ANALYSIS OF DIGITAL INDIA ACT DRAFT- ISSUES AND CHALLENGES

Aarushi Aggarwal, LLM, School of Law, IILM University, Greater Noida, Uttar Pradesh

ABSTRACT

The introduction of the Digital India Act (DIA) draft signals a move to update India's aging cyber laws that currently fall under the Information Technology Act, 2000. Digital services, artificial intelligence, social media, and other technology driven services have seen explosive growth and a modern and comprehensive digital law is overdue. This paper engages with the draft Digital India Act critically with respect to its legal scope, structural changes, the reforms within the ambit of regulation vis-a -vis the constitution, global best practices, and the comprehensive digital goals of India.

The challenges in the draft include the nesting of ambiguity in streams of regulation, potential state overreach, risk to the right of free speech, lack of definitional clarity in data protection and user entitlements, and the lack of alignment with proposed data protection laws, varying regulations in different sectors, and the potential for the Act to lack coherence and enforceability. Through comparison with the EU's Digital Services Act and the U.S. approach to regulation, the draft emphasizes the importance of a balanced legal framework that protects innovation and civil rights. This paper ends with policy.

Keywords: Cyber legal framework, Regulatory framework, Constitutional rights, Legal scope.

INTRODUCTION

India's rapid digital economic growth has shown that there is a need for a legal outline that covers cyberspace, digital platforms, data governance, and emerging technologies. The Digital India Act (DIA) is an attempt to replace the out-of-date Information Technology Act of 2000 and is an attempt to provide an updated view to digital regulation that defends user rights and promotes technology. As digital interactions—especially e-commerce, AI, and social media—become more complex, the government's role of promoting innovation and taking care of security, accountability, and public trust, only gets more complex. The draft of the DIA seeks to meet these challenges through provisions on content moderation, misinformation, privacy, data protection, accountability of platforms, and transparency of algorithms, among others. The paper critically evaluates the draft DIA and identifies the legal, constitutional, and technological challenges it poses while providing recommendations for the creation of equity and the enabling of a digital governance system that looks towards the future.

BACKGROUND AND LEGAL CONTEXT

- **The Information Technology Act, 2000 and Its Limitations**

  The Information Technology Act of 2000 was a milestone piece of Indian legislation because it commercialized the country's first digital transactions, legalized electronic signatures, and addressed basic cyber offences. Its scope was gradually expanded through amendments to cover cybercrimes and the liabilities of intermediaries. Nonetheless, it is becoming increasingly difficult for this legislation to meet contemporary challenges in cyber law. Modern issues such as algorithmic injuries, abusive data collection, AI misuse, cyber harassment, false information and deepfake technology, and other AI-generated content largely escape this legislation's prohibitive reach. Additionally, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which assign content moderation responsibilities to digital platforms, have come under fire for the vague and disproportionate powers granted to intermediaries and authorities, particularly in relation to the unlawful limitations of free expression and the right to privacy.

- **Need for New Framework**

  Streamlined modernization of India's digital governance architecture could entail the

proposed Digital India Act. Other initiatives include the enactment of the Digital Personal Data Protection (DPDP) Act, 2023, which legislated rights regarding ownership of one's personal data. The DPDP Act also introduced the concept of data fiduciaries, with graded obligations linked to risk. Equally significant is the India AI Mission, which the Cabinet approved in 2024, aimed at scaling AI compute infrastructure (more than 10,000 GPUs) to support indigenous foundational models, enable responsible AI and strengthen access to high quality non personal datasets, and establish AI innovation centres. Within such parameters, the Government contends that the legal regime in force is outdated and inadequate, with the IT Act 2000 and its amendments providing insufficient means to address challenges of complex regulation, such as opaque algorithms, extensive data processing, AI-enabled content distribution, and provision of inadequate privacy in digital ecosystems. The proposed Digital India Act will address these issues by providing the necessary adaptive anticipatory regulation.

OBJECTIVES & KEY PROVISIONS OF THE DIGITAL INDIA ACT DRAFT

Based on policy consultations, Ministry of Electronics and Information Technology presentations, and stakeholder feedback, the main objectives and core features expected under the Digital India Act (DIA) include[1]:

1. Modernising the Legal Framework:

   The DIA seeks to supersede the Information Technology Act, 2000, commonly viewed as insufficient to address the level, velocity, and sophistication of Internet mediated harms and new technologies. Its architecture is meant to place India's digital law in accordance with present international standards and future requirements.

