INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"CONSTITUTIONALISING CYBERSPACE: DOMESTIC ENFORCEMENT OF DIGITAL RIGHTS VS. GLOBAL INTERNET GOVERNANCE, AND THE IMPORTANCE OF ALGORITHMIC TRANSPARENCY

Opening the Black Box: Legal Audits for Algorithmic Explainability"

AUTHOR – JOHN PAUL MANJALY, INDEPENDENT RESEARCHER

BEST CITATION – JOHN PAUL MANJALY, "CONSTITUTIONALISING CYBERSPACE: DOMESTIC ENFORCEMENT OF DIGITAL RIGHTS VS. GLOBAL INTERNET GOVERNANCE, AND THE IMPORTANCE OF ALGORITHMIC TRANSPARENCY, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (12) OF 2026, PG. 226-240, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

Constitutional law was built for a world in which power sat with the state and stopped at its borders. Cyberspace unsettles both assumptions: much of the power over speech, privacy and opportunity online now lies with a few private platforms that operate across jurisdictions through automated systems whose reasoning is hidden even from their users. This paper studies how India, the European Union and the United States have tried to carry constitutional values into this space, and where those efforts meet territorial sovereignty and the loose arrangements of global internet governance. The paper then asks whether a 'right to explanation' can be made real through legal audits. Drawing on developments up to October 2026, including the Sahyog portal ruling, *Dun & Bradstreet Austria* and the first non-compliance decision under the Digital Services Act, it argues that declarations of rights achieve little without institutions able to inspect the systems they govern, and proposes that India add an individual right against solely automated decisions and a statutory audit mechanism, with confidentiality safeguards, under an independent regulator.

Keywords: digital constitutionalism; internet governance; data protection; algorithmic accountability; right to explanation; Digital Services Act; India.

I. INTRODUCTION

In 1996 John Perry Barlow told the 'Governments of the Industrial World' that they had no sovereignty where cyberspace gathers.[669] Thirty years later, states block websites, insist that data be stored at home and fine foreign companies sums that once seemed absurd. Yet Barlow was not wholly wrong. The everyday rules on what a person may post, whose content is seen and how personal data is used are still written largely by private firms and enforced by software far more often than by courts. Lessig saw this early: the architecture of a network regulates behaviour as surely as any statute, so that 'code is law'.[670]

[669] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (Davos, 8 February 1996).
[670] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 6.

This paper sits where these two realities meet. It asks what it means to 'constitutionalise' cyberspace and how far India, the European Union (EU) and the United States (US) treat digital interests as fundamental rights; how domestic enforcement of those rights fares against a global internet governed partly by multistakeholder bodies and partly by rival sovereign claims; and whether law, through rights to explanation and audits, can open the 'black box' of algorithmic decisions.

The method is doctrinal and comparative, covering developments up to October 2026. The paper first deals with constitutionalisation and digital rights, then with global governance and sovereignty, and then with algorithmic transparency and audits, before setting out findings and suggestions and concluding.

1.Constitutionalising Cyberspace and Digital Rights

1.1 CONSTITUTIONALISATION: MEANING AND SCOPE

In this paper, the term 'constitutionalisation' is not used in the sense of drafting a written constitution for the internet. It describes how values that have traditionally limited public power, such as legality, due process, proportionality, equality and free expression, are carried into the digital environment and applied to the private actors who hold power there, a process scholars call 'digital constitutionalism'. For Celeste, it is an ideology whose purpose is to fit the core commitments of present-day constitutionalism to the conditions of a digitised society.[671] De Gregorio traces a European shift from shielding intermediaries to help the market grow towards limiting platform power in the name of fundamental rights.[672] Teubner had earlier suggested that transnational private regimes develop 'constitutional fragments' of their own.[673]

Two features of cyberspace make the task hard. The first is where power lies: platforms decide on millions of posts a day under terms of service they write and revise at will. Klonick describes these companies as the 'New Governors' of speech on the internet.[674] For Balkin, free speech is now a triangle of states, private infrastructure owners and speakers.[675] The second is automation: most decisions on visibility and removal are made by classifiers, so notice, hearing and reasons must be rebuilt for machines, which Citron called 'technological due process'.[676]

1.2 ELEVATING DIGITAL RIGHTS TO FUNDAMENTAL STATUS

The UN Human Rights Council declared in 2012 that whatever rights individuals enjoy in the physical world deserve equal protection on the internet.[677] Stating this idea is easy; giving it practical effect is not. Three rights show the difficulty.

