INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

PROTECTING USERS IN THE DIGITAL AGE: COMPARATIVE LEGAL APPROACHES TO PLATFORM ACCOUNTABILITY, CHILD SAFETY, AND TIKTOK

AUTHORED BY - PAYAL RONAK CHOKSI
Student/Researcher, Kuala Lumpur, Federal Territory, Malaysia

ABSTRACT

The regulation of digital platforms has become one of the defining challenges of modern law, raising pressing questions about constitutionalism, sovereignty, and the protection of fundamental rights in the digital domain. At the centre of this debate lies the problem of accountability: how should states ensure that powerful platforms safeguard users, particularly children, without undermining democratic freedoms or innovation? This paper addresses that question through a comparative analysis of three distinct legal approaches: the European Union's rights-based framework under the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), the United Kingdom's regulator-driven model under the Online Safety Act, and India's interventionist strategy culminating in the prohibition of TikTok.

The study adopts a doctrinal and comparative legal methodology. Key instruments including the GDPR, the DSA, the United Kingdom's Online Safety Act, and India's Information Technology Act (IT Act) and Intermediary Guidelines and Digital Media Ethics Code Rules 2021 (IT Rules 2021), are examined through the frameworks of digital constitutionalism, proportionality, and the United Nations Convention on the Rights of the Child (UNCRC). The TikTok ban in India is treated as a case study to illuminate the constitutional and policy implications of sovereignty-driven restrictions.

The findings reveal divergent trajectories. The European Union foregrounds proportionality and rights-preserving accountability, the United Kingdom relies on regulator-led safety enforcement, while India privileges sovereignty and security at the cost of user freedoms. India's prohibition redistributed risks rather than resolving them, whereas the European and British approaches demonstrate the potential of structured accountability mechanisms. Across jurisdictions, tensions persist between political authority, commercial interests, and user rights.

ISSN: 2582-6433

This paper contributes to legal scholarship by situating platform regulation within broader debates on constitutionalism and the rule of law in digital governance. It advances a normative framework for accountability that integrates proportionality analysis, algorithmic transparency, and privacy-preserving child-safety safeguards. In doing so, it offers both theoretical insights for comparative constitutional law and practical lessons for policymakers navigating the global digital ecosystem.

Keywords: *digital privacy; platform regulation; TikTok ban; Digital Services Act; Online Safety Act; Information Technology Rules (India); comparative legal analysis; children & social media; national security; content moderation.*

INTRODUCTION

TikTok has become a focal point for one of the hardest questions in platform governance: how can law hold very large platforms accountable to users, especially children, without sacrificing constitutional guarantees and the openness of the digital economy. India's decision on 29 June 2020 to block fifty-nine mobile applications, including TikTok, under Section 69A of the IT Act and the 2009 Blocking Rules, was justified on grounds of sovereignty and security. The ban instantly removed a service that had an estimated user base of 200 million in India, generating both domestic and global debate (Press Information Bureau, 2020; TIME, 2025). For the purposes of this paper, platform accountability refers to the legal, institutional, and technical mechanisms by which digital platforms are required to anticipate, prevent, and remediate harms arising from their operation. It is not limited to ex post liability but extends to ex ante duties of risk assessment, algorithmic transparency, and responsive compliance with statutory obligations such as those under the EU's DSA and the UK's Online Safety Act 2023 (European Commission, 2022; UK Government/Ofcom, 2023). Platform accountability, in this sense, reflects a shift from self-regulation and corporate codes of conduct toward enforceable, rights-based obligations subject to external oversight (Suzor, 2018; De Gregorio, 2022).

Similarly, child safety, as employed in this study, refers to the protection of individuals under the age of eighteen (as defined by the UNCRC) from content, data practices, and platform designs that risk undermining their privacy, dignity, or development in the digital environment (UNCRC Committee, 2021). It encompasses both direct harms, such as exposure to sexual or violent content, and indirect harms, such as manipulative algorithmic targeting or unlawful data processing, as illustrated by the €379 million fine imposed on TikTok for default settings that

ISSN: 2582-6433

exposed minors' personal data (Data Protection Commission, 2023). Child safety here therefore means the affirmative duty of platforms and regulators to ensure privacy-preserving age assurance, proportionate content moderation, and design safeguards that align with children's best interests.

