Professor, School of Legal Studies, The Neotia University, West Bengal, India

Corresponding Author: * Soumyadip Panda

DOI: https://doi.org/10.5281/zenodo.21477986

Abstract

The exponential proliferation of digital data ecosystems has transformed privacy from a classical negative liberty into a multidimensional legal entitlement encompassing informational autonomy, contextual integrity, and dignitarian protection. Yet contemporary data protection frameworks—including the European Union's General Data Protection Regulation (GDPR) [1], India's Digital Personal Data Protection Act, 2023 (DPDPA 2023) [2], and the Indian Supreme Court's landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India [3]—deploy privacy discourse in conceptually imprecise and internally inconsistent ways that obscure the true structure of legal relationships among data principals, data fiduciaries, regulatory authorities, and the state. This paper applies Wesley Newcomb Hohfeld's analytical jurisprudence [4]—specifically the four correlative pairs of rights-duty, privilege-no-right, power-liability, and immunity-disability—as a reconstructive theoretical lens to map the normative architecture of digital privacy across these three frameworks. Through doctrinal analysis and comparative legal method, the paper demonstrates that Hohfeldian disaggregation exposes structural asymmetries, accountability deficits, and constitutional tensions that surface-level statutory interpretation fails to capture. The analysis contributes an original jurisprudential matrix of digital privacy relations and proposes targeted normative recommendations for doctrinal coherence, regulatory design, and cross-jurisdictional harmonisation.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 13-06-2026
- **Accepted:** 16-07-2026
- **Published:** 21-07-2026
- **IJCRM:** 5(4); 2026: 403-411

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Panda S, Joshi R K. Hohfeldian Analysis of Digital Privacy Rights: Reconstructing Data Protection Frameworks under GDPR, DPDPA 2023, and Puttaswamy. Int J Contemp Res Multidiscip. 2026;5(4):403-411.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Hohfeldian jurisprudence, digital privacy rights, GDPR, DPDPA 2023, Puttaswamy, data protection law, informational self-determination.

1. INTRODUCTION

The governance of personal data has emerged as one of the most consequential and contested domains of twenty-first-century law. The convergence of artificial intelligence, surveillance capitalism, algorithmic governance, biometric identification systems, and transnational data flows has rendered privacy not merely a personal interest but a structural condition for the exercise of fundamental freedoms, democratic participation, and human dignity [5]. In this context, the legal frameworks ostensibly designed to protect privacy—including the GDPR, the DPDPA 2023, and constitutional privacy doctrine as articulated in Puttaswamy—have assumed critical governance significance. However, these instruments exhibit a persistent conceptual ambiguity: they invoke the language of rights, duties, consent, and accountability without systematically specifying the precise legal relations they establish or the normative structure within which those relations operate [6].

Wesley Newcomb Hohfeld's Fundamental Legal Conceptions, first published between 1913 and 1917 [4], offered a rigorous analytical taxonomy of legal relations that disaggregated the omnibus concept of 'right' into four distinct jural categories—claim-rights, privileges, powers, and immunities—each paired with a corresponding jural opposite and jural correlative. Though developed in the context of property and contract law, Hohfeld's framework has demonstrated remarkable adaptability across constitutional theory, international law, and regulatory governance [7]. Its application to digital privacy rights is not merely academically novel; it is jurisprudentially necessary. Only by disaggregating the composite notion of 'privacy' into its Hohfeldian constituents can legal scholars, courts, and regulators precisely specify who owes what to whom, under what conditions, and with what legal consequences for non-compliance.

This paper proceeds in nine substantive sections. Following the literature review and conceptual exposition of Hohfeldian jurisprudence, the paper conducts a comparative analysis of GDPR, DPDPA 2023, and Puttaswamy, constructs an original Hohfeldian matrix of digital privacy relations, and derives both analytical and policy conclusions. The central argument is that Hohfeldian reconstruction reveals significant doctrinal incoherence across all three frameworks and that addressing these incoherences is essential for the development of legally precise, constitutionally robust, and institutionally effective digital privacy governance.

2. LITERATURE REVIEW

The scholarship on privacy law has evolved through three broad phases. The foundational phase, inaugurated by Warren and Brandeis's 1890 Harvard Law Review essay [8], conceived privacy as a right to be let alone—a classical negative liberty protecting individuals from unwarranted intrusion. This liberal-individualist conception, though enormously influential in American constitutional law, proved inadequate for the networked information environment. The second phase, exemplified by Westin's taxonomy of privacy as control over personal information [9] and Fried's contractarian account of privacy as a precondition for intimacy and love [10], shifted the conceptual centre toward informational self-determination. The German Federal Constitutional Court's 1983 Census Judgment (Volkszählungsurteil) [11] constitutionalised this shift, establishing the doctrine of informational self-determination (Recht auf informationelle Selbstbestimmung) that directly informed the architecture of European data protection law.

The third and current phase is characterised by the constitutionalisation and internationalisation of data protection. Bygrave's comparative analysis of data protection as a fundamental right [12] demonstrates that national and supranational instruments increasingly ground data protection in constitutional dignity rather than mere regulatory utility. Solove's taxonomy of privacy violations [13] offers a systematic account of the diverse harms that informational privacy seeks to prevent, while Nissenbaum's contextual integrity theory [14] proposes that privacy norms are context-relative rather than universally fixed—a proposition with significant implications for cross-border regulatory harmonisation. Rouvroy and Poullet's critique of algorithmic governance [15] highlights the emerging challenge of automated decision-making to subjective autonomy, a challenge that existing consent-based frameworks demonstrably fail to address.