Privacy is the most developed. In *Puttaswamy* a nine-judge bench of the Supreme Court of India held that privacy is a fundamental right protected by Article 21 and by Part III as a whole, and that any intrusion must satisfy legality, legitimate aim and proportionality.[678] The plurality discussed

[671] Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers & Technology 76.
[672] Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022).
[673] Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (OUP 2012).
[674] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598.
[675] Jack M Balkin, 'Free Speech Is a Triangle' (2018) 118 Columbia Law Review 2011.
[676] Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.
[677] UNHRC Res 20/8, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (5 July 2012) UN Doc A/HRC/RES/20/8.
[678] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

informational privacy in the era of big data and asked the government to put a data protection regime in place. Parliament responded with the Digital Personal Data Protection Act 2023 (DPDP Act). The rules framed under it were notified in November 2025, and the bulk of the obligations placed on data fiduciaries take effect only after a further eighteen months.[679]

The right to be forgotten is less settled. It began with *Google Spain*, where the Court of Justice of the European Union (CJEU) held that a search engine could be required to delist links to information about a person that was inadequate, irrelevant or no longer relevant.[680] It is now the right to erasure under Article 17 of the General Data Protection Regulation (GDPR).[681] In India, Kaul J's concurring opinion in *Puttaswamy* accepted the idea, subject to free expression, archiving and public interest.[682] High Courts have granted relief case by case, as in *Jorawar Singh Mundy*.[683] Section 12 of the DPDP Act gives a right to erasure, but it is tied to consent and purpose and does not resolve the conflict with the press or open court records.

Access to the internet is the least settled. The Kerala High Court in *Faheema Shirin* held that cutting off a student's internet access in a college hostel violated her rights to education and privacy.[684] The Supreme Court in *Anuradha Bhasin* accepted that expression and business conducted online fall within the protection of Article 19(1)(a) and (g), and it insisted that any shutdown be necessary, proportionate, limited in time and subject to periodic review. The Court stopped short, though, of recognising internet access as an independent fundamental right.[685] Protection for a medium is not an entitlement to it, and the state's duty to provide connectivity remains a question of policy rather than of right.

1.3 COMPARATIVE CONSTITUTIONAL APPROACHES

INDIA

The Indian approach has been led by the courts. In *Shreya Singhal* Vs. Union of India, the Supreme Court of India struck down section 66A of the Information Technology Act 2000 (IT Act) for vagueness and read down section 79(3)(b), so that intermediaries need act only on a court order or government notification.[686] *Puttaswamy* supplied the proportionality test, which the Aadhaar judgment applied to the national digital identity scheme, striking down section 57 of the Aadhaar Act so far as it allowed private use.[687] What India lacks is an independent regulator: the Data Protection Board is appointed by the Central Government under sections 18 and 19 of the DPDP Act, and section 17(2)(a) lets the government exempt its own agencies.

EUROPEAN UNION

The EU model is the most openly rights-based. Article 7 of the Charter of Fundamental Rights protects private life, and Article 8 adds a separate right to data protection supervised by an independent

[679] Digital Personal Data Protection Act 2023 (Act 22 of 2023); Digital Personal Data Protection Rules 2025 (notified 13 November 2025).
[680] Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* EU:C:2014:317.
[681] Regulation (EU) 2016/679 on the protection of personal data [2016] OJ L119/1 (GDPR), art 17.
[682] *Puttaswamy* (n 10) (Kaul J).
[683] *Jorawar Singh Mundy v Union of India* WP(C) 3918/2021 (Delhi HC, order dated 12 April 2021).
[684] *Faheema Shirin RK v State of Kerala* (Kerala HC, 19 September 2019).
[685] *Anuradha Bhasin v Union of India* (2020) 3 SCC 637.
[686] *Shreya Singhal v Union of India* (2015) 5 SCC 1.
[687] *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1.

authority.[688] The GDPR gives effect to Article 8 and has become the global reference point. The Digital Services Act (DSA) goes further. Under it, the largest platforms have to identify and mitigate the 'systemic risks' their services pose to fundamental rights, and an outside auditor must examine how far they comply.[689] The platform is treated less as private property and more as power that must be checked.

UNITED STATES

The American model starts at the other end. Since *Reno v ACLU* the internet has enjoyed full First Amendment protection, and *Packingham Vs. North Carolina* called social media perhaps the most important places for the exchange of views.[690] Under the Fourth Amendment, *Riley* and *Carpenter* required warrants for phone searches and historical cell-site records, departing from the third-party doctrine of *Smith v Maryland*.[691] But these protections bind only the government, and platforms are themselves speakers: *Moody v NetChoice* treated feed curation as protected expression, making neutrality or must-carry rules hard to impose.[692] With section 230 of the Communications Decency Act shielding platforms from liability for user content and good-faith moderation, the system protects speakers from the state but leaves private power largely alone.[693]

1.4 HORIZONTAL AND VERTICAL APPLICATION OF RIGHTS

The gap is widest on who is bound by rights. Under the American state action doctrine, rights run only against government actors; *Halleck* held that a private body running a forum for speech does not become a state actor by opening it to the public.[694] The company-town doctrine of *Marsh v Alabama* has never been extended to platforms.[695]

India has moved the other way. In *Kaushal Kishor* a Constitution Bench held, by majority, that rights under Articles 19 and 21 can be enforced even against persons other than the state and its instrumentalities.[696] The ruling has not yet been tested against a platform's moderation choices, but it opens the door to claims that the Article 12 test of 'State' had kept shut.

