

The Changing Face of Justice: Law's Role in a Digital Society

*Parhlad Singh Ahluwalia, School of Management and Business Studies, Jamia Hamdard,
New Delhi, India*

Abstract

The diffusion of digital technologies into nearly every domain of social life has unsettled the foundational assumptions on which modern legal systems were built — territorial jurisdiction, human authorship of decisions, evidentiary permanence, and the presumption that law regulates conduct after the fact rather than architecture before it. This paper undertakes an analytical, scoping-review-informed examination of how law is being reconstituted as a regulatory, adjudicative, and normative instrument in a digital society. Using a PRISMA-ScR-informed screening process applied to an author-supplied bibliography supplemented by independently sourced legal and socio-legal literature (48 sources in total, all published in 2024 or earlier), the paper synthesises five interlocking strands of scholarship: cyberlaw foundations and the "code is law" thesis; platform governance and intermediary speech regulation; artificial intelligence, algorithmic decision-making and due process; data protection and informational privacy; and the digitalisation of courts and access to justice. A comparative analysis of the European Union's General Data Protection Regulation, India's Digital Personal Data Protection Act 2023, the Information Technology Act 2000, and the Council of Europe's Budapest Convention is presented in tabular form to illustrate convergence and divergence in regulatory design. The paper argues that digital society has produced a triple displacement in legal ordering — from rules to code, from courts to platforms, and from human to algorithmic discretion — and that an "analytical reality exposing" reading of the literature reveals a persistent accountability gap between technological capability and legal remedy. The paper concludes that the changing face of justice is not simply digitisation of existing procedure but a structural renegotiation of where normative authority resides, and it proposes a research and policy agenda centred on explainability, jurisdictional cooperation, and algorithmic due process.

Keywords: *digital society; cyberlaw; algorithmic accountability; data protection; access to justice; artificial intelligence and law; platform governance*

1. Introduction

Law has always lagged behind the technologies it seeks to govern, but the scale and speed of the current transition are without precedent. Within a single generation, communication, commerce, employment, healthcare, political discourse, and the administration of justice itself have migrated substantially onto digital infrastructures owned, designed, and operated largely outside the direct control of elected legislatures or national courts (1,2). This paper asks a deceptively simple question: what does it mean for "justice" — understood both as a set of institutional processes and as a substantive value — when the environment in which disputes

arise, evidence is generated, and decisions are increasingly made is architected by code rather than by statute?

The question matters for three reasons. First, digital infrastructures are not neutral conduits; they encode choices about what is permitted, what is visible, and what is remembered, and those choices function, in practice, as a form of regulation that operates prior to and sometimes independently of law (1). Second, a growing share of socially consequential decisions — creditworthiness scoring, content moderation, predictive policing, eligibility for welfare benefits, even elements of sentencing risk assessment — are now made or substantially informed by automated systems whose internal logic may be proprietary, statistically opaque, or genuinely emergent (3,17,18). Third, the dispute-resolution apparatus of the state is itself undergoing a parallel digitisation, from e-filing and video hearings to fully online courts, which changes who can access justice and on what terms (5,6).

This paper situates itself within the broader socio-legal and cyberlaw tradition that treats "law and technology" not as a narrow specialist sub-field but as a lens through which the ordinary operation of law can be re-examined (4,10,11). The phrase "analytical reality exposing," which frames the methodological orientation of this paper, is used here to denote a critical-analytical mode of inquiry that deliberately foregrounds the gap between the formal promises of legal regulation (consent, transparency, redress, equality before the law) and the empirical and doctrinal realities documented in the scholarship — a gap that becomes especially visible once digital infrastructures are added to the analysis (3,17,19,20).

This orientation is deliberately distinguished, at the outset, from two weaker alternatives that are common in the broader literature on law and technology. The first is a purely *descriptive* approach, which catalogues new statutes and judicial decisions without interrogating whether their stated objectives are actually achieved once the instrument meets the technical system it purports to regulate; such an approach risks mistaking the existence of a rule for the existence of a remedy. The second is a purely *normative* approach, which argues from first principles what the law *ought* to require of digital systems without first establishing, through the literature, what the law currently *does* require and how that requirement performs against the specific technical realities — opacity, scale, distributed authorship — that digital systems present. The "analytical reality exposing" method adopted here instead proceeds in three deliberate steps for each thematic cluster reviewed: it states the formal legal or regulatory position as the literature records it; it reports what the cited empirical or doctrinal scholarship finds about that position's operation in practice; and it names, explicitly, any gap between the two. This structure is applied consistently across Sections 4.1–4.8 and is the basis for the synthesis offered in Section 6.

The paper is organised as follows. Section 2 sets out the scoping-review methodology, including a PRISMA-ScR-informed account of how the literature base was assembled and screened. Section 3 develops a conceptual framework distinguishing three registers in which law engages digital society: law *of* technology, law *through* technology, and law *as* technology. Section 4 presents the related-research synthesis across eight thematic clusters, reporting the results, outputs, and competing perspectives found in the literature. Section 5 offers a comparative analysis of data-protection and cybercrime regimes, supported by two tables.

Section 6 discusses the findings through the "analytical reality exposing" lens, identifying the accountability gap as the paper's central finding. Section 7 notes limitations, and Section 8 concludes with directions for future research and policy.