On Hohfeldian analysis specifically, Halpin's reconstruction [16] and Simmonds's critical examination [7] offer the most systematic modern treatments, while Wenar's application of Hohfeldian categories to human rights theory [17] provides the most directly relevant precedent for the present study. Critically, however, no published scholarship has applied the Hohfeldian framework comprehensively to the tripartite architecture of GDPR, DPDPA 2023, and Puttaswamy simultaneously. Studies of Puttaswamy have largely focused on its constitutional implications within the Indian constitutional order [18], without examining its compatibility with transnational data protection regimes. Similarly, comparative analyses of GDPR and DPDPA 2023 have proceeded along conventional regulatory dimensions—scope, consent, enforcement—without deploying a coherent jurisprudential lens capable of exposing their underlying normative structure [19]. This study bridges that gap.

3. CONCEPTUAL FOUNDATIONS OF HOHFELDIAN JURISPRUDENCE

Wesley Newcomb Hohfeld argued that legal discourse suffers from systematic ambiguity because the single term 'right' is used indiscriminately to denote four fundamentally distinct legal positions [4]. Each of these positions stands in a correlative relationship with a complementary position held by another legal person, and each has a jural opposite that represents its negation. Understanding these distinctions is indispensable for precise legal analysis, particularly in complex multi-party regulatory relationships of the kind that characterise data protection law.

The first Hohfeldian category is the claim-right (or right stricto sensu), which exists whenever one party has a duty toward the right-holder. A claim-right in the digital privacy context arises whenever a data principal can demand that a data fiduciary refrain from processing personal data without lawful basis—

this is the normative core of the GDPR's Article 6 and Article 17 framework. The correlative of a claim-right is a duty: wherever a claim-right exists, there must be a corresponding duty incumbent upon an identifiable legal person. The jural opposite of a claim-right is a no-right, meaning the absence of any claim enforceable against the other party.

The second category is the privilege (or liberty), which denotes freedom from a duty rather than the imposition of a duty on another. A data fiduciary who is permitted by law to process data for a legitimate interest without requiring consent exercises a privilege. Crucially, a privilege carries no duty on anyone else to facilitate its exercise—it merely signifies the absence of a prohibitory duty on the privilege-holder. The correlative of a privilege is a no-right in the other party: the data principal who cannot claim that a particular processing is unlawful when it falls within a recognised exemption holds only a no-right with respect to that processing.

The third category, power, is the legal ability to alter existing legal relations—to create, modify, or extinguish rights, duties, privileges, or other legal positions. Powers in the data protection context include: the regulatory authority's power to issue binding decisions, impose fines, or revoke certifications; the data principal's power to exercise consent withdrawal (Article 7(3) GDPR), which alters the lawful basis for ongoing processing; and the state's constitutional power to legislate data protection frameworks subject to proportionality review. The correlative of a power is a liability: whoever is subject to another's power is in a position of liability, meaning their legal position can be altered by the other's exercise of the power.

The fourth and most analytically distinctive category is immunity, which denotes exemption from another person's power—the legal disability of a party to alter one's legal position. Constitutional entrenchment of privacy rights creates immunities: the Indian state cannot, through ordinary legislation, abrogate the fundamental right to privacy established in Puttaswamy, because the constitutional order imposes a disability upon the legislature in this regard. The correlative of immunity is disability: the party who cannot alter another's legal position is under a legal disability. This Hohfeldian framework, as elaborated in Table 1 below, provides the analytical vocabulary for the comparative examination that follows.

Table 1: Hohfeldian Jural Relations and Their Digital Privacy Equivalents

Jural Position	Jural Correlative	Jural Opposite	Digital Privacy Example (GDPR)	Digital Privacy Example (DPDPA/Puttaswamy)
Claim-Right	Duty	No-Right	Art. 17 right to erasure; Art. 15 right of access	Puttaswamy fundamental right to privacy; DPDPA s.13 data principal rights
Privilege	No-Right	Duty	Legitimate interest processing (Art. 6(1)(f)); research exemptions	State security exemptions (DPDPA s.17); reasonable restriction under Art. 19(2)
Power	Liability	Disability	EDPB power to issue binding opinions; DPA power to levy fines (Art. 83)	DPBI regulatory powers (DPDPA s.18–28); Parliament's legislative power over data
Immunity	Disability	Liability	Art. 9 prohibition on sensitive data processing; constitutional rights as immunities	Puttaswamy proportionality shield; constitutional entrenchment of fundamental rights

Source: Adapted from Hohfeld [4]; GDPR [1]; DPDPA 2023 [2]; Puttaswamy [3]. Table constructed by the authors.

Table 1 illustrates that the Hohfeldian vocabulary is not merely terminological but structural: it exposes that what data protection regimes call a 'right to erasure' is in Hohfeldian terms a claim-right correlating with a duty of deletion incumbent upon the data fiduciary, whereas what they call a 'legitimate interest' processing basis is a privilege correlating with a no-right in the data principal to object absolutely. This disaggregation has immediate practical import for enforcement, remedies, and proportionality analysis.