The EU stands in between. Charter rights formally bind EU institutions and member states but reach private parties through legislation; Article 14(4) of the DSA, requiring platforms to apply their terms with due regard to users' fundamental rights, is horizontal effect by statute. In Gardbaum's terms, the EU relies on statutory horizontal effect, India is experimenting with the direct form, and the US rejects both at the constitutional level.[697]

1.5 JURISDICTIONAL CHALLENGES AGAINST TRANSNATIONAL TECHNOLOGY COMPANIES

Enforcing domestic rights against global companies is an old problem in a new setting: data is stored in one country, processed in another and viewed everywhere. Goldsmith and Wu showed that

[688] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7, 8, 11 and 47.
[689] Regulation (EU) 2022/2065 on a Single Market for Digital Services [2022] OJ L277/1 (DSA), arts 34, 35 and 37.
[690] *Reno v American Civil Liberties Union* 521 US 844 (1997); *Packingham v North Carolina* 582 US 98 (2017).
[691] *Riley v California* 573 US 373 (2014); *Carpenter v United States* 585 US 296 (2018); *Smith v Maryland* 442 US 735 (1979).
[692] *Moody v NetChoice LLC* 603 US 707 (2024).
[693] 47 USC § 230.
[694] *Manhattan Community Access Corp v Halleck* 587 US 802 (2019).
[695] *Marsh v Alabama* 326 US 501 (1946).
[696] *Kaushal Kishor v State of Uttar Pradesh* (2023) 4 SCC 1.
[697] Stephen Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102 Michigan Law Review 387.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

governments still hold strong levers, because companies need local assets, payment channels and staff.[698] The *Yahoo!* dispute of 2000, in which a Paris court ordered the company to stop French users reaching auctions of Nazi memorabilia, showed both the reach of local law and the difficulty of enforcing it abroad; the Ninth Circuit later dismissed Yahoo!'s suit against the French order without settling its enforceability.[699]

Three tools are now in common use. The first is prescriptive jurisdiction based on targeting, as in Article 3(2) of the GDPR and section 3(b) of the DPDP Act, which extend each law to processing abroad connected with offering goods or services within the territory.[700] The second is a demand for local presence. Under Rule 4(1) of the Intermediary Rules 2021, every significant social media intermediary must name three officers who live in India: a Chief Compliance Officer, a nodal contact person and a Resident Grievance Officer.[701] The third is conditional immunity: a platform that ignores lawful orders loses its safe harbour under section 79 of the IT Act.

The harder question concerns remedies with global effect. The CJEU ruled in *Google v CNIL* that a search engine was under no EU-law obligation to remove results across all its global versions, while leaving national authorities free to order such removal once they had weighed the competing rights.[702] Nine days later, in *Glawischnig-Piesczek*, it allowed a national court to order worldwide removal of identical or equivalent defamatory content.[703] A right that stops at the border can be defeated with a virtual private network; one that crosses it imposes one country's balance between speech and privacy on everyone else. Svantesson's test of substantial connection and legitimate interest, rather than territory alone, is the more defensible middle path, because it ties the reach of a remedy to the forum's link with the harm.[704]

2.GLOBAL INTERNET GOVERNANCE VERSUS DOMESTIC SOVEREIGNTY

2.1 THE MULTISTAKEHOLDER MODEL AND STATE-CENTRIC MODELS

Internet governance grew up outside treaty structures. Names and numbers are coordinated by ICANN, a Californian non-profit that worked under a US government contract until the IANA stewardship transition of 1 October 2016 passed oversight to the global multistakeholder community.[705] According to the Tunis Agenda of 2005, internet governance means that governments, business and civil society, each acting 'in their respective roles', develop and apply common principles, norms and rules; the same document requested the UN Secretary-General to set up the Internet Governance Forum (IGF).[706] The IGF has no authority to issue binding decisions and functions as a forum for discussion. In December 2025 the UN General Assembly made the IGF permanent and reaffirmed the multistakeholder

[698] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006).
[699] *LICRA v Yahoo! Inc* (Tribunal de Grande Instance de Paris, 20 November 2000); *Yahoo! Inc v La Ligue Contre Le Racisme et L'Antisemitisme* 433 F 3d 1199 (9th Cir 2006).
[700] GDPR (n 13) art 3(2); Digital Personal Data Protection Act 2023, s 3(b).
[701] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (IT Rules 2021), r 4(1).
[702] Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.
[703] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Ltd* EU:C:2019:821.
[704] Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017).
[705] ICANN, 'Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends' (Press release, 1 October 2016).
[706] World Summit on the Information Society, 'Tunis Agenda for the Information Society' (18 November 2005) WSIS-05/TUNIS/DOC/6(Rev.1)-E, paras 34 and 72.

approach.[707] In a similar vein, the 2024 Global Digital Compact commits to a digital future that is open, free and secure, yet it sets up no new institution with binding powers.[708]

State-centric models reject equal rule-making with companies and civil society. China's Cybersecurity Law of 2017 asserted cyberspace sovereignty and, in Article 37, required critical information infrastructure operators to store personal information and important data inside China.[709] Two statutes passed in 2021, the Data Security Law and the Personal Information Protection Law, extended this foundation. Russia's 2014 amendments required citizens' personal data to be stored in Russia, and its 2019 'sovereign internet' law lets the regulator manage routing centrally and, in an emergency, cut Russia off from the global network.[710] At the UN, both states favour forums in which governments alone decide.