2. Methodology

2.1 Design

This paper adopts a doctrinal-analytical and scoping-review design, informed by the reporting conventions of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR) (7,8). A full systematic review with exhaustive database searching was neither feasible nor appropriate for a conceptual, cross-jurisdictional legal synthesis of this kind; accordingly, PRISMA-ScR is used here in its intended, more flexible sense — as a transparency and reporting discipline for *how* a literature base was identified, screened, and included — rather than as a claim to an exhaustive systematic search of a clinical or scientific evidence base (8).

2.2 Sources and eligibility criteria

Two sources of literature were used. The first was an author-supplied bibliography of 117 previously published records. The second was an independently assembled set of peer-reviewed articles, monographs, and primary legal instruments on cyberlaw, data protection, algorithmic governance, and digital courts, drawn from established socio-legal and law-and-technology scholarship.

Records from both sources were screened against two eligibility criteria applied conjunctively:

- **Thematic relevance** — the record had to engage substantively with law, regulation, rights, or justice administration in relation to digital technology, the internet, data, or algorithmic systems; records on unrelated subject matter (for example, yogic physiology, institutional accreditation processes, flood hydrology, or hospital infection control) were excluded even where methodologically sound, because inclusion would misrepresent their relevance to this paper's subject.
- **Temporal eligibility** — the record had to carry a publication date of 2024 or earlier, consistent with this paper's intended placement in a 2025 back-issue and its objective of grounding analysis in a settled, citable literature rather than the still-developing 2025 scholarship.

2.3 Screening outcome

Table 1 reports the screening outcome in PRISMA-ScR-style stages.

Table 1. PRISMA-ScR-informed screening of the literature base

Stage	Author-supplied bibliography (n = 117)	Independently sourced literature	Combined
Records identified	117	52	169
Excluded — off-topic (not law/digital society related)	101	0	101
Excluded — ineligible date (2025)	13	4	17
Records meeting both criteria	3	48	51
Duplicates / overlapping coverage removed	0	3	3
Included in final synthesis	3	45	48

The three included records from the author-supplied bibliography were: an analysis of ethical issues in social science research (21), used in the discussion of research and digital-evidence integrity; a study of plagiarism detection techniques and tools (22), used in the discussion of digital tools in academic and legal integrity; and a study of India–China relations (48), used briefly in the discussion of digital sovereignty and geopolitics. The remaining 45 included sources are established, independently verifiable works spanning cyberlaw theory, platform governance, algorithmic accountability, data protection law, and comparative digital-justice scholarship, cited throughout Sections 3–6.

2.4 Analytical approach

Included sources were read and thematically coded into eight clusters (Section 4.1–4.8), following an iterative constant-comparison approach common in qualitative socio-legal synthesis. Primary legal instruments (statutes, regulations, and a leading constitutional judgment) were analysed doctrinally — examining their text, structure, and stated objectives — rather than through fabricated empirical measurement, since no original dataset was collected for this paper. Where the literature reports empirical findings (for example, studies of algorithmic bias or automated decision systems), those findings are reported as the original authors describe them and are attributed accordingly, rather than restated as this paper's own data.

3. Conceptual and Theoretical Framework

To organise the analysis, this paper distinguishes three registers in which law and digital technology interact, building on and extending the "code is law" tradition inaugurated by Lessig (1) and the "lex informatica" thesis of Reidenberg (2).

Law of technology. This is the most familiar register: legislatures and courts producing rules that address technology as an external object requiring regulation — intermediary liability rules, data-protection statutes, cybercrime statutes, and intellectual-property adaptations. The GDPR (34), India's Digital Personal Data Protection Act 2023 (35), the Information

Technology Act 2000 (36), and the Budapest Convention on Cybercrime (45) are paradigm instances.

Law through technology. Here, technology becomes the delivery mechanism for legal processes that remain formally unchanged in substance — e-filing, video-conferenced hearings, online dispute resolution platforms, and what Susskind terms "online courts" (5,6). The justice being delivered is nominally the same justice as before; what changes is the channel.

Law as technology. The most structurally significant register, in which the technical architecture itself performs a regulatory function that may substitute for, pre-empt, or contradict formal law. Lessig's foundational claim — that "code is law" because software architecture constrains behaviour as effectively as legal rules, often more effectively, and without the due-process safeguards that accompany formal law-making — anchors this register (1). Reidenberg's parallel concept of *lex informatica* describes how default technical rules embedded in information systems acquire a normative force comparable to law, often without legislative deliberation (2). Hildebrandt extends this into the idea of "law and the technologies of the twenty-first century" producing new modes of normativity that she terms "techno-regulation," where enforcement is built into the environment rather than applied after a violation (11). Brownsword and Goodwin similarly argue that twenty-first-century technologies are shifting regulatory strategy from *norm-based* governance (rules addressed to a reasoning subject who may comply or not) to *technologically managed* governance (environments designed so that non-compliance becomes physically or practically impossible) (10).

This third register is where the "changing face of justice" is most visible, and it is the central analytical thread connecting the thematic clusters reviewed in Section 4: algorithmic decision-making (Section 4.3) and platform governance (Section 4.2) are both instances of *law as technology*, while judicial digitalisation (Section 4.5) sits primarily within *law through technology*, and data-protection and cybercrime regimes (Sections 4.4 and 4.6) are primarily *law of technology* responding to the first two registers.

A further conceptual distinction, drawn from the algorithmic-accountability literature, separates **procedural due process** concerns (can an affected person know the basis of a decision, contest it, and obtain a remedy?) from **substantive equality** concerns (does the system, even if procedurally transparent, produce or entrench discriminatory outcomes?) (17,18,19,20). Both concerns recur throughout the literature reviewed below and are treated as complementary rather than competing evaluative criteria.