4. COMPARATIVE LEGAL FRAMEWORK ANALYSIS

4.1 The General Data Protection Regulation (GDPR)

The GDPR, which entered into force on 25 May 2018, represents the most comprehensive supranational data protection instrument to date [1]. Its conceptual architecture rests upon seven foundational principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability (Article 5). From a Hohfeldian perspective, the GDPR constructs an elaborate matrix of claim-rights held by data subjects against data controllers and processors, paired with correlative duties of compliance, notification, and erasure.

The six lawful bases for processing enumerated in Article 6—consent, contract, legal obligation, vital interests, public task, and legitimate interests—can be reconceptualised as conditions that either generate a data subject's claim-right (in the case of unlawful processing) or constitute a privilege permitting processing notwithstanding the data subject's prima facie claim-right to informational autonomy.

The GDPR's Chapter III rights—access (Article 15), rectification (Article 16), erasure (Article 17), restriction (Article 18), portability (Article 20), and objection (Article 21)—constitute positive claim-rights enforceable against identifiable duty-bearers. Critically, Article 17 ('right to be forgotten') is not an absolute claim-right but a defeasible one: the controller's duty to erase is displaced in circumstances enumerated in Article 17(3), including scientific research, public interest, and legal claims. This defeasibility structure is analytically equivalent to a Hohfeldian privilege that overrides the claim-right under specified conditions—a nuance that conventional rights-language obscures entirely [6].

4.2 The Digital Personal Data Protection Act, 2023 (DPDPA 2023)

India's DPDPA 2023, assented to on 11 August 2023, marks India's first comprehensive statutory framework for digital personal data protection [2]. While drawing inspiration from GDPR's conceptual vocabulary, the Act exhibits several structurally significant departures. The Act introduces the concept of 'Data Fiduciary'—an entity that determines the purpose and means of processing—and 'Data Principal'—the natural person to whom data pertains. Section 6 requires consent as the primary lawful basis, though Section 7 permits processing for 'legitimate uses' (including national security, legal proceedings, and employer purposes) without consent. Critically, and unlike the GDPR, the DPDPA 2023 does not enumerate a closed list of data subject rights but provides six rights: information access, correction and erasure, grievance redressal, nomination, and the right not to be subject to automated decision-making without human oversight.

The Act's most significant Hohfeldian feature is its asymmetric power structure. The Data Protection Board of India (DPBI), established under Section 18, holds extensive powers to investigate breaches, impose penalties, and issue directions—powers that generate correlative liabilities in data fiduciaries. However, the DPDPA 2023's scheme of state exemptions under Section 17, which permits the Government to exempt any data fiduciary or class of data fiduciary from the Act's provisions by notification, creates a sweeping and constitutionally contestable disability in data principals: they are rendered unable to invoke their statutory rights against entities so exempted. Whether this disability is consistent with the constitutional claim-rights established in Puttaswamy is a central analytical question examined in Section 6 below.

4.3 Justice K.S. Puttaswamy v. Union of India

The nine-judge bench decision in Puttaswamy (2017) [3] constitutionalised privacy as a fundamental right under Article 21 of the Indian Constitution, overruling the earlier decisions in M.P. Sharma (1954) and Kharak Singh (1963). The judgment's significance for digital privacy is threefold. First, the unanimous recognition of privacy as fundamental establishes constitutional claim-rights against state interference that operate as immunities in Hohfeldian terms—the state legislature and executive are under a constitutional disability to abrogate privacy without satisfying a tripartite proportionality test (legality, legitimate aim, and proportionality stricto sensu). Second, the concurring judgment of Justice D.Y. Chandrachud explicitly recognised informational privacy as a distinct dimension of the right, encompassing the right to control personal data, the right to data protection, and the right to be forgotten in the digital sphere. Third, the majority endorsed the doctrine of informational self-determination, thereby providing constitutional grounding for statutory data protection frameworks.

Puttaswamy's constitutional architecture is best understood through the immunity-disability pair. The fundamental right to privacy functions as an immunity conferring upon every individual a sphere of legal protection from state power—an immunity that cannot be extinguished by ordinary legislative action. However, the judgment simultaneously recognised that privacy is not absolute and is subject to reasonable restriction under Articles 19(2)-(6) and the general doctrine of proportionality. This means that state authorities, in specified circumstances and subject to proportionality review, hold residual powers vis-à-vis the immunity, generating a complex nested structure of immunities and disabilities that the simple rights-language of the judgment inadequately conveys.