In contrast, the European Union has developed a rights-based model of platform governance. The GDPR and the DSA establish systemic duties of transparency, risk assessment, and algorithmic accountability for significantly large intermediaries, defined as those reaching more than forty-five million users in the Union (European Commission, 2022; European Commission, 2023). This approach situates regulation within a constitutional framework of proportionality and fundamental rights. The United Kingdom has also avoided prohibition, instead enacting the Online Safety Act in 2023. The Act empowers Ofcom to impose risk assessments, design standards, and age-appropriate safeguards with a strong emphasis on child protection (Government of the United Kingdom, 2025; Ofcom, 2025). However, despite these obligations, recent data from the Children's Commissioner for England reveal that children's exposure to harmful content remains widespread, showing that enforcement and outcomes are as important as formal rules (The Guardian, 2025).

TikTok has tested these regulatory regimes. In 2023, following a binding decision of the "European Data Protection Board, the Irish Data Protection Commission fined TikTok €379 million for infringements involving the processing of children's data and ordered extensive design changes (European Data Protection Board, 2023; Data Protection Commission, 2023)". This demonstrates a model of accountability that modifies platform practices rather than expelling services from the market.

This paper advances two claims. First, ban-first approaches tend to displace rather than reduce risks, as evidenced by India's post-2020 migration of users to domestic substitutes with weaker safeguards (Reuters, 2025; TIME, 2025). Second, structured accountability that integrates proportionality analysis, algorithmic transparency, and privacy-preserving safeguards is better suited to align child safety with rights protection. Doctrinally, the paper compares the European Union, the United Kingdom, and India across scope, duties, enforcement, and remedies. Normatively, it proposes a framework that legislatures and regulators can operationalise without undermining constitutional protections.

ISSN: 2582-6433

LITERATURE REVIEW

Research on platform governance has increasingly focused on digital constitutionalism, a framework that regards platforms not merely as private intermediaries but as entities exercising quasi-public power that must adhere to constitutional standards of accountability and rights protection (Suzor, 2018; Celeste, 2018). De Gregorio (2022) demonstrates how the European Union (EU) has integrated this vision into its legal framework through the implementation of the GDPR (EUR-Lex, 2016) and the DSA (European Commission, 2022), thereby promoting a rights-based regulatory model. The DSA's focus on systemic risk assessments and transparency for very large online platforms (VLOPs) shows proportionality analysis, which makes sure that actions taken are in line with the risks found.

The notion of proportionality is a fundamental tenet in comparative constitutional law. Its use in digital governance shows that platform control shouldn't automatically lead to too many restrictions. Instead, it should find a balance between protecting children and allowing free speech and data privacy (Brookings Institution, 2023). India's ban-first strategy, which included banning TikTok and fifty-eight additional apps in 2020 (Press Information Bureau, 2020), is an example of a different path. Kumar (2023) contends that the prohibition transferred risks to alternative platforms instead of mitigating them, while other scholars emphasize how such measures expose the inadequacies of sovereignty-driven approaches (Atlantic Council, 2021).

The UK Government's Online Safety Act 2023 and Ofcom's regulatory advice (UK Government/Ofcom, 2023) move toward an enforcement paradigm led by regulators. It requires responsibilities of care, risk assessments, and child protection protocols. This is in line with the UN Committee on the Rights of the Child's General Comment No. 25 (2021), which expanded the UNCRC to include digital spaces. But in reality, exposure to hazardous content is still high, which shows that strong regulations must be backed up by strong enforcement (The Guardian, 2025).

Child safety in digital environments is a frequent subject in empirical study. Critics say that TikTok's design puts kids at risk of seeing damaging mental health content (Amnesty International, 2021) and that it collects biometric data without enough protections (TechGDPR, 2021). The EU has fined TikTok €379 million for not protecting minors' data, which is a huge amount of money (TechCrunch, 2023). At the same time, Indian parents have called for

ISSN: 2582-6433

stronger protections for kids online, pointing out flaws in the IT Rules 2021 (MeitY, 2021). Research indicates that the TikTok ban in India had minimal impact on diminishing adolescent susceptibility to dangerous content, as alternative platforms such as Moj and Chingari rapidly occupied the void (Taddi, 2024).