India's position is mixed: multistakeholder in international forums, but sovereigntist at home, as seen in the Reserve Bank of India's 2018 payment data localisation direction, the power under section 16 of the DPDP Act to restrict transfers, and Rule 13(4) of the DPDP Rules on localising specified data.[711] In Bradford's terms, India borrows from all three 'digital empires', the American market-driven, Chinese state-driven and European rights-driven models, without committing to any.[712]

2.2 CONFLICT OF LAWS AND EXTRATERRITORIAL REACH

Extraterritorial statutes are the main source of friction. The GDPR applies to controllers outside the EU who offer goods or services to, or monitor the behaviour of, people in the Union, and such controllers must usually appoint a representative there.[713] Because global firms find it cheaper to apply one standard everywhere, EU rules spread far beyond Europe, an effect Bradford named the 'Brussels Effect'.[714]

India's IT Rules 2021 do not claim to govern conduct abroad, but they impose duties with global consequences. Under Rule 4(2), a significant social media intermediary that offers messaging must be able to trace the 'first originator' of a message whenever a court or the government directs it to do so.[715] For an end-to-end encrypted service, compliance would mean redesigning the product worldwide, and WhatsApp's 2021 challenge in the Delhi High Court is still pending. Section 75 of the IT Act also reaches offences abroad that involve a computer system in India.

The result is overlapping and sometimes conflicting duties: a US company may be asked by India to remove speech protected at home, by the EU to delist it for privacy, and by its own government to share data only under the CLOUD Act.[716] No rule of international law decides which claim prevails.

[707] UNGA, Outcome document of the high-level meeting on the twenty-year review of the World Summit on the Information Society (adopted 17 December 2025).
[708] UNGA Res 79/1, 'The Pact for the Future' (22 September 2024) UN Doc A/RES/79/1, annex I (Global Digital Compact).
[709] Cybersecurity Law of the People's Republic of China 2016 (in force 1 June 2017), art 37.
[710] Federal Law No 242-FZ of 21 July 2014; Federal Law No 90-FZ of 1 May 2019 (Russian Federation).
[711] Reserve Bank of India, 'Storage of Payment System Data' (RBI/2017-18/153, 6 April 2018); Digital Personal Data Protection Act 2023, s 16; Digital Personal Data Protection Rules 2025, r 13(4).
[712] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).
[713] GDPR (n 13) arts 3(2) and 27.
[714] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020).
[715] IT Rules 2021 (n 33) r 4(2).
[716] Clarifying Lawful Overseas Use of Data Act, Pub L No 115-141, div V, 132 Stat 1213 (2018).

2.3 THE 'SPLINTERNET' AND ITS CONSEQUENCES FOR CONSTITUTIONAL RIGHTS

Taken together, these pressures are gradually dividing what was one global network into national and regional segments. The 'splinternet' includes technical fragmentation of routing and naming, governmental fragmentation through blocking, localisation and firewalls, and commercial fragmentation through walled gardens. For Mueller, the real danger is not technical collapse but the political choice to align the internet with national borders.[717]

Fragmentation has constitutional costs. Article 19(2) of the International Covenant on Civil and Political Rights guarantees the freedom to look for and receive information irrespective of borders, and fragmentation erodes that guarantee.[718] It also hands power to whoever controls national chokepoints, as India's record of more internet shutdowns than any other democracy shows,[719] and creates unequal citizenship online: Indian and European users of the same service hold different rights merely because of where they live.

2.4 INTERNATIONAL LAW AND SOFT LAW INSTRUMENTS

Binding international law on cyberspace is thin. India has not joined the Council of Europe's Budapest Convention of 2001, objecting partly to Article 32(b), which permits access to data stored in another party's territory with the consent of the person authorised to disclose it.[720] The UN Convention against Cybercrime, adopted on 24 December 2024 and opened for signature in Hanoi on 25 October 2025, was signed by India in September 2026, having been negotiated in a forum where India had an equal voice.[721]

As regards the behaviour of states, the UN Groups of Governmental Experts (GGE) reached a consensus in 2013 that existing international law, the UN Charter above all, governs conduct in cyberspace too. In 2015 they agreed eleven voluntary norms of responsible state behaviour, reaffirmed in 2021.[722] The non-binding but widely cited Tallinn Manual 2.0 sets out 154 rules on how international law applies to cyber operations, beginning with state sovereignty in cyberspace.[723]

None of this protects individuals against platforms: the GGE norms deal with states, the cybercrime treaties with crime and evidence, and the Tallinn Manual with sovereignty and conflict. Protection for users against corporate power is therefore left to national law and to non-binding standards, the UN Guiding Principles on Business and Human Rights being the main example.[724] That is why domestic constitutional law has had to stretch to fill the gap.

[717] Milton L Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity 2017).
[718] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19(2).
[719] Access Now, '#KeepItOn' annual reports on internet shutdowns (2018–2024).
[720] Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185, art 32(b).
[721] UNGA Res 79/243 (24 December 2024) UN Doc A/RES/79/243; 'India signs UN Convention against Cybercrime' *Onmanorama* (28 September 2026).
[722] UNGA, Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Docs A/68/98 (2013), A/70/174 (2015) and A/76/135 (2021).
[723] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) r 1.
[724] UNHRC, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (21 March 2011) UN Doc A/HRC/17/31.