Table 2: Comparative Analysis of GDPR, DPDPA 2023, and Puttaswamy across Key Regulatory Dimensions

Dimension	GDPR	DPDPA 2023	Puttaswamy
Legal Nature	Supranational Regulation (EU)	National Statute (India)	Constitutional Judgment (India)
Basis of Privacy	Fundamental right (Art. 8 EU Charter) + data protection right	Statutory entitlement; constitutional grounding via Puttaswamy	Fundamental right under Art. 21 Constitution of India
Consent Framework	One of six lawful bases; freely given, specific, informed, unambiguous (Art. 7)	Primary lawful basis (s.6); legitimate uses without consent (s.7)	Autonomy as prerequisite; no statutory consent framework
Data Subject / Principal Rights	Seven rights (Arts. 15–22) incl. portability and automated decision-making	Six rights (ss. 11–16) incl. grievance redress and nomination	Informational self-determination; right to be forgotten (Chandrachud J.)
State Surveillance Limits	Art. 23 derogations subject to necessity and proportionality; CJEU oversight	Broad s.17 exemptions for state entities; limited judicial oversight ex ante	Tripartite proportionality test: legality, legitimate aim, proportionality
Regulatory Enforcement	National DPAs + EDPB; fines up to 4% global turnover (Art. 83)	DPBI; civil penalties (s.33); no criminal liability	Constitutional courts; writ jurisdiction under Arts. 32, 226
Fiduciary / Accountability Model	Controller/Processor accountability; DPIAs; privacy by design (Art. 25)	Data Fiduciary obligations (ss. 8–10); significant data fiduciary category	State as fiduciary of constitutional rights; horizontal application possible
Cross-Border Data Flows	Adequacy decisions, SCCs, BCRs (Chapter V)	Government-notified permissible territories (s.16)	Not directly addressed; data sovereignty implicit

Source: Authors' comparative analysis. GDPR [1]; DPDPA 2023 [2]; Puttaswamy [3].

Table 2 reveals structural divergences across the three frameworks that have direct Hohfeldian implications. Most significantly, the GDPR establishes a more determinate set of claim-rights paired with identifiable duties, while the DPDPA 2023's broad exemption clauses generate zones of legal ambiguity where data principals hold formal claim-rights under

the statute but effective no-rights against exempted entities. The constitutional framework in Puttaswamy theoretically supplies immunities that constrain these exemptions, but the absence of a statutory mechanism for constitutional review of exemption decisions leaves a significant accountability lacuna.

5. RESEARCH METHODOLOGY

This study adopts a doctrinal and comparative legal research methodology. Doctrinal research involves the systematic analysis, interpretation, and synthesis of legal rules, principles, and doctrines derived from primary and secondary legal sources, with the aim of producing a coherent, internally consistent account of the law as it is and as it ought to be [20]. The study does not employ empirical methods, statistical analysis, quantitative datasets, machine learning techniques, or experimental designs. Its epistemological foundation is jurisprudential—concerned with the logical structure of legal relations, the normative coherence of legal frameworks, and the doctrinal consistency of judicial and legislative reasoning.

Primary sources consulted include: the GDPR and its recitals; the DPDPA 2023 and its Statement of Objects and Reasons; the Indian Constitution (Articles 14, 19, 21); the full nine-judge bench judgment and individual concurrences in Puttaswamy; relevant CJEU jurisprudence including Schrems I [21] and Schrems II [22]; the EDPB's binding opinions and guidelines; DPBI consultation documents; and relevant decisions of national data protection authorities. Secondary sources include peer-reviewed articles, treatises, and comparative law scholarship identified through systematic searches of Westlaw, HeinOnline, JSTOR, and Google Scholar using search terms including 'Hohfeld privacy,' 'GDPR data subject rights,' 'DPDPA 2023 analysis,' 'Puttaswamy informational privacy,' and 'digital constitutionalism.'

The comparative method employed is that of functional comparison, as developed by Zweigert and Kötz [23]: legal institutions across the three frameworks are compared according to their functional roles in regulating the data principal-fiduciary relationship, rather than merely their formal textual similarities. The Hohfeldian framework serves as the tertium comparationis—the common evaluative standard against which each framework's normative structure is assessed. This approach enables the identification of not merely doctrinal differences but structural asymmetries in the allocation of legal positions across institutional actors.

6. ANALYTICAL FRAMEWORK: HOHFELDIAN MAPPING OF DIGITAL PRIVACY

The analytical framework developed in this section constructs an original Hohfeldian matrix of legal relations among the five categories of actors central to data governance: data principals, data fiduciaries (controllers/processors), state authorities, regulatory bodies, and third parties. This mapping is presented first in diagrammatic form and then elaborated through doctrinal analysis across the three comparative frameworks.