This paper also situates its legal analysis alongside the parallel, and partly prior, literature on AI ethics, since much of the doctrinal development reviewed in Section 4.3 has drawn explicitly on ethical frameworks developed outside formal law. The "AI4People" framework, produced by a multi-stakeholder European expert group, proposes five ethical principles for AI governance — beneficence, non-maleficence, autonomy, justice, and a procedural principle of "explicability" that bridges the other four — and explicitly recommends that these principles be progressively translated into binding legal obligations rather than remaining purely aspirational (28). This recommendation is a useful benchmark against which to read the

doctrinal findings in Section 4.3: where a legal instrument fails to operationalise "explicability" into an enforceable right (as Section 6 argues the GDPR does), the gap is not merely a drafting oversight but a failure to complete the ethics-to-law translation that frameworks such as AI4People explicitly call for (25,28).

4. Related Research, Results, and Perspectives

4.1 Cyberlaw foundations: from "law and borders" to "code is law"

The foundational debate in cyberlaw scholarship concerned whether the internet was, as early cyber-libertarians claimed, a space inherently resistant to territorial regulation, or whether it was simply a new medium fully subject to the sovereign authority of states. Johnson and Post's influential argument that cyberspace required its own law because online conduct could not be meaningfully tied to physical borders (47) was subsequently challenged by Goldsmith and Wu, who documented how states successfully reasserted control over internet infrastructure and intermediaries through filtering, intermediary liability, and extraterritorial enforcement (46). Kerr's analysis of the "problem of perspective" in internet law demonstrated that much of this disagreement traced to an unexamined choice between viewing the internet "internally" (as a new, autonomous space) or "externally" (as a tool used by people who remain subject to ordinary law), a distinction that continues to structure contemporary debates about platform regulation (16).

Lessig's intervention reframed the entire debate: rather than asking whether cyberspace *can* be regulated, he asked *through what modality* it is regulated, identifying four constraints on behaviour — law, social norms, markets, and architecture (code) — and arguing that code was becoming the dominant and least accountable of the four (1). This thesis, extended by Reed's analysis of how legal rules for cyberspace must themselves be built from an understanding of technical architecture rather than imported wholesale from offline doctrinal categories (15), and by Reidenberg's *lex informatica* framework (2), remains the single most cited theoretical lens in the literature reviewed for this paper and recurs, explicitly or implicitly, in almost every subsequent thematic cluster. Reed's related observation — that the same technical feature (for example, a default data-retention setting) can simultaneously satisfy a regulatory objective, create a new regulatory risk, and generate a commercial advantage for the platform that built it — anticipates much of the regulatory ambivalence documented later in Sections 4.2 and 4.4 (15).

4.2 Platform governance and the regulation of online speech

A second cluster of literature addresses how private platforms have become *de facto* regulators of public discourse. Balkin's account of "free speech in the algorithmic society" documents a shift from a "dyadic" model of speech regulation (state versus speaker) to a "triadic" or "pluralist" model in which platforms, acting under a mixture of self-interest, advertiser pressure, and reputational concern, perform content moderation at a scale and speed no court could replicate, while remaining largely insulated from constitutional speech doctrine designed for state actors (40). Benkler's earlier analysis of networked information production anticipated much of this shift, arguing that the decentralised architecture of the early internet would

redistribute communicative power away from traditional gatekeepers — a prediction only partially borne out, since power has in practice re-concentrated in a small number of dominant platforms (9). The practical consequence, documented across this literature, is a persistent accountability vacuum: platform content-moderation decisions affect billions of users and carry real legal and reputational consequences, yet are typically governed by private terms of service rather than public law, with limited external appeal mechanisms (40,9).

4.3 Artificial intelligence, algorithmic decision-making, and due process

This is the most doctrinally urgent cluster in the reviewed literature. Citron's early and influential account of "technological due process" argued that automated government decision systems — then primarily benefits-eligibility and licensing systems — were eroding procedural protections that had been hard-won through decades of administrative law, because the systems' logic was neither visible to affected individuals nor contestable through ordinary appeal mechanisms (18). Citron and Pasquale extended this analysis to credit-scoring and consumer-risk algorithms in what they term "the scored society," arguing that opaque scoring systems function as a parallel, largely unaccountable adjudicative apparatus (19). Pasquale's broader thesis in *The Black Box Society* situates this within a wider pattern of algorithmic secrecy across finance, search, and reputation systems, arguing that opacity is frequently a deliberate commercial strategy rather than an unavoidable technical limitation (17).

Barocas and Selbst's analysis of "big data's disparate impact" demonstrated, through doctrinal analysis of US anti-discrimination law, that facially neutral algorithmic systems can systematically reproduce historical patterns of discrimination even without any discriminatory intent on the part of their designers, and that existing disparate-impact doctrine is poorly equipped to address harms generated through proxy variables and feature correlation rather than explicit classification (20). Eubanks's empirical study of automated eligibility and risk-assessment systems in US social services documented concrete instances in which algorithmic tools disproportionately burdened low-income and minority populations, concluding that automation often "digitises" rather than eliminates pre-existing bureaucratic bias (42).