This body of literature proposes three normative foundations for comparative analysis: digital constitutionalism, which subjects platforms to constitutional principles; proportionality, which necessitates measured regulatory actions; and children's rights, which contextualize platform accountability as a concern of both privacy and developmental welfare. This study contextualizes the TikTok issue within extensive discussions on constitutionalism, sovereignty, and the global administration of digital platforms by examining the methods of the EU, UK, and India.

Comparative Legal Framework

Legal regimes governing platforms in the EU, the UK, and India reflect distinct constitutional traditions and regulatory logics. While the EU embeds digital governance within the language of fundamental rights and proportionality, the UK privileges enforceable safety duties, and India prioritises sovereignty and security.

The European Union

The General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, remains the cornerstone of EU digital governance. Article 5 codifies “principles of lawfulness, fairness and transparency, and Article 25 imposes data protection by design and by default”. These obligations are particularly salient for platforms like TikTok, whose algorithmic profiling of children has raised repeated concerns (European Data Protection Board, 2023).

The DSA, Regulation (EU) 2022/2065, builds on this foundation. Article 34 mandates systemic risk assessments for Very Large Online Platforms (VLOPs), while Article 37 requires independent annual audits. Article 45 empowers “the European Commission to impose fines of up to 6 percent of annual global turnover for violations”. The DSA’s recitals emphasise protecting minors, declaring that VLOPs must “take appropriate and proportionate measures to protect children, including with regard to their mental health.” Enforcement is coordinated between national Digital Services Coordinators and the Commission, embodying the EU’s “constitutional pluralism.”

ISSN: 2582-6433

The United Kingdom

The UK's Online Safety Act 2023 represents a post-Brexit recalibration. Section 11 introduces a duty of care requiring providers to prevent children's access to harmful or pornographic content. Section 68 empowers Ofcom to issue codes of practice covering risk assessment, age-assurance, and reporting systems. Section 116 authorises fines of up to ten percent of annual worldwide revenue for breaches. The Act goes further than the EU by codifying specific child-safety duties: Ofcom guidance requires platforms to demonstrate "highly effective" age-verification, a term directly quoted in the regulator's 2025 statement. Unlike the EU's proportionality-anchored framework, the UK model operationalises enforcement through regulator discretion and measurable compliance, echoing a risk-management ethos rather than constitutional balancing.

India

India has pursued an interventionist path grounded in sovereignty. Section 69A of the IT Act authorises the government to block public access to information "in the interest of sovereignty and integrity of India, defence of India, security of the State or public order." It was under this provision, read with the 2009 Blocking Rules, that the government on 29 June 2020 banned fifty-nine apps, including TikTok (Press Information Bureau, 2020).

The IT Rules 2021 impose additional obligations. Rule 4(2) requires traceability of the "first originator of information," raising privacy and encryption concerns. Rule 3(1)(b) obliges intermediaries to take down within 36 hours any content deemed unlawful by government order. Critics argue that these rules, together with the TikTok ban, represent a ban-and-interventionist model rather than a rights-preserving framework (Kumar, 2023; Brookings Institution, 2023). Empirical studies suggest that the ban displaced users toward domestic substitutes such as Moj and Chingari but did little to mitigate harms (Taddi, 2024).

Table 1. Regulatory Frameworks Governing Platform Accountability: EU, UK, and India

Jurisdiction	Core Instruments	Key Duties	Enforcement Body	Sanctions	Child Safety Provisions
EU	GDPR (2016/679); DSA	Art. 25 GDPR (privacy by	National DSCs + European	Fines up to 6% of global turnover	Recital 71 DSA: "appropriate

ISSN: 2582-6433

	(2022/2065)	design); Art. 34 DSA (systemic risk assessment); Art. 37 DSA (audits)	Commission		and proportionate measures to protect children"
UK	Online Safety Act 2023	Sec. 11 (duty of care); Sec. 68 (codes of practice)	Ofcom	Fines up to 10% of global revenue	Ofcom guidance: "highly effective" age verification
India	IT Act 2000, Sec. 69A; IT Rules 2021	Rule 4(2) (traceability); Rule 3(1)(b) (takedown within 36 hrs)	Ministry of Electronics & IT	Blocking orders; criminal liability for non-compliance	No direct child-safety design duties; reliance on bans and parental pressure