2. Open Internet Principles:

   Some central guiding principles are to ensure choice, competition, online diversity, equal market access, and simplifying business compliance particularly for new entrants. This also means stopping gatekeeping by leading platforms (for example, in ad tech or app stores), encouraging interoperability, and that new rules do not disproportionately

[1] https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf?

benefit big incumbents.

3. **Classification and Differential Obligations for Intermediaries:**

   Platforms of all types (e-commerce, AI platforms, OTT platforms, gaming platforms, search platforms, ad-tech platforms, social media intermediaries etc.) are likely to be categorized according to risk, size, and reach. Each category will have varying regulatory requirements.

4. **Review / Revision of Safe Harbour:**

   The safe harbour principle in Section 79 of the IT Act safeguarding intermediaries from liability for user generated content—is destined to be reconsidered. Either it will be made subject to compliance requirements (e.g. moderation, traceability) or its scope will be contracted or deleted for some categories of intermediaries.

5. **Regulation of Emerging Technologies & User Harm:**

   The DIA will likely implement "guardrails" for new technology (AI/ML, blockchain, IoT, etc.), putting user harm (addiction, privacy violation, misinformation, deepfakes) at the forefront of risk analysis. The law could compel platforms to conduct risk assessments, reveal algorithms, and be transparent[2].

6. **Accountability, Safety, & Trust for Users:**

   Provisions would seek to safeguard vulnerable stakeholders (children), govern content monetisation, subject content to grievance redressal mechanisms (in platform appeal or in-house appellate forums), enforce age gating, provide privacy of users, may mandate "do not track" for ad targeting, and ensure traceability if something goes wrong.

7. **Sector-Sensitive Regulation & Institutional Mechanisms:**

   The paper visualizes a standalone regulator or regulatory body for Internet/digital services, or analogous institutional arrangements, which can resolve disputes, enforce

[2]https://www.khaitanco.com/sites/default/files/202303/The%20Digital%20India%20Act%20Overhauling%20India%E2%80%99s%20Technology%20Laws.pdf?

commitments, and enforce compliance. Lighter touch of regulation for lower risk platforms is also addressed to ensure that regulation does not dampen innovation.

CRITICAL ISSUES AND CHALLENGES

The main challenges faced under the Digital India Act (DIA) include:

1. **Free Speech and Censorship Concerns:**

   One of the principal controversies of the draft DIA is that it adds further burden to platforms to police user content, potentially undermining the safe harbour immunity under Section 79 of the IT Act.

   Risk: Platforms may over censor or delete legal content pre emptively so as to prevent liability, and have a chilling effect on free expression.

   Problem: Important terms like "harmful," "misleading," or "unlawful" are not explicitly defined, leaving room for uneven or biased enforcement.

   Relevant Case: The Supreme Court in Shreya Singhal v. Union of India (2015) struck down Section 66A of the IT Act on the grounds that the ambiguous language was in violation of Article 19(1)(a) (freedom of speech). The court also interpreted Section 79 to mean that intermediaries are only liable when they are given a court order or a notice from the concerned authority on removal of content, thus maintaining stronger safeguards for online speech[3].

2. **Privacy and Surveillance Risks:**

   The preliminary DIA can impose trace origin requirements and demand businesses surrender decryption keys.

   Problem: Such requirements weaken end to end encryption (E2EE), which is the heart of user privacy and secure communication.

   Inconsistency: Although the DPDP Act, 2023 focuses on user privacy rights,

[3] https://indiankanoon.org/doc/110813550/

traceability requirements in other legislations can be at odds with those assurances. (E2EE would be weakened if all messages are traceable)[4].

Risk of Abuse: In the absence of effective oversight or precise limitations, sweeping surveillance authorities set off alarms of abuse in terms of bulk monitoring or targeting of dissent particularly when metadata or message source information are retained.

3. **Intermediary Liability and Compliance Burden:**

The DIA seems to recast who is an "intermediary" and quite heavily buries them in requirements they have to meet.

Problem: Mandates like hiring grievance officers, deleting content within strict timeframes (e.g., 24 hours), algorithmic audits, and traceability compliance require significant legal, technical, and infrastructural investment—vital resources which may be possessed by large platforms but are likely not available to startups and SMEs.