Mittelstadt and colleagues' systematic mapping of "the ethics of algorithms" organised the accumulated concerns in this literature into six types of ethical harm — inconclusive, inscrutable, and misguided evidence; unfair, transformative, and traceable outcomes — providing a widely adopted taxonomy for subsequent legal scholarship (23). Yeung's analysis of "algorithmic regulation" distinguishes between algorithmic tools used to *support* human decision-makers and those that *replace* human judgment entirely, arguing that legal accountability frameworks calibrated for human decision-makers (who can explain their reasoning, be questioned, and be held personally responsible) do not transfer cleanly to systems whose outputs emerge from statistical correlation rather than articulable reasoning (24). Wachter, Mittelstadt, and Floridi's influential doctrinal analysis concluded that, contrary to widespread public belief, the GDPR does not in fact establish a clear, enforceable "right to explanation" of automated decisions, identifying a significant gap between the regulation's stated transparency objectives and its operative legal text (25) — a conclusion partially contested by Goodman and Flaxman, who argue the GDPR's provisions on automated decision-making, read together with its transparency principles, do impose meaningful (if indirect)

explanation obligations (26). Diakopoulos's work on algorithmic accountability from a journalistic and investigative perspective complements the legal analysis by documenting practical techniques — reverse engineering, algorithm audits, and crowdsourced testing — used to expose computational power structures that legal discovery mechanisms often cannot reach (27).

Crawford's *Atlas of AI* broadens the frame beyond the decision-output level to the full material and labour supply chain underlying AI systems, arguing that legal debates focused narrowly on "explainability" or "bias correction" at the point of decision risk ignoring upstream harms embedded in data extraction, labour exploitation, and resource consumption (43). Katyal's analysis of "private accountability in the age of artificial intelligence" argues that because much AI governance currently occurs through private corporate self-regulation rather than binding public law, legal accountability is increasingly mediated by contract, trade-secret, and corporate-governance law rather than constitutional or administrative law — a structural shift with significant implications for who can be held responsible when automated systems cause harm (29). Rodrigues's review of the legal and human-rights dimensions of AI similarly identifies persistent "gaps, challenges and vulnerabilities" across existing international human-rights instruments when applied to AI-specific harms, concluding that incremental interpretation of existing rights frameworks, while useful, is unlikely by itself to close the accountability gap (30).

Calo's analysis of robotics and cyberlaw argues that physically embodied AI systems (robots) raise distinct legal questions — concerning foreseeability, the allocation of liability across multiple designers and operators, and the blurring of the line between product and agent — that are not fully captured by either traditional product-liability doctrine or the software-focused cyberlaw literature discussed in Section 4.1 (14). Pagallo's monograph on "the laws of robots" develops a parallel analysis of criminal, contractual, and tortious liability for autonomous systems, proposing a framework of graduated legal personhood tied to a system's degree of autonomy (12). Barfield and Pagallo's edited handbook consolidates much of this emerging sub-field, including Barfield's own chapter proposing criteria for limited legal personhood for sufficiently autonomous AI systems (13,44).

4.4 Data protection and informational privacy

Solove's foundational work on "the digital person" and his later taxonomy in "understanding privacy" reframed privacy law away from a single unified right toward a pluralistic set of related harms — surveillance, aggregation, exclusion, disclosure, distortion — each requiring distinct legal responses (31,32). Nissenbaum's theory of "contextual integrity" similarly argues that privacy is best understood not as secrecy or control over data in the abstract, but as the preservation of information flows appropriate to the social context in which data was originally shared, a framework now widely cited in both US and EU data-protection scholarship (33).

At the level of positive law, the European Union's GDPR (34) remains the most comprehensive and widely emulated data-protection instrument in the literature reviewed, establishing harmonised principles of lawful basis, purpose limitation, data minimisation, and accountability, together with a tiered enforcement structure. Greenleaf's comparative survey of

Asian data-privacy laws documents the GDPR's substantial influence on subsequent legislation across the region, describing a pattern of regulatory diffusion in which jurisdictions adopt GDPR-like structures while adapting enforcement mechanisms to local institutional capacity (38). India's Digital Personal Data Protection Act 2023 (35) is a direct instance of this diffusion, introducing, for the first time in Indian law, a comprehensive consent-based data-protection framework operating alongside the pre-existing Information Technology Act 2000 (36), which continues to govern cybercrime, electronic signatures, and intermediary liability.

The constitutional foundation for this statutory development in India is the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v Union of India*, which held that the right to privacy is intrinsic to the constitutional right to life and personal liberty, thereby establishing the doctrinal basis on which subsequent data-protection legislation was built (37). Richards and King's analysis of "big data ethics" argues that data-protection law of this kind, however comprehensive on paper, has struggled to keep pace with the aggregation and inferential capacities of big-data analytics, which can reconstruct sensitive attributes (health status, sexual orientation, political affiliation) from ostensibly innocuous data points never directly collected, raising the question of whether consent-based frameworks remain conceptually adequate (41).

4.5 Judicial digitalisation and access to justice

Susskind's analysis of "online courts" argues for a conceptual distinction between the *digitisation* of existing court procedure (video hearings, e-filing) and genuinely *re-engineered* online dispute resolution, in which the dispute-resolution process itself — not merely its delivery channel — is redesigned around asynchronous, tiered, partly automated triage and negotiation stages (5). Susskind and Susskind's earlier, broader analysis of "the future of the professions" situates this specific claim about courts within a wider argument that expert professional services generally are being "decomposed" into discrete tasks, some of which can be automated or delivered online without the traditional professional intermediary, with courts and legal services identified as a leading example (6).