2.5 Case Studies

Cross-Border Data Transfers: The Schrems Litigation

Max Schrems' complaints against Facebook Ireland produced two landmark rulings. In *Schrems I* the CJEU struck down the Safe Harbour decision because US law permitted generalised access to personal data by public authorities.[725] In *Schrems II* it struck down the Privacy Shield, holding that US surveillance under section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 was not limited to what was strictly necessary and that EU persons lacked an effective remedy as Article 47 of the Charter requires.[726] After the US created a new redress mechanism, the Commission adopted the EU-US Data Privacy Framework in July 2023, which the General Court upheld in *Latombe* in September 2025.[727] A court used fundamental rights to judge a foreign sovereign's surveillance law, and that sovereign changed its law: the clearest example of rights enforcement reaching across borders.

Platform Takedowns: X Corp v Union of India

India supplies the opposite example. During the 2021 farmers' protests the Ministry of Electronics and Information Technology (MeitY) issued blocking orders under section 69A of the IT Act against many accounts and posts. Twitter, now X, complied, partly under protest, and later challenged them. In June 2023 a single judge of the Karnataka High Court upheld the orders and imposed costs of ₹50 lakh for delayed compliance.[728]

The second round of litigation was about the Sahyog portal, a web platform that lets central ministries and police forces issue content removal notices to intermediaries, relying on section 79(3)(b) of the IT Act together with Rule 3(1)(d) of the IT Rules. X argued that it bypassed the safeguards of section 69A upheld in *Shreya Singhal*. On 24 September 2025 Justice M Nagaprasanna dismissed the petition, holding that Article 19 rights belong to citizens, not foreign corporations, calling the portal 'an instrument of public good' and refusing to transplant American free speech doctrine.[729] In October 2025 Rule 3(1)(d) was amended to require senior-rank officers and monthly Secretary-level review.[730] X appealed, and in mid-2026 the Supreme Court, on the Union's transfer petitions, stayed the High Court proceedings of X, DigiPub News, Kunal Kamra and others, so the portal's legality will likely be settled there.[731] Meanwhile, February 2026 amendments cut the time for complying with takedown orders to three hours and introduced labelling duties for synthetic content.[732]

Two points follow. Denying a foreign platform Article 19 does not dispose of the rights of Indian users whose speech is removed; they are rarely parties and seldom told why their content disappeared. The contrast with *Schrems* is also telling: in Europe a court used rights to restrain state surveillance, while

[725] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650.
[726] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* EU:C:2020:559.
[727] Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 [2023] OJ L231/118; Case T-553/23 *Latombe v Commission* (General Court, 3 September 2025).
[728] *X Corp v Union of India* WP No 13710 of 2022 (Karnataka HC, 30 June 2023).
[729] *X Corp v Union of India* WP No 7405 of 2025 (Karnataka HC, 24 September 2025).
[730] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, notified October 2025, in force 15 November 2025, amending r 3(1)(d).
[731] *Union of India v DigiPub News India Foundation* Transfer Petition (Civil) Nos 2071–2074 of 2026 (SC, order reported 7 August 2026).
[732] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, notified 10 February 2026, in force 20 February 2026.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Indian courts have so far used sovereignty to strengthen state control over platforms. Neither outcome is wrong in itself, but only the first gives the individual a direct remedy.

3. ALGORITHMIC TRANSPARENCY AND EXPLAINABILITY

3.1 THE 'BLACK BOX' PROBLEM

Pasquale's *The Black Box Society* described how the algorithms used in finance and search work in secret, even as the people subject to them become ever more visible to those who run them.[733] Burrell distinguishes three sources of opacity: secrecy that firms choose, the public's lack of technical knowledge, and the opacity inherent in machine-learning systems, whose inner workings do not follow the way humans reason.[734] Law can address the first through disclosure duties and the second through expert intermediaries such as auditors; the third is the hardest.

The problem appears in at least three fields. In credit scoring, a person may be refused a loan because of a score built from inputs they never see; Citron and Pasquale argued that such scores need due process protections.[735] Where content is moderated, it is usually automated classifiers that decide which posts remain visible, and the user is often told no more than a standard message. Predictive policing relies on old arrest data to predict the places where offences will occur or the persons likely to commit them, and in doing so it may carry forward whatever bias the original policing data contained.[736] In each field, people cannot challenge what they cannot see.