Impact: Those duties may add expense and operational sophistication for small players, potentially discouraging innovation, rewarding incumbents, and widening digital inequality.

4. **Institutional Challenges and Regulatory Overlaps:**

The whitepaper suggests setting up a Digital India Authority (or an entity with equivalent powers) to undertake most of the DIA's regulatory role.

Challenge: There already exist very powerful bodies like TRAI (Telecom Regulatory Authority of India), CCI (Competition Commission of India), and the Data Protection Board whose mandates could overlap with what the new authority could potentially be tasked with[5].

Risk: Such overlap would risk jurisdictional uncertainty, ineffectual enforcement, or even conflict of regulation. The process of appeals or redress may be ambiguous, and

[4] https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-traceability-and-endtoend-encryption-coexist-heres-the-legal-view/67001/1?
[5] https://www.livelaw.in/high-court/kerala-high-court/kerala-high-court-trai-cci-overlap-jurisdiction-oust-294129?

there is a risk of overconcentration of regulatory authority without adequate restraints.

EMERGING TECHNOLOGIES: REGULATION VS INNOVATION

i. AI and Algorithmic Governance

The Digital India Act introduces regulation of AI systems and algorithms particularly when employed for automated decision making, personalization, or content recommendation. Positively, transparency requirements, bias audits, and greater control for users over algorithmic processes are welcome as they can minimize harm, enhance trustworthiness, and encourage fairness. That said, there are real challenges: India does not yet have strong technical standards, certified auditors, or judicial precedent for judging proprietary AI systems; the lack makes it harder to regulate algorithmic bias or error. There is also the risk that excessive regulation will disproportionately bear down on startups and smaller firms, stifling innovation and slowing the pace of development of new AI driven services. Experts and legal analysts have referred to the danger that regulatory uncertainty or rigid compliance requirements can benefit large incumbents who have the budget for audits and lawyering, further expanding the innovation gap.

ii. Digital Addiction and Youth Safety

The DIA's proposal has provisions to safeguard children from the addictive potential of digital technologies—like content or interface designs that promote long-term use, endless scrolling, nudges, etc. The purpose is noble: to ensure age-appropriate content environments, limit manipulative design techniques, and ensure that platforms have measures to protect children online. Implementation, however, raises some challenges. Age verification that is trusted is a challenging technical and legal issue; government IDs are not available to many minors, family shared devices make device level controls tricky, and authenticating parental permission poses privacy risks and abuse of personal information. Design decisions such as age gating or identity checks on demand, unless narrowly targeted, also risk imposing disproportionate harm on vulnerable groups, limiting access, or causing surveillance across families. Experts also warn that safeguards need to be struck in a balance so they do not ostracize or stigmatize children,

or unduly limit their rights to access useful resources online[6].

COMPARATIVE INTERNATIONAL PERSPECTIVE

Country Name	Key Legislation / Regime	Main Features & Lessons for India
European Union	Digital Services Act (DSA)	Tiered obligations, algorithm transparency, notice-and-action, independent regulators. The EU's DSA puts tiered obligations on digital platforms, with more onerous compliance obligations for those with major reach ("Very Large Online Platforms / Search Engines"). It requires greater transparency regarding algorithms, particularly content recommendation engines, enables users to appeal moderation actions, and imposes stronger requirements on prohibited or harmful content (disinformation, hate speech, etc.)[7].
United States of America	Section 230 of the Communications Decency Act (CDA)	Section 230 gives comprehensive legal immunity to platforms regarding user-generated content, shielding them from being treated as publishers of that content. It further enables platforms to moderate content without being held responsible for their moderation decisions, provided they do it in "good faith." Yet, it is increasingly coming under fire for perceived shortcomings in accountability[8].
Australia	Online Safety Act 2021	This legislation broadens the remit of Australia's e-Safety Commissioner to cover online harms targeting children and adults. It features schemes for taking down "seriously abusive content," enhances measures for safeguarding against cyberbullying and image-based abuse, and compelling platforms to meet "basic online safety expectations." It also brings mandatory industry codes for

[6] https://techbharat.in/age-verification-for-social-media-impact-on-users-and-the-debate-among-parents-and-children/23241/?

[7] https://commission.europa.eu/news-and-media/news/digital-services-act-keeping-us-safe-online-2025-09-22_en?