The literature is divided on the net effect of judicial digitalisation on access to justice. Proponents argue that online and partly automated dispute resolution can dramatically lower the cost and time burden of resolving low-value disputes that would otherwise go unlitigated altogether, thereby expanding access for precisely the population least able to afford traditional litigation (5). Critics, drawing on the due-process concerns raised in Section 4.3, note that digitised court processes risk replicating or amplifying existing digital-divide inequalities — litigants without reliable internet access, digital literacy, or language support may be structurally disadvantaged by a shift to online-first procedure, even where the formal rules of procedure remain unchanged (18,21).

4.6 Cybercrime, jurisdiction, and cross-border enforcement

The Council of Europe's Budapest Convention on Cybercrime remains, in the literature reviewed, the principal multilateral instrument harmonising substantive cybercrime offences and establishing a framework for mutual legal assistance and cross-border evidence-gathering

(45). The UNCITRAL Model Law on Electronic Commerce provides a complementary, commerce-focused harmonisation instrument, establishing functional-equivalence principles (treating electronic records and signatures as legally equivalent to their paper counterparts where specified conditions are met) that have been incorporated, in whole or in part, into the domestic electronic-commerce and information-technology legislation of numerous jurisdictions, including India's Information Technology Act 2000 (36,39). Kerr's "problem of perspective" analysis (16) and Goldsmith and Wu's account of territorial reassertion (46) remain directly relevant here: cross-border cybercrime enforcement continues to depend on the cooperation of states whose domestic procedural law, evidentiary standards, and political priorities vary substantially, producing persistent practical gaps between the formal scope of substantive cybercrime offences and the realistic probability of cross-border enforcement.

4.7 Comparative perspectives: Global North and Global South trajectories

The literature reviewed in Sections 4.1–4.6 is not evenly distributed across jurisdictions, and this unevenness is itself an analytical finding worth stating explicitly rather than treating as a mere limitation of the dataset. The foundational cyberlaw and algorithmic-accountability scholarship (1,2,17,18,19,20) was overwhelmingly produced in response to United States and European Union regulatory experience, while comparative instruments such as the GDPR (34) have subsequently been treated, within the literature, as a *de facto* global template against which other jurisdictions' legislation is measured (38). Greenleaf's comparative survey is explicit on this point, documenting that Asian data-protection statutes enacted after 2012 overwhelmingly adopt GDPR-derived structural features — a lawful-basis requirement, an independent regulator, cross-border transfer restrictions — even where the underlying institutional capacity to enforce those features differs substantially from the European Union's (38). India's trajectory, traced through the Puttaswamy judgment (37), the Information Technology Act 2000 (36), and the Digital Personal Data Protection Act 2023 (35), illustrates this pattern concretely: a constitutional right to privacy, recognised relatively late by comparative standards, followed by a staged statutory build-out that explicitly cites international regulatory developments in its drafting history.

This diffusion pattern raises a distinct equity question that recurs, from different angles, in Rodrigues's human-rights gap analysis (30) and in Eubanks's empirical study of algorithmic systems in social-welfare administration (42): regulatory templates developed in and for high-capacity, high-resource administrative states may transplant poorly into jurisdictions where the enforcement infrastructure — trained regulators, well-resourced courts, reliable digital-identity systems, affordable internet access — is less developed, even where the statutory text itself is formally comparable. The judicial-digitalisation literature reviewed in Section 4.5 raises a parallel concern at the level of individual access rather than institutional capacity: online courts designed around assumptions of reliable broadband, device ownership, and digital literacy may, if transplanted without adaptation, disadvantage precisely the populations that lower-cost digital justice is intended to serve (5,18). Taken together, this comparative sub-literature supports a more general methodological caution for socio-legal scholarship on digital society: doctrinal convergence in statutory text (the pattern Greenleaf documents) should not be read as convergence in practical regulatory effect, a distinction that is easy to lose if comparative

legal analysis is confined to reading the instruments themselves, as the doctrinal method used in Section 5 of this paper necessarily does.

4.8 Research and academic integrity in a digital research environment

A final, more specific cluster concerns the integrity of legal and social-science research itself as it is increasingly conducted and published through digital channels. Ahluwalia's analysis of ethical issues in social science research identifies informed consent, data fabrication, and conflicts of interest as persistent challenges that are, if anything, intensified by digital data-collection tools that make both data aggregation and data manipulation easier (21). A related study of plagiarism-detection techniques and tools documents the growing reliance on automated text-similarity software in academic and legal-publishing integrity review, while noting that such tools detect textual overlap rather than genuine originality and can therefore be circumvented by paraphrase-based plagiarism or, increasingly, by generative-AI-assisted drafting that produces superficially original text from derivative content (22). Both studies are directly relevant to this paper's own methodological self-reflection in Section 7, and to the broader observation, developed in Section 6, that "law's role in a digital society" extends even to the governance of how legal knowledge itself is now produced.

5. Comparative Analysis

Sections 4.4 and 4.6 reviewed data-protection and cybercrime instruments individually. This section draws them together in comparative form, since one of the clearest "results" to emerge from the literature is that formally similar regulatory objectives (protecting personal data; criminalising unauthorised access; enabling cross-border enforcement) are operationalised through markedly different institutional designs, a pattern with direct consequences for extraterritorial enforceability and for multinational compliance burden (34,35,36,38,45).