3.2 LEGAL FRAMEWORKS MANDATING EXPLAINABILITY

GDPR ARTICLE 22

Under Article 22(1) of the GDPR, a person is entitled not to be subjected to a decision reached purely by automated means, profiling included, where that decision has legal consequences for them or affects them in a comparably significant way. Where such decisions are allowed, Article 22(3) requires human intervention and the rights to be heard and to contest. Controllers must also, under Articles 13(2)(f), 14(2)(g) and 15(1)(h), give the data subject meaningful information on 'the logic involved'. Recital 71 mentions a right to an explanation, but recitals do not bind, and the point was long debated. Wachter, Mittelstadt and Floridi read the provisions as giving only general information about how a system works.[737] Selbst and Powles disagreed, contending that information is meaningful only if the data subject can make sense of it, which means it must extend to the particular decision.[738]

The CJEU has now largely adopted the wider reading. In *SCHUFA* it held that calculating a credit score is itself a 'decision' under Article 22 where a third party draws strongly on it.[739] In *Dun & Bradstreet Austria* it held that Article 15(1)(h) gives a genuine right to an intelligible explanation of the procedure and principles actually applied, which a complex formula does not satisfy.[740] Earlier, *Ligue des droits*

[733] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[734] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society 1.
[735] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1.
[736] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).
[737] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.
[738] Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 International Data Privacy Law 233.
[739] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* EU:C:2023:957.
[740] Case C-203/22 *Dun & Bradstreet Austria* (CJEU, 27 February 2025).

humains barred screening passenger data with self-learning systems whose criteria change without human control, as they defeat effective judicial review.[741]

3.3 THE EU AI ACT

The Artificial Intelligence Act takes a risk-based approach.[742] Article 5 bans practices such as social scoring and predicting criminality solely from profiling, and Annex III classes credit scoring and several law enforcement uses as high-risk. Article 13 obliges providers to build in enough transparency for deployers to understand what the system produces, and Article 14 obliges them to design it so that humans can oversee it. Certain deployers must assess fundamental rights impacts (Article 27), and Article 86 gives affected persons a right to 'clear and meaningful explanations' of the system's role in a decision. Though the Act was adopted in 2024, its timetable has since moved. That timetable was revised by the Digital Omnibus on AI, in force since July 2026, which pushed back the high-risk duties for Annex III systems until 2 December 2027.[743] The architecture is in place, but the start date has slipped.

3.4 INDIA'S DPDP ACT

The DPDP Act has no counterpart to Article 22. It gives a Data Principal a summary of the data and processing (section 11) and rights of correction and erasure (section 12), but no right to contest an automated decision or receive an explanation. The closest the Act comes is section 10, which empowers the government to notify certain entities as significant data fiduciaries and to require them to conduct data protection impact assessments and audits at regular intervals. Rule 13 of the DPDP Rules makes these annual and, in Rule 13(3), requires such fiduciaries to 'observe due diligence to verify that technical measures including algorithmic software' adopted by them 'are not likely to pose a risk to the rights of Data Principals'.[744] This first express reference to algorithmic risk in Indian data protection law is, however, a duty owed to the Board rather than a right of the individual, and audit findings are not public. MeitY's India AI Governance Guidelines, issued in November 2025, deliberately stopped short of proposing a dedicated AI statute and opted for voluntary principles instead, one of which is that systems should be 'understandable by design'.[745] Compared with the EU, and even China, whose Personal Information Protection Law lets individuals seek explanations and refuse solely automated decisions, India's protection is weak.[746]

3.5 ALGORITHMIC AUDITS: TYPES AND AUDITORS

An algorithmic audit is a structured examination of a system to test whether it behaves as claimed and complies with legal or ethical standards. Audits fall broadly into three categories, although the lines between them are often blurred.

[741] Case C-817/19 *Ligue des droits humains v Conseil des ministres* EU:C:2022:491.
[742] Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence [2024] OJ L1689 (AI Act).
[743] Regulation (EU) 2026/1744 amending Regulation (EU) 2024/1689 (Digital Omnibus on AI), in force 27 July 2026.
[744] Digital Personal Data Protection Rules 2025, r 13(1)–(3); Digital Personal Data Protection Act 2023, s 10(2)(c).
[745] Ministry of Electronics and Information Technology, *India AI Governance Guidelines* (5 November 2025).
[746] Personal Information Protection Law of the People's Republic of China 2021, art 24.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

A bias audit asks whether a system treats protected groups differently in its results. New York City's Local Law 144 of 2021, enforced since July 2023, requires employers that use automated employment decision tools to obtain an independent bias audit each year and to publish a summary of the results.[747]

Compliance audits check whether a system or organisation meets specific legal requirements. The DSA's Article 37 audit is the leading example. Each year, an independent body must audit every very large online platform and search engine and record, for each obligation, whether its opinion is 'positive', 'positive with comments' or 'negative'.[748]

Impact assessments are carried out before or during deployment to identify risks to rights. Examples include the GDPR's data protection impact assessment under Article 35, the DSA's systemic risk assessment under Article 34, the AI Act's fundamental rights impact assessment under Article 27 and the annual assessment for significant data fiduciaries under the DPDP Rules.

Who audits matters as much as the type of audit. *Internal* audits have full access but conflicts of interest, though Raji and her co-authors proposed an internal framework because external auditors arrive too late to change design choices.[749] *Third-party* audits bring independence, but the audited firm pays, as in financial auditing. *Regulatory* audits carry legal authority; the AI Act lets market surveillance authorities, on reasoned request, access a high-risk system's source code where other verification is insufficient.[750] A sound system needs all three: testing inside the firm, independent verification and a regulator with power to inspect.