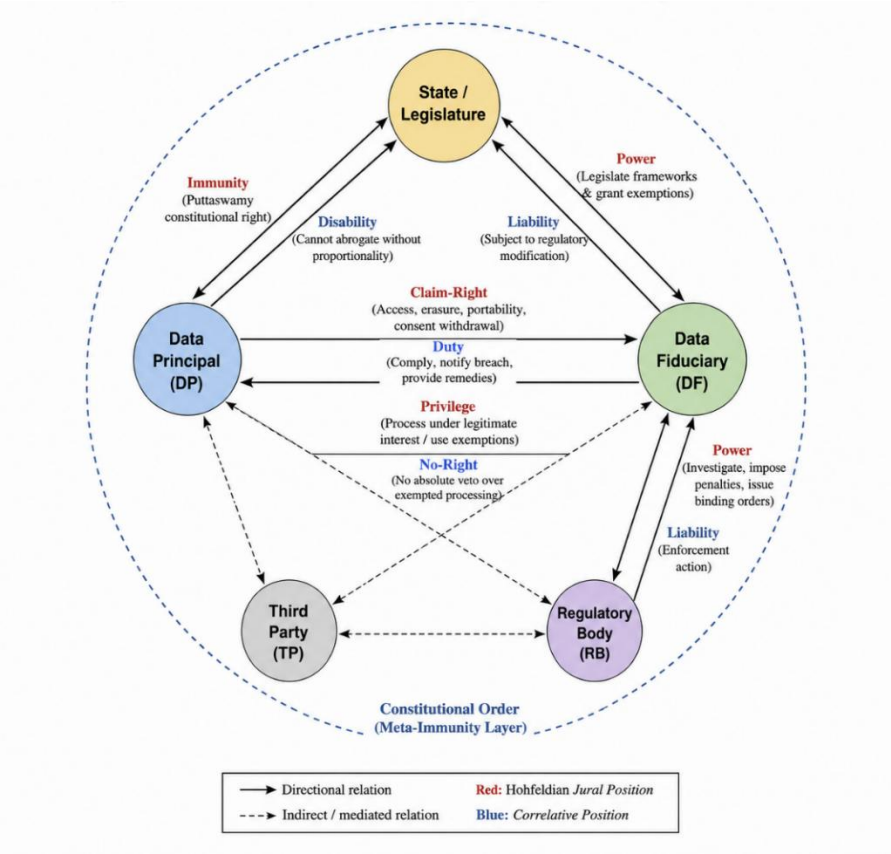

Figure 1: Hohfeldian Relational Map of Digital Privacy — See Description Below

Figure 1 illustrates that digital privacy governance does not consist of a single bilateral relationship between the data subject and a controller, but of a nested, multi-party legal structure in which Hohfeldian positions at each level are constrained by positions at higher levels of legal authority. The constitutional immunity established in Puttaswamy functions as a meta-constraint upon the state's legislative and executive powers: even the expansive exemption clauses of the DPDPA 2023 cannot, on a proper reading, extend to operations that would violate the proportionality standard mandated by the constitutional claim-right to privacy.

Table 3: Hohfeldian Matrix of Digital Privacy Relations across GDPR, DPDPA 2023, and Puttaswamy

Jural Position	Right-Holder / Power-Holder	Duty-Bearer / Liable Party	Legal Basis	Doctrinal Significance
Claim-Right	Data Principal / Data Subject	Data Fiduciary / Controller	Art. 15-22 GDPR; ss. 11-16 DPDPA; Puttaswamy Art. 21	Establishes enforceable entitlements; breach generates remedies via DPA or court
Correlative Duty	Data Fiduciary / Controller	Owed to Data Principal	Art. 5-6 GDPR; ss. 8-10 DPDPA	Duty to minimise data, maintain accuracy, enable access/erasure, appoint DPO
Privilege	Data Fiduciary (exempted processing)	No correlative duty; data principal holds no-right	Art. 6(1)(f) GDPR; ss. 7, 17 DPDPA; State surveillance powers	Creates processing space free from consent; must be bounded by proportionality
Power	Regulator (DPA/DPBI); State Legislature	Data Fiduciary (liable); Data Principal (liable to legislative modification)	Art. 83 GDPR; ss. 18-33 DPDPA; Parliamentary sovereignty subject to Art. 21	Enables dynamic adjustment of legal relations; must be exercised within constitutional bounds
Immunity	Data Principal (constitutional)	State (disability to abrogate); Regulator (disability beyond statutory mandate)	Puttaswamy Art. 21; Art. 8 EU Charter; ECHR Art. 8	Constitutional entrenchment shields right from ordinary legislative modification; proportionality test as immunity standard

Source: Authors' Hohfeldian matrix. Constructed from GDPR [1], DPDPA 2023 [2], Puttaswamy [3], Hohfeld [4].

The Hohfeldian matrix in Table 3 makes explicit what implicit in the legislative texts: that data protection law is not a unidimensional grant of rights but a complex allocation of claim-rights, privileges, powers, and immunities distributed across institutional actors. Most significantly, the matrix reveals a structural tension in the DPDPA 2023: data principals nominally hold claim-rights under Chapter III, but the state, through Section 17 notification powers, can transform those claim-rights into effective no-rights by exempting processing entities from the statute's application—a power that, on Hohfeldian analysis, generates a liability in the data principal and effectively suspends their statutory claim-right. Whether this transformation is constitutionally valid depends upon whether it satisfies the proportionality immunity established in Puttaswamy.