[8] https://www.acm.org/public-policy/ustpc/hottopics/section-230?utm

		content moderation and new standards for handling illegal content[9].
China	Cybersecurity Law; Data Security Law; Personal Information Protection Law (PIPL)	China's regulatory environment is characterized by robust state control over data flows, wide-ranging defined national security interests, and domestic data storage requirements. Personal information processing in PIPL is strictly governed, including cross-border transfers, with severe penalties for non-adherence and provisions for consent, sensitivity classification, and overseas representative offices for foreign entities[10].
Canada	Bill C-63 / Proposed Online Harms Legislation	Introduce in 2024, this bill would mandate platforms to act against all "online harms" such as hate speech, sexual exploitation of children, violent inciting content, self-harm, etc. It also had provisions for age-appropriate design, and establishment of a federal regulatory agency to oversee enforcement. Despite the bill lapsing with dissolution of Parliament, it mirrors Canada's shift towards holding platforms accountable[11].
Japan	Act on Improving Transparency and Fairness of Specified Digital Platforms + Information Distribution Platform Regulation Act	According to the Japanese law, platforms that satisfy some size or effect requirements are categorized as "specified digital platform providers." The platforms are required to make and explain their content moderation policies, disclose terms of service, openness of algorithms to some extent (ranking, takedown decisions), implement takedown procedures, and disclose information to the Minister of Internal Affairs and Communications[12].
Brazil	Law No. 15.211/2025 (“ECA Digital” / New Law for the Protection of Minors in Digital Environments)	This legislation compels online platforms to have effective age verification systems in place and limit access to age-inappropriate content. Platforms with significant numbers of underage users have to report content moderation statistics, suspension of accounts,

[9] https://www.esafety.gov.au/newsroom/whats-on/online-safety-act?utm
[10] https://www.gtlaw.com/en/insights/2021/9/china-promulgates-personal-information-protection-law?
[11] https://digitalpolicyalert.org/event/29509-ministry-of-internal-affairs-and-communications-issued-order-designating-platforms-as-large-specified-telecommunications-service-providers-under-information-distribution-platform-regulation-act?
[12] https://www.canada.ca/en/canadian-heritage/services/online-harms.html?

	Bill PL 2768/2022 – Bill Regulating Digital Platforms / Digital Markets Bill	and steps taken to safeguard children. The legislation calls for such measures to be technologically secure, proportionate, and auditable[13]. This bill would treat certain platforms with significant yearly revenue (threshold in local currency) as "essential access control power holders," subject to transparency/reporting requirements, limits on discriminatory treatment against smaller competitors, and regulatory scrutiny. Fines and inspection fees are included in the proposal[14].

Takeaways for India:

- India can use clearly defined legal terms and inbuilt safeguards to prevent ambiguities and misuses, just as the EU has done under the Digital Services Act.

- Regulation should be left with autonomous regulatory or supervisory agencies, independent of political or platform direct control, to maintain a fair enforcement[15].

- Preservation of the rights of citizens in the cyber space must involve strong due process safeguards, such as adequate notice, ability to respond, mechanisms to appeal, and open decision-making. India should adopt **well-defined legal terms and built-in safeguards** to avoid ambiguity and prevent misuse, similar to what the EU has done under the Digital Services Act[16].

RECOMMENDATIONS

1. **Ensuring Legal Clarity and Precision:**

   India's regulatory scheme should have well-drafted wording to prevent overbroad or ambiguous provisions. Phrases like "harmful content," "misleading information," or "unlawful behaviour" should be clearly defined either in the statute or through delegated legislation with strict standards. This will serve to disapprove arbitrary

[13] https://digitalpolicyalert.org/event/29509-ministry-of-internal-affairs-and-communications-issued-order-designating-platforms-as-large-specified-telecommunications-service-providers-under-information-distribution-platform-regulation-act?
[14] https://itif.org/publications/2025/03/07/brazil-single-firm-conduct-regulation/?
[15] https://www.thegovernors.eu/eu-ai-act-key-takeaways/?
[16] https://digitalservicesact.eu/wp-content/uploads/2020/06/DSA-Policy-Brief-Content-Moderation.pdf?

choices or abuse of regulatory authority. Robust procedural protections must be established so that content removals are not performed without adequate notice, cause, or opportunity for the reply.