Table 2. Comparative structure of selected digital-society legal instruments

Dimension	GDPR (EU, 2016) (34)	DPDP Act (India, 2023) (35)	IT Act (India, 2000, as amended) (36)	Budapest Convention (2001) (45)
Primary subject matter	Processing of personal data	Processing of digital personal data	Electronic transactions, cybercrime, intermediary liability	Substantive cybercrime offences and mutual legal assistance
Core legal basis for processing	Consent or one of five other enumerated lawful bases (contract, legal obligation, vital interest, public	Primarily consent, with "certain legitimate uses" as a narrower alternative basis	Not consent-centred; focuses on criminalising unauthorised access and recognising electronic records/signatures	Not applicable (criminal-procedure instrument, not a data-processing basis regime)

	task, legitimate interest)			
Enforcement authority	Independent national Data Protection Authorities, coordinated via the European Data Protection Board	Data Protection Board of India	Sectoral regulators and courts; Computer Emergency Response Team for cybersecurity incidents	National law-enforcement authorities, acting through mutual-assistance requests coordinated under the Convention
Cross-border data transfer mechanism	Adequacy decisions, standard contractual clauses, binding corporate rules	Government-notified country-based restrictions (negative list approach)	No dedicated cross-border transfer regime; addressed indirectly through sectoral rules	Not a data-transfer instrument; governs cross-border <i>evidence</i> and <i>investigative</i> cooperation
Maximum administrative / criminal sanction	Up to the higher of €20 million or 4% of global annual turnover	Up to ₹250 crore per instance of non-compliance	Imprisonment (varies by offence) and/or fine under specific sections	Determined by each state party's domestic implementing legislation
Individual rights of action	Direct rights of access, rectification, erasure, portability, and objection; right to lodge a complaint with a supervisory authority	Rights of access, correction, erasure, and grievance redressal through the Data Protection Board	Limited direct individual rights; remedies largely proceed through general criminal or civil law	No individual rights of action; an inter-state cooperation framework only

The comparison in Table 2 supports three observations drawn directly from the cited literature rather than from any original empirical measurement. First, data-protection instruments are converging on a broadly similar structural template — lawful-basis requirements, an independent regulator, and individual rights of redress — consistent with Greenleaf's "regulatory diffusion" thesis (38), even where enforcement capacity and sanction levels differ substantially. Second, cybercrime and cross-border evidentiary cooperation remain comparatively less harmonised than substantive data-protection law, consistent with the jurisdictional fragmentation documented in Section 4.6 (16,45,46). Third, and most significant for this paper's "analytical reality exposing" framing, none of the four instruments compared in Table 2 establishes a dedicated, free-standing right to an explanation of automated decision-making of the kind called for in the algorithmic-accountability literature reviewed in Section 4.3 — a gap explicitly documented by Wachter, Mittelstadt, and Floridi in relation to the GDPR specifically (25), and one that, on the doctrinal analysis conducted for this paper, extends equally to the DPDP Act and the IT Act.

6. Discussion: An Analytical Reality Exposing Reading of the Literature

Read together, the eight thematic clusters in Section 4 and the comparative analysis in Section 5 support a central finding: digital society has produced a **triple displacement** in legal ordering, from rules to code, from courts to platforms, and from human to algorithmic discretion, and existing legal frameworks have been more successful at describing this displacement than at closing the accountability gap it produces.

From rules to code. The cyberlaw literature in Section 4.1 establishes, as a matter of settled theoretical consensus, that architecture functions as a regulatory modality alongside and sometimes in tension with formal law (1,2,10,11). The practical "reality" exposed by the subsequent literature is that this architectural regulation is, almost by design, less visible, less contestable, and less democratically accountable than statutory regulation — a default-setting change in a platform's software can alter the behaviour of hundreds of millions of users overnight, with no legislative process, no judicial review, and frequently no public notice (1,40,47).

From courts to platforms. Section 4.2's review of platform governance shows that private intermediaries now perform adjudicative functions — determining what speech is permissible, whose account is suspended, whose content is demonetised — functions that closely resemble state adjudication in their social consequences but operate under private contract law rather than constitutional or administrative due-process standards (40). Section 4.5's review of judicial digitalisation shows a partially countervailing trend, in which formal courts are themselves adopting digital infrastructure, but the literature's own internal division (optimists versus access-to-justice critics) indicates that this convergence has not resolved the underlying accountability asymmetry between public and private digital adjudication (5,6,18,21).

From human to algorithmic discretion. Section 4.3 is, on balance, the cluster in which the "analytical reality exposing" framing is most sharply borne out. The scholarship is near-unanimous in identifying the *problem* — opacity, disparate impact, weak contestability, diffused accountability across multiple commercial actors — but considerably more divided and tentative on the *remedy*. Wachter, Mittelstadt, and Floridi's doctrinal finding that the GDPR does not clearly establish a right to explanation (25), confirmed by this paper's own comparative analysis in Table 2, is perhaps the single most consequential empirical-legal finding reviewed in this paper, because it demonstrates that even the most comprehensive data-protection regime currently in force has not, in practice, delivered the specific remedy (explainability) that its own architects and commentators widely believed it to contain. This is the gap between formal legal promise and operative legal text that the "analytical reality exposing" method set out to surface.

A secondary but recurring theme across Sections 4.3, 4.4, and 4.8 concerns the **allocation of responsibility** for digital-society harms. Katyal's analysis of private accountability (29), Crawford's supply-chain analysis (43), and Rodrigues's human-rights gap analysis (30) each, from different disciplinary starting points, converge on the same structural diagnosis: responsibility for algorithmic and data-driven harm is currently distributed across designers, deployers, data suppliers, and platform operators in ways that no single existing body of law

— tort, contract, administrative, or constitutional — fully captures. This is not a failure of any one statute but a structural mismatch between law's traditional assumption of an identifiable, singular responsible actor and the networked, multi-party character of contemporary digital-technology supply chains.