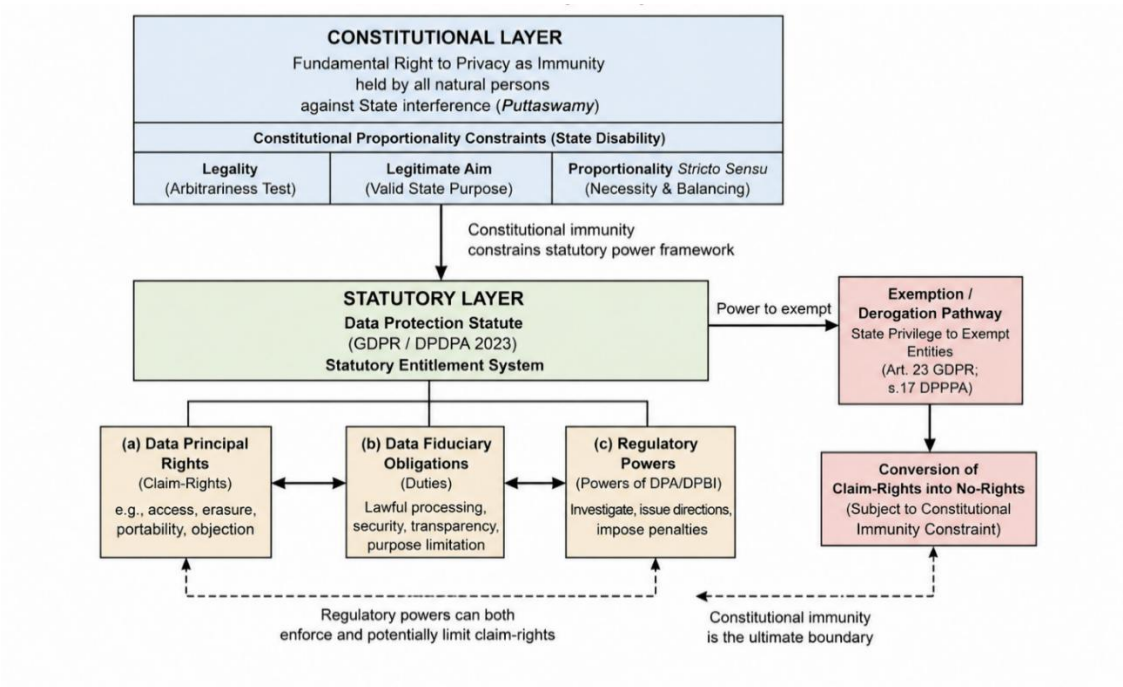

Figure 2: Immunity-Disability Architecture — Constitutional vs. Statutory Privacy — See Description Below]

Figure 2 conceptualises what may be termed the 'vertical dimension' of Hohfeldian privacy analysis: the relationship between constitutional immunities and statutory powers. This vertical dimension is critically important for evaluating the DPDPA 2023's exemption architecture. The Section 17 government notification power is a statutory power; its exercise generates a liability (suspension of statutory claim-rights) in data principals. However, this liability is itself constrained by the constitutional immunity established in Puttaswamy: if the exemption operates disproportionately or without a legitimate aim, the data principal may invoke the constitutional immunity to resist the statutory modification of their legal position. This nested structure—in which constitutional immunities constrain the exercise of statutory powers, which in turn modulate operational claim-rights—is the central analytical contribution of the present framework.

7. DISCUSSION

7.1 Doctrinal Coherence and Structural Asymmetries

The Hohfeldian analysis conducted above reveals that all three frameworks exhibit distinct doctrinal strengths and weaknesses. The GDPR's claim-right architecture is its most coherent feature: the six categories of data subject rights in Chapter III are each paired with identifiable duties of the controller, supported by enforcement mechanisms and remedies that provide institutional bite to the correlative structure. The accountability principle in Article 5(2) and the requirement for records of processing activities in Article 30 further strengthen the duty-side of the legal relation by creating transparency obligations that enable regulatory verification of compliance. Yet the GDPR's claim-right framework is partially undermined by its over-reliance on consent as a foundational mechanism. Scholarly consensus increasingly recognises that consent in the digital environment is structurally coerced, contextually opaque, and cognitively burdensome [24]—features that transform the formal claim-right to withdraw consent (Article 7(3)) into an effective no-right in data subjects who lack meaningful alternatives.

The DPDPA 2023 presents more pronounced structural asymmetries. While it introduces the useful concept of the Significant Data Fiduciary (SDF) under Section 10, which subjects large-scale processors to enhanced obligations, the Act's accountability mechanisms are substantially weaker than the GDPR's in three respects. First, the absence of a Data Protection Officer requirement for all data fiduciaries (only SDFs are so required) leaves the duty side of the claim-right relation without institutional embodiment in a large class of processing entities. Second, the Board's dependence on Government appointment and the absence of structural guarantees of its independence creates a power structure that does not adequately constrain the regulatory authority's own exercise of power—a disability deficit that undermines the accountability function attributed to the DPBI in the Hohfeldian matrix. Third, and most significantly, the breadth of Section 17 exemptions renders a substantial proportion of data processing by state-connected entities effectively immune from statutory claim-right enforcement—an ironic inversion of the constitutional immunity structure, in which it is the state that acquires effective immunity rather than the individual [25].

7.2 Emerging Challenges: AI, Automated Decision-Making, and Biometric Governance

The application of the Hohfeldian framework to emerging digital challenges exposes further limitations of all three instruments. Artificial intelligence systems and automated decision-making introduce a new category of actors—algorithmic systems—that exercise de facto powers over data principals (by determining creditworthiness, employability, criminal risk, and insurance eligibility) without holding legal personhood and therefore without legal liability in the conventional sense [26]. Article 22 of the GDPR provides a partial response by conferring upon data subjects a right not to be subject to solely automated decisions with significant effects—a claim-right that correlates with a duty of human oversight in the controller. However, the DPDPA 2023's equivalent provision under Section 14 is structurally underspecified, and the enforcement pathway for violations in the AI context remains jurisprudentially underdeveloped in both jurisdictions.