2. **Protecting Encryption and Privacy:**

Any law mandating traceability of communication or decryption keys must be subject to judicial review or similar autonomous authority, to protect against abuse or surveillance misuse. Digital privacy regulations and legislation—like India's DPDP Act, 2023—need to be harmonized so new legislation does not contradict existing rights and expectations. Harmonization is necessary for user trust to be maintained and in order to ensure privacy safeguards are not inadvertently undermined[17].

3. **Proportionate Regulation for Startups:**

The regulatory requirements need to be balanced to the size, extent, and risk profile of players—platforms or intermediaries. Small and medium enterprises (SMEs) and start-ups should have lower compliance requirements, e.g., lesser reporting or easy audit requirement, so that they are not being overly stifled in their innovative spirits. And also, sandbox mechanisms—temporary, regulated relief or trial beds—can facilitate innovators to pilot novel models, technologies, and products under oversight without being entirely subject to the most stringent obligations right from the beginning. Indications of the DPDP draft rules reveal that startup organizations are already seeking "tiered compliance obligations[18].

4. **Strengthening Institutional Mechanisms:**

Strong oversight relies on creating institutions that are autonomous, well funded, and transparent. An ad hoc executive department should not enforce new digital rules, audit, or settle disputes; this should be done by a digital regulator. The process of selecting its leadership should be transparent, merit based, and protected from politics. Moreover, strong grievance redressal mechanisms—both platform-based and external oversight—

[17] https://recordoflaw.in/technology-law-data-protection-in-india-after-the-digital-personal-data-protection-act-2023-a-critical-analysis/?
[18] https://www.fortuneindia.com/enterprise/draft-dpdp-rules-tech-body-seeks-clarity-on-ai-ethics-compliance/119976?

need to be instituted so that the rights of people are protected in a timely manner. The DPDP Act's creation of the Data Protection Board, while the welcome move that it is, has been queried for having an ambiguity regarding autonomy and procedures.

5. **Promoting Digital Literacy and Civil Society Engagement:**

Regulation alone is not enough without an educated public capable of comprehending and asserting their online rights. The government must invest in awareness programs among users—rural or marginalized communities in the first instance—on rights, responsibilities, and remedy in the online space. Civil society, the academy, and technical specialists need to be engaged proactively in the formulation of not only legislation, but also rules, standards, and guidelines for implementation. Increased stakeholder participation guarantees that regulation is feasible, culturally appropriate, and less likely to neglect actual world circumstances and limitations. A number of discussions regarding the DPDP Act and draft rules highlight that in the absence of literacy and awareness, legal entitlements can remain out of reach[19].

CONCLUSION

The Draft Digital India Act (DIA) promises to redefine India's digital governance in an era of AI, disinformation, and platform power. But unless carefully calibrated, it also threatens to erode constitutional safeguards and snuff out innovation. The ambitions of the law to police harms such as deepfakes, platform misuse, and algorithmic discrimination are commendable, but they cannot be at the cost of freedom of speech, privacy, and due process.

To have a strong and reliable digital future, India can follow a rights respecting path: the DIA needs to use clear definitions and legal protections, avoid arbitrary content removals, and subject any surveillance or traceability requirements to judicial review. It needs to provide proportionate burdens, with less onerous requirements for startups and sandboxing for new technologies. Having an independent regulator with open appointments and grievance redressal is essential. Also critical is maintaining stakeholder engagement and online literacy so that regulation is both responsive and inclusive.

[19] https://lawfullegal.in/decoding-the-right-to-privacy-in-the-digital-age-a-critical-analysis-of-data-protection-laws-in-india-under-the-dpdp-act-2023/?

By rooting the DIA in the values of the Constitution, aligning it with the DPDP Act, and borrowing lessons from international best practices, India can foster a digital environment that is as conducive to innovation as it is protective of rights. By doing so, the DIA can be rewritten as a bedrock of digital trust, accountability, and democratic legitimacy.

REFERRENCES

I. Surana & Surana, Decoding Digital India Act: A Critical Analysis (2023)

II. Law Curb, India's Digital India Act Explained (2023)

III. Drishti IAS Editorial, India's Digital Future – The Digital India Act (2023)

IV. NASSCOM, Discussion Paper on Scaling Digital Governance (2023)

V. Monday, Digital India Act: Looking Through the Crystal Ball (2023)

VI. MeitY Presentations and DIA Draft Consultations

VII. Supreme Court judgments: Shreya Singhal v. Union of India,

Puttaswamy v. Union of India