3.6 THE RIGHT TO EXPLANATION VERSUS TRADE SECRET AND IP PROTECTION

Firms resist disclosure on the ground that their models are trade secrets or protected intellectual property. The EU Trade Secrets Directive protects information that has commercial value because it is secret.[751] Recital 63 of the GDPR says that the right of access should not adversely affect trade secrets or intellectual property, but adds that this should not result in a refusal to provide all information.

Dun & Bradstreet Austria gives the EU's answer: trade secrets cannot justify a blanket refusal. Allegedly protected information must be given to the supervisory authority or court, which weighs the competing rights and decides how much the data subject may receive,[752] a familiar form of closed review. American experience agrees: in *Houston Federation of Teachers*, teachers whose jobs depended on a secret value-added model were allowed to pursue a due process claim because they could not otherwise check their scores.[753] Wexler goes further, arguing that trade secret privilege should not apply at all in criminal proceedings where liberty is at stake.[754]

This study suggests a graded approach: disclosure should rise with the stakes. For low-impact systems such as product recommendations, general information on the main parameters is enough. For decisions on credit, employment, welfare or liberty, the person affected should receive a decision-

[747] New York City Local Law 144 of 2021, codified at NYC Administrative Code §§ 20-870 to 20-874.
[748] DSA (n 21) art 37; Commission Delegated Regulation (EU) 2024/436 on audits of very large online platforms and search engines.
[749] Inioluwa Deborah Raji and others, 'Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing' in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020) 33.
[750] AI Act (n 74) art 74(13).
[751] Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) [2016] OJ L157/1.
[752] *Dun & Bradstreet Austria* (n 72).
[753] *Houston Federation of Teachers, Local 2415 v Houston Independent School District* 251 F Supp 3d 1168 (SD Tex 2017).
[754] Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 Stanford Law Review 1343.

specific explanation of the factors that counted and what change would have altered the result, and the regulator or court should have confidential access to the model. Such an explanation need not reveal source code. Wachter, Mittelstadt and Russell demonstrate that a 'counterfactual' explanation can show an individual which facts would have needed to change to produce another result, while leaving the model itself closed.[755] The clash with trade secrets is therefore narrower than it first appears.

3.7 JUDICIAL AND REGULATORY ENFORCEMENT: THE CAPACITY QUESTION

Can courts and regulators actually audit algorithms? Courts can rule on such systems when the question is framed legally rather than technically. In 2020 the District Court of The Hague struck down SyRI, a welfare-fraud risk-scoring system, because the legislation gave no insight into the risk model, so its interference with private life under Article 8 of the European Convention on Human Rights could not be shown to be necessary and proportionate.[756] In *Bridges*, the Court of Appeal of England and Wales held police use of live facial recognition unlawful, partly because the force had not checked whether the software was biased by race or sex.[757] Neither court read the code; each required the state to know how its system worked and to justify it.

Regulators face a capacity gap. European data protection authorities report a shortage of technical staff, and the Commission had to build a specialised DSA team. In India the Data Protection Board is small and government-appointed, no agency is mandated to examine algorithms, judges rarely have technical training, and court-appointed technical experts are seldom used. Edwards and Veale warned that individual rights to explanation rarely work alone, since individuals lack the time and expertise to use them, and favoured collective and institutional mechanisms.[758] The lesson for India is plain: rights without auditors will stay on paper.

3.8 CASE STUDIES

COMPAS

COMPAS, developed by Northpointe (now Equivant), is used by American courts to predict reoffending. In 2016 ProPublica analysed the scores of more than 7,000 people arrested in Broward County, Florida, and found that Black defendants who did not reoffend were nearly twice as likely as white defendants to have been labelled higher risk.[759] Northpointe replied that the tool was equally accurate across races in a different statistical sense.[760] Both could be right: where base rates differ, the common definitions of fairness cannot all be met at once.[761] Dressel and Farid then found COMPAS no more accurate than people with no criminal justice expertise.[762]

[755] Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard Journal of Law & Technology 841.
[756] *NJCM v The State of the Netherlands* ECLI:NL:RBDHA:2020:1878 (District Court of The Hague, 5 February 2020).
[757] R *(Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
[758] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.
[759] Julia Angwin and others, 'Machine Bias' *ProPublica* (23 May 2016).
[760] William Dieterich, Christina Mendoza and Tim Brennan, 'COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity' (Northpointe Inc, 8 July 2016).
[761] Jon Kleinberg, Sendhil Mullainathan and Manish Raghavan, 'Inherent Trade-Offs in the Fair Determination of Risk Scores' in *Proceedings of the 8th Innovations in Theoretical Computer Science Conference* (2017); Alexandra Chouldechova, 'Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments' (2017) 5 Big Data 153.
[762] Julia Dressel and Hany Farid, 'The Accuracy, Fairness, and Limits of Predicting Recidivism' (2018) 4(1) Science Advances eaao5580.

In *State v Loomis* the Wisconsin Supreme Court allowed COMPAS scores at sentencing, but required written cautions that its methodology was a trade secret and had not been validated on a Wisconsin population, and held that the score could not be determinative.[763] The US Supreme Court declined review. *Loomis* is criticised for accepting a secret tool in a decision about liberty; its lesson here is that a warning label is a poor substitute for an audit.