Biometric governance represents a further frontier of Hohfeldian concern. The processing of biometric data—fingerprints, facial geometry, iris patterns—creates irreversible identifiers whose misuse or unauthorised processing cannot be remedied through erasure in any meaningful sense: a data principal cannot change their biometric profile as they can change their password. This creates what may be termed a 'permanent liability': the data principal is exposed to an ongoing risk of legal-relation modification by any entity that acquires biometric data, with no practical immunity shield beyond ex ante regulation. The GDPR addresses this through the special category regime in Article 9, which prohibits biometric processing for identification purposes as a default—effectively establishing an immunity-disability structure for biometric data. The DPDPA 2023's handling of sensitive personal data is, by contrast, considerably weaker: the Act delegates to central government notification the definition of sensitive categories, which introduces regulatory discretion into a domain where constitutional immunities arguably require rule-based protection [27].

7.3 Cross-Border Data Flows and Transnational Hohfeldian Gaps

The cross-border dimension of digital privacy governance creates what this paper terms 'transnational Hohfeldian gaps': situations in which a data principal holds a nominal claim-right under one jurisdiction's framework but lacks any corresponding duty-bearer in another jurisdiction's legal order. The GDPR's adequacy decision regime (Article 45) seeks to bridge this gap by conditioning data transfers on the receiving country's data protection law meeting European standards—effectively projecting GDPR claim-rights across borders by requiring foreign systems to generate corresponding duties. The CJEU's decisions in Schrems I and Schrems II [21,22] reinforced this by invalidating adequacy frameworks that failed to provide effective immunity from mass surveillance, thereby reasserting

the constitutional immunity structure of the EU Charter as a transnational constraint on data transfer powers.

The DPDPA 2023's approach to cross-border flows under Section 16 is instrumentally different: it delegates adequacy determination entirely to the Central Government, which may permit data transfer to 'such countries or territories outside India as may be prescribed.' This delegation creates a power-liability structure in which data principals are liable to having their data transferred to jurisdictions with potentially weaker protections, without any independent adjudication of the adequacy of protection. From a Hohfeldian perspective, this statutory power is exercised in a context where the constitutional immunity established in Puttaswamy provides the only available meta-constraint—yet Puttaswamy does not directly address cross-border flows, leaving the doctrinal question substantially open [28].

8. POLICY IMPLICATIONS

The foregoing analysis generates several concrete policy recommendations addressed to legislators, courts, regulatory bodies, and international governance institutions. These recommendations are organised around the four Hohfeldian categories to maintain analytical coherence.

With respect to claim-rights and correlative duties, legislatures should codify a minimum irreducible core of data principal claim-rights that is resistant to executive exemption. The DPDPA 2023's Section 17 notification power should be qualified by a proportionality requirement, procedural safeguards (including prior parliamentary scrutiny), and sunset clauses, so as to ensure that the exercise of the government's power does not disproportionately convert data principals' claim-rights into effective no-rights. Courts exercising constitutional review should treat any statutory provision that categorically removes data principals' claim-rights against state entities as presumptively incompatible with the Puttaswamy immunity, subject to strict proportionality review rather than the deferential reasonableness test applied under Article 19(2) restrictions.

With respect to privileges and the risk of their expansion, regulatory bodies should develop sector-specific guidelines that clearly delineate the boundaries of legitimate interest processing (GDPR) and legitimate use processing (DPDPA 2023). The balancing test required by Article 6(1)(f) GDPR should be operationalised through published regulatory guidance that specifies how the data principal's no-right against legitimate interest processing is determined and what contextual factors transform a privilege back into a duty of non-processing. This would introduce greater legal certainty and reduce the risk of privilege expansion that has characterised AI-driven data monetisation practices.

With respect to powers and liabilities, the independence and resourcing of data protection regulatory bodies is a structural precondition for effective accountability. The DPBI's dependence on executive appointment mechanisms under the DPDPA 2023 must be addressed through statutory amendments providing for parliamentary confirmation, security of tenure, and financial independence analogous to constitutional bodies. The GDPR's co-regulatory model through the EDPB provides a useful reference point. Furthermore, cross-border regulatory cooperation agreements should be developed with Hohfeldian precision: rather than vague commitments to information exchange, they should specify which powers each authority may exercise with respect to processing entities domiciled in the other jurisdiction, thereby closing the transnational Hohfeldian gaps identified in Section 7.3.

With respect to immunities and disabilities, the constitutional immunity established in Puttaswamy should be rendered more operationally precise through a comprehensive data protection constitutional amendment or through a series of authoritative Supreme Court decisions that specify the proportionality thresholds applicable to surveillance legislation, algorithmic governance, and biometric data processing. The European model of explicit fundamental rights recognition for data protection under Article 8 of the EU Charter offers a partial template; however, India's constitutional order, with its more expansive socio-economic rights framework and greater judicial deference to security legislation, requires a contextually calibrated immunity standard that reflects Indian constitutional jurisprudence.