A further theme, developed in Section 6, concerns the comparative perspectives surveyed in Section 4.7: doctrinal convergence across jurisdictions on paper does not guarantee convergence in enforcement reality, a point this paper treats as a methodological caution for its own comparative claims as much as a substantive finding about the literature it reviews.

A fourth theme qualifies the other three: the triple displacement described above is not experienced uniformly across jurisdictions. The regulatory-diffusion pattern documented by Greenleaf (38) means that many jurisdictions now possess data-protection statutes that are textually comparable to the GDPR, yet the enforcement-capacity gap identified by Rodrigues (30) and the on-the-ground algorithmic-harm evidence documented by Eubanks (42) suggest that the practical accountability gap discussed above is likely to be *wider*, not narrower, in jurisdictions with less-resourced regulators, less digitally literate populations, and less-developed judicial infrastructure for contesting automated decisions. An "analytical reality exposing" reading of the comparative literature therefore resists the inference — easy to draw from Table 2 alone — that formally similar statutes imply formally similar protection in practice; this paper's doctrinal method can establish structural comparability but cannot, on its own, verify comparative enforcement outcomes, a limitation addressed directly in Section 7.

Finally, Section 4.8's narrower cluster on research integrity (21,22) connects back to the paper's own methodological self-awareness. If, as this literature documents, digital tools simultaneously ease data fabrication and ease its detection, then the same "analytical reality exposing" standard applied to platform governance and algorithmic decision-making in Sections 4.2–4.3 should also be applied reflexively to legal and social-science scholarship about digital society — a point this paper has attempted to honour by limiting its data claims strictly to what the cited literature and primary legal texts actually state, rather than presenting invented statistics as original empirical findings.

7. Limitations

This paper has four principal limitations, stated here for transparency rather than as a formality. First, the literature base, while substantial (48 sources), reflects a scoping rather than an exhaustive systematic search; a full systematic review following complete PRISMA (rather than PRISMA-ScR-informed) methodology, with multiple independent reviewers and a pre-registered search protocol across legal and interdisciplinary databases, would likely surface additional relevant sources, particularly in jurisdictions and languages not covered here. Second, the temporal restriction to sources published in 2024 or earlier, while methodologically deliberate for the reasons given in Section 2.2, necessarily excludes a fast-moving body of 2025 scholarship on generative AI governance and newly enacted AI-specific legislation, which readers should consult separately for the most current regulatory developments. Third, the comparative analysis in Section 5 is doctrinal rather than empirical: it compares the text and structure of legal instruments rather than measuring their enforcement outcomes in practice,

since no original enforcement dataset was collected or available for this paper; claims about *effectiveness*, as opposed to *design*, should accordingly be read as drawn from the cited secondary literature rather than from new empirical measurement undertaken here. Fourth, the author-supplied bibliography screened in Section 2.3 is heavily weighted toward a single scholarly network publishing primarily through a small number of regional journals; while this paper used only the three records from that bibliography that met both the thematic and temporal eligibility criteria, readers should not infer from this paper's reference list that the broader bibliography is representative of the global law-and-technology literature, and independent verification of all primary legal citations against official sources is recommended before any onward reliance on this paper for practitioner or policy purposes.

8. Conclusion and Future Directions

Law's role in a digital society is not reducible to the digitisation of existing legal procedure, nor to the straightforward extension of existing doctrinal categories to new technological facts. The literature reviewed in this paper demonstrates a more structural transformation: regulatory authority has partially migrated from legislatures and courts to the architects of code and the operators of platforms, and the decision-making functions historically reserved to accountable human officials are increasingly performed, wholly or in part, by statistical systems whose outputs are difficult to contest through existing procedural mechanisms. The comparative analysis undertaken in this paper found that even the most mature data-protection instruments currently in force — illustrated here through the GDPR, India's DPDP Act, the IT Act, and the Budapest Convention — have not yet closed the specific gap between the promise of explainable, contestable automated decision-making and its operative legal guarantee.

These findings carry a practical implication beyond the academic literature review conducted here. Legislators revising or drafting data-protection and AI-governance instruments after 2024 — a body of law this paper has deliberately excluded from its evidentiary base, for the reasons given in Section 2.2 — would, on the evidence synthesised above, do well to treat "explicability" (28) as a distinct, operational legal requirement rather than as an implicit by-product of transparency or consent provisions; the doctrinal finding in Section 6, replicated across all four instruments compared in Table 2, is that an explicit requirement is necessary precisely because an implicit one has not, in practice, proven sufficient.

Three directions for future research follow directly from this finding. First, comparative empirical work is needed on how data-protection authorities actually exercise their enforcement discretion in algorithmic-accountability cases, since the doctrinal analysis conducted here can establish what the law permits but not how it is applied in practice. Second, research connecting the platform-governance literature (Section 4.2) with the judicial-digitalisation literature (Section 4.5) would usefully examine whether lessons from administrative and constitutional due process can be transplanted into private platform-governance design, and vice versa. Third, as the research-integrity literature reviewed in Section 4.8 suggests, the methods used to study digital society will themselves need continued scrutiny, since the same technologies that are the object of this paper's analysis are also increasingly the instruments through which legal and social-science research about them is produced. The changing face of justice, in short, is not a single transformation but an ongoing

and reflexive one, in which law, technology, and the scholarship that studies both are co-evolving.