FACEBOOK/META CONTENT MODERATION AUDITS

Facebook commissioned a civil rights audit in 2018, led by Laura Murphy, whose 2020 final report criticised its handling of hate speech, voter suppression and political speech.[764] Meta also commissioned human rights assessments, including a Business for Social Responsibility (BSR) review of the May 2021 conflict in Israel and Palestine, which found adverse effects on Palestinian users' freedom of expression through over-enforcement against Arabic content.[765] An India human rights impact assessment was commissioned too, but only a short summary was published in 2022, drawing civil society criticism.[766] These audits were voluntary, scoped by the company and published at its discretion, which shows the limits of self-regulation.

3.10. EU DSA TRANSPARENCY OBLIGATIONS

The DSA turns voluntary practice into law. Its obligations on the largest platforms include a systemic risk assessment (Article 34), a yearly independent audit (Article 37), disclosure of the key parameters behind recommender systems (Article 27), reasons to users whenever their content is moderated (Article 17), a public advertising repository (Article 39) and data access for vetted researchers (Article 40). Fines can reach 6 per cent of worldwide annual turnover under Article 74. On 5 December 2025 the Commission fined X €120 million for its deceptive paid blue checkmark, an inadequate advertising repository and denial of researcher access to public data, in breach of Articles 25, 39 and 40(12).[767] Every breach concerned transparency, which the DSA treats as a legal obligation, not a courtesy.

4.FINDINGS AND SUGGESTIONS

4.1 Findings

From the comparative study above, five findings emerge.

The constitutionalisation of cyberspace is uneven, and the decisive variable is who is bound by rights. The EU reaches private platforms through statute, India has begun to do so through the courts after *Kaushal Kishor Vs State of Uttar Pradesh*, and the US declines to do so at all. A user's protection therefore depends on geography rather than on the nature of the harm.

In India, platform litigation has been framed as a contest between the state and foreign companies. The *X Corp* rulings, the Sahyog portal and the three-hour takedown rule strengthen state control, while the users whose speech is removed have no right to notice or a hearing.

[763] *State v Loomis* 2016 WI 68, 371 Wis 2d 235, 881 NW 2d 749, cert denied 137 S Ct 2290 (2017).
[764] Laura W Murphy and Megan Cacace, *Facebook's Civil Rights Audit: Final Report* (8 July 2020).
[765] Business for Social Responsibility, *Human Rights Due Diligence of Meta's Impacts in Israel and Palestine in May 2021* (September 2022).
[766] Meta Platforms Inc, *Meta Human Rights Report: Insights and Actions 2020–2021* (July 2022).
[767] European Commission, 'Commission fines X €120 million under the Digital Services Act' (Press release, 5 December 2025).

International law covers relations between states but leaves a gap between individuals and platforms. Soft law and voluntary audits have not filled that gap.

A right to explanation can be no more effective than the bodies that exist to enforce it. The EU now has an enforceable right (*Dun & Bradstreet Austria*) and a working audit system (the DSA). India has a due diligence duty on algorithmic software in Rule 13(3), but no individual right and no published audits.

Trade secrets are not a serious barrier where confidential review by a court or regulator is available. The real barrier is technical capacity.

4.2 SUGGESTIONS

The following suggestions are offered for India:

(1) Amend the DPDP Act to give Data Principals a right not to be subject to solely automated decisions with legal or similarly significant effects, together with a right to a decision-specific explanation and to human review, drawing on Article 22 of the GDPR and Article 86 of the AI Act.

(2) Require significant data fiduciaries to publish a summary of the findings of their annual audits under Rule 13, with commercially sensitive material kept in a confidential annex for the Board.

(3) Create, through amendment of the IT Act or a future digital law, a statutory audit framework for high-impact algorithmic systems in welfare, policing, credit and employment, with accredited independent auditors and a power for the regulator to inspect models under confidentiality.

(4) Give users notice of takedown orders affecting their content and a right to seek review, and publish aggregate data on orders issued through the Sahyog portal and under section 69A.

(5) Make the Data Protection Board structurally independent of the executive, fund it to employ technical staff, and encourage courts to appoint technical experts in cases involving algorithmic systems.

(6) Abroad, continue to take part in multistakeholder forums and seek bilateral agreements on access to data, rather than relying only on unilateral extraterritorial rules.

5. CONCLUSION

Barlow imagined a cyberspace beyond the reach of law. What has emerged instead is a space crowded with competing laws: European rights, American free speech, Chinese and Russian sovereignty, and an Indian approach that borrows from each. Constitutionalising cyberspace, in this setting, does not mean exporting one country's constitution to the world. It means making sure that whoever holds power online, whether a ministry or a platform, is subject to the basic constitutional demands of legality, reasons, proportionality and a remedy.

Global governance bodies cannot deliver this alone; they were built for coordination, not rights protection. Domestic law can, but it runs into the limits of territory and invites fragmentation when it overreaches. The most promising tool is the least glamorous: the audit. A right to explanation tells a person what they are owed; an audit checks whether the system deserves trust. Europe's experience under the GDPR and the DSA shows that transparency can be made enforceable. India has taken a first

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

step in Rule 13(3) of the DPDP Rules; the next is to give individuals usable rights and to build institutions able to look inside the black box.