9. CONCLUSION

This paper has applied Wesley Newcomb Hohfeld's analytical framework of legal relations to the comparative examination of digital privacy rights under the GDPR, DPDPA 2023, and the constitutional doctrine established in Puttaswamy. The Hohfeldian reconstruction exposes that what each of these frameworks denominates as 'privacy rights' encompasses four structurally distinct categories of legal position—claim-rights, privileges, powers, and immunities—each carrying different legal implications for enforcement, accountability, and constitutional legitimacy. The analysis reveals significant structural asymmetries: the DPDPA 2023's exemption architecture risks converting statutory claim-rights into effective no-rights without adequate constitutional justification; the GDPR's consent-based claim-right framework is partially undermined by structural power imbalances in digital markets; and the constitutional immunity established in Puttaswamy, though theoretically robust, lacks the statutory operationalisation necessary for effective protection in AI, biometric, and transnational data governance contexts. The original Hohfeldian matrix and nested immunity-disability framework developed here contribute a novel analytical vocabulary to the legal scholarship on data protection, enabling more precise doctrinal critique, more targeted policy design, and more coherent judicial reasoning. Future research should extend this framework to automated decision-making, federated AI systems, and the emerging architecture of digital identity governance.

REFERENCES

1. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation). Off J Eur Union. 2016;L119:1-88. Available

from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
2. Government of India. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Ministry of Electronics and Information Technology; 2023. Available from: https://digitalindia.gov.in/dpdpa
3. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors. (2017) 10 SCC 1 (Nine-Judge Bench).
4. Hohfeld WN. Some fundamental legal conceptions as applied in judicial reasoning. Yale Law J. 1913;23(1):16-59. doi:10.2307/785533.
5. Zuboff S. The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs; 2019.
6. Dagan H, Kreitner R. The new jurisprudence of legal realism. Calif Law Rev. 2017;105(6):1657-1704.
7. Simmonds NE. Rights at the cutting edge. In: Kramer MH, Simmonds NE, Steiner H, editors. A debate over rights: Philosophical enquiries. Oxford: Oxford University Press; 2001. p. 113-232.
8. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193-220. doi:10.2307/1321160.
9. Westin AF. Privacy and freedom. New York: Atheneum; 1967.
10. Fried C. Privacy. Yale Law J. 1968;77(3):475-493. doi:10.2307/794941.
11. Federal Constitutional Court of Germany (Bundesverfassungsgericht). Census Act Case (Volkszählungsurteil), BVerfGE 65, 1. Karlsruhe: Bundesverfassungsgericht; 1983.
12. Bygrave LA. Data privacy law: An international perspective. Oxford: Oxford University Press; 2014. doi:10.1093/acprof:oso/9780199675555.001.0001.
13. Solove DJ. A taxonomy of privacy. Univ Penn Law Rev. 2006;154(3):477-564. doi:10.2307/40041279.
14. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Stanford: Stanford University Press; 2010.
15. Rouvroy A, Poullet Y. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In: Gutwirth S, et al., editors. Reinventing data protection? Dordrecht: Springer; 2009. p. 45-76. doi:10.1007/978-1-4020-9498-9_2.
16. Halpin A. The concept of a legal power. Oxf J Leg Stud. 1996;16(1):129-152. doi:10.1093/ojls/16.1.129.
17. Wenar L. The nature of rights. Philos Public Aff. 2005;33(3):223-252. doi:10.1111/j.1088-4963.2005.00032.x.
18. Chandrachud DY. Privacy and its dimensions: A judicial perspective. Indian Law Rev. 2020;4(2):105-127. doi:10.1080/24730580.2020.1779697.
19. Parsheera S. Comparing India's DPDPA 2023 with the GDPR: Structural convergences and divergences. J Cyber Law Intellect Prop Soc Justice. 2023;2(1):1-28.
20. McKerchar M. Philosophical paradigms, inquiry strategies and knowledge claims: Applying the principles of research design and conduct to taxation. eJ Tax Res. 2008;6(1):5-22.
21. Court of Justice of the European Union. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems I). Case C-362/14. ECLI:EU:C:2015:650. Luxembourg: CJEU; 2015.
22. Court of Justice of the European Union. Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II). Case C-311/18. ECLI:EU:C:2020:559. Luxembourg: CJEU; 2020.
23. Zweigert K, Kötz H. An introduction to comparative law. 3rd ed. Weir T, translator. Oxford: Oxford University Press; 1998.
24. Barocas S, Nissenbaum H. Big data's end run around anonymity and consent. In: Lane J, Stodden V, Bender S, Nissenbaum H, editors. Privacy, big data and the public good. Cambridge: Cambridge University Press; 2014. p. 44-75.
25. Greenleaf G, Chander A. India's new data protection law: International comparisons and shortfalls. Comput Law Secur Rev. 2023;51:105903. doi:10.1016/j.clsr.2023.105903.
26. Doshi-Velez F, Kortz M, Budish R, Bavitz C, Gershman S, O'Brien D, et al. Accountability of AI under the law: The role of explanation. Berkman Klein Center Working Paper. 2017. doi:10.48550/arXiv.1711.01134.
27. Bhandari V. The inadequacy of India's DPDPA 2023 for sensitive personal data and biometric governance. Indian J Law Technol. 2023;19(1):42-78.
28. Kak A, editor. Regulating biometrics: Global approaches and urgent questions. New York: AI Now Institute, New York University; 2020.

About the Author

Soumyadip Panda is a Research Scholar at the School of Legal Studies, The Neotia University, West Bengal, India. His research interests include constitutional law, data protection, privacy rights, cyber law, and emerging legal issues in the digital era. He is committed to advancing interdisciplinary legal research and contributing to contemporary legal scholarship.