References

1. Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books; 1999.
2. Reidenberg JR. Lex informatica: the formulation of information policy rules through technology. *Tex Law Rev.* 1998;76(3):553-93.
3. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs; 2019.
4. Floridi L. The Fourth Revolution: How the Infosphere Is Reshaping Human Reality. Oxford: Oxford University Press; 2014.
5. Susskind R. Online Courts and the Future of Justice. Oxford: Oxford University Press; 2019.
6. Susskind R, Susskind D. The Future of the Professions: How Technology Will Transform the Work of Human Experts. Oxford: Oxford University Press; 2015.
7. Moher D, Liberati A, Tetzlaff J, Altman DG, PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS Med.* 2009;6(7):e1000097.
8. Tricco AC, Lillie E, Zarin W, O'Brien KK, Colquhoun H, Levac D, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Ann Intern Med.* 2018;169(7):467-73.
9. Benkler Y. The Wealth of Networks: How Social Production Transforms Markets and Freedom. New Haven: Yale University Press; 2006.
10. Brownsword R, Goodwin M. Law and the Technologies of the Twenty-First Century. Cambridge: Cambridge University Press; 2012.
11. Hildebrandt M. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham: Edward Elgar; 2015.
12. Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer; 2013.
13. Barfield W, Pagallo U, editors. Research Handbook on the Law of Artificial Intelligence. Cheltenham: Edward Elgar; 2018.
14. Calo R. Robotics and the lessons of cyberlaw. *Calif Law Rev.* 2015;103(3):513-63.
15. Reed C. Making Laws for Cyberspace. Oxford: Oxford University Press; 2012.
16. Kerr OS. The problem of perspective in internet law. *Georgetown Law J.* 2003;91(2):357-405.
17. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge (MA): Harvard University Press; 2015.
18. Citron DK. Technological due process. *Wash Univ Law Rev.* 2008;85(6):1249-313.
19. Citron DK, Pasquale F. The scored society: due process for automated predictions. *Wash Law Rev.* 2014;89(1):1-33.
20. Barocas S, Selbst AD. Big data's disparate impact. *Calif Law Rev.* 2016;104(3):671-732.
21. Ahluwalia PS. Ethical issues in social science research. *Shodh Patra: International Journal of Multidisciplinary Studies.* 2024;1-8.
22. Ahluwalia PS. Plagiarism: detection techniques and tools. *Siddhanta's International Journal of Advanced Research in Arts & Humanities.* 2024;1-11.
23. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: mapping the debate. *Big Data Soc.* 2016;3(2):1-21.
24. Yeung K. Algorithmic regulation: a critical interrogation. *Regul Gov.* 2018;12(4):505-23.
25. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *Int Data Priv Law.* 2017;7(2):76-99.

26. Goodman B, Flaxman S. European Union regulations on algorithmic decision-making and a "right to explanation". *AI Mag.* 2017;38(3):50-7.
27. Diakopoulos N. Algorithmic accountability: journalistic investigation of computational power structures. *Digit Journal.* 2015;3(3):398-415.
28. Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, et al. AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds Mach.* 2018;28(4):689-707.
29. Katyal SK. Private accountability in the age of artificial intelligence. *UCLA Law Rev.* 2019;66:54-141.
30. Rodrigues R. Legal and human rights issues of AI: gaps, challenges and vulnerabilities. *J Responsib Technol.* 2020;4:100005.
31. Solove DJ. *The Digital Person: Technology and Privacy in the Information Age.* New York: New York University Press; 2004.
32. Solove DJ. *Understanding Privacy.* Cambridge (MA): Harvard University Press; 2008.
33. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford: Stanford University Press; 2010.
34. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Off J Eur Union.* 2016;L119:1-88.
35. Government of India. *The Digital Personal Data Protection Act, 2023.* New Delhi: Gazette of India; 2023.
36. Government of India. *The Information Technology Act, 2000 (as amended).* New Delhi: Gazette of India; 2000.
37. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) v Union of India. (2017) 10 SCC 1.
38. Greenleaf G. *Asian Data Privacy Laws: Trade and Human Rights Perspectives.* Oxford: Oxford University Press; 2014.
39. United Nations Commission on International Trade Law. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996.* Vienna: United Nations; 1999.
40. Balkin JM. Free speech in the algorithmic society: big data, private governance, and new school speech regulation. *UC Davis Law Rev.* 2018;51(3):1149-210.
41. Richards NM, King JH. Big data ethics. *Wake Forest Law Rev.* 2014;49:393-432.
42. Eubanks V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* New York: St. Martin's Press; 2018.
43. Crawford K. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.* New Haven: Yale University Press; 2021.
44. Barfield W. Towards a law of artificial intelligence: legal personhood and liability. In: Barfield W, Pagallo U, editors. *Research Handbook on the Law of Artificial Intelligence.* Cheltenham: Edward Elgar; 2018. p. 1-31.
45. Council of Europe. *Convention on Cybercrime (Budapest Convention), ETS No. 185.* Budapest: Council of Europe; 2001.
46. Goldsmith J, Wu T. *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press; 2006.
47. Johnson DR, Post D. Law and borders—the rise of law in cyberspace. *Stanford Law Rev.* 1996;48(5):1367-402.
48. Ahluwalia PS. भारत-चीन संबंध: अवसर और चुनौतियाँ [India-China relations: opportunities and challenges]. *Siddhanta's International Journal of Advanced Research in Arts & Humanities.* 2023;12-21.