The EU's framework reflects digital constitutionalism, embedding proportionality into platform obligations. The UK focuses on enforceability and regulator discretion, prioritising demonstrable compliance. India privileges sovereignty and market exit, deploying bans and sweeping intermediary obligations. Each reflects its own constitutional DNA; rights in the EU, regulation in the UK, sovereignty in India; yet their comparative lesson is that effectiveness depends not on the strictness of rules alone but on their proportionality, legitimacy, and enforceability.

METHODOLOGY

This research utilizes a doctrinal and comparative legal technique. The doctrinal approach is essential as the research focuses on the analysis of binding primary instruments, including the General Data Protection Regulation (Regulation (EU) 2016/679), the Digital Services Act

ISSN: 2582-6433

(Regulation (EU) 2022/2065), the Online Safety Act 2023 in the United Kingdom, and India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 in conjunction with Section 69A of the Information Technology Act 2000. These texts are analyzed in conjunction with official directives, including Ofcom's statutory codes and the European Commission's enforcement messages, to elucidate the extent of duties, rights, and enforcement methods. The comparative aspect is executed via the functional methodology of comparative law, which evaluates the responses of various legal systems to a common social issue: platform accountability and child protection. This technique is appropriate because, despite the differing constitutional contexts of the EU, UK, and India, they have the same difficulty of addressing the vulnerabilities associated with substantial platforms like TikTok.

The research employs a case study methodology, considering India's 2020 TikTok ban as a significant example of sovereignty-driven action. This instance is examined in relation to the outcomes noted in Europe and the UK, facilitating an evaluation of whether market exit tactics mitigate risk or merely relocate it. Secondary sources, such as peer-reviewed academia, policy think-tank publications, and empirical studies on children's online behaviors, are utilized to contextualize theological findings. Triangulating various sources such as legal text, regulatory practice, and social impact studies, ensures validity. This hybrid doctrinal-empirical orientation establishes the paper's normative framework in both legal principles and empirical results.

Case Study – India & TikTok ban

The Indian government said in a press statement on June 29, 2020, that fifty-nine mobile apps, including TikTok, will be banned under Section 69A of the Information Technology Act 2000 and the 2009 Blocking Rules. The ruling said that the apps on the list were "harmful to India's sovereignty and integrity, India's defense, state security, and public order" (Press Information Bureau, 2020). TikTok had almost 200 million active users in India at the time, making it the company's biggest foreign market and putting millions of creators and small companies at risk of rapid disruption (Kumar, 2023).

The restriction came at a time when geopolitical tensions were rising after Indian and Chinese troops clashed along the border in Ladakh. There were national security worries over cross-border data transfers, and some people said that TikTok's data collection methods could let foreign governments spy on people (Brookings Institution, 2023). The use of Section 69A shows the sovereignty-based approach: the law gives the central government the power to block access to information "in the interest of sovereignty and integrity of India, defence of India,

ISSN: 2582-6433

security of the State or public order" without requiring a review of proportionality or prior judicial oversight (Information Technology Act, 2000, s.69A).

The immediate effects on the market were huge. Moj, Josh, and Chingari rapidly took over the space that was left by the lack of competition. Moj alone said it had 80 million monthly active users within months after the prohibition, and users spent more than 30 minutes a day on average (Taddi, 2024). Instagram Reels also took a lot of TikTok's old creators (Kumar, 2023). However, studies show that these platforms had less strict rules for moderation and safety, which makes people wonder if the prohibition really made kids safer (Brookings Institution, 2023).

Empirical analysis indicates that the prohibition shifted hazards rather than mitigated them. Brookings analysts determined that “banning apps does not eliminate harms; it merely redirects them to alternative services” (Brookings Institution, 2023, p. 7). Research on adolescents' digital participation indicates that detrimental exposure continued, with numerous individuals transitioning effortlessly to new applications (Taddi, 2024). Indian parents' demands for more protections, especially for children's data privacy, show even more how ineffective ban-first laws are (Amnesty International, 2021).

The IT Rules 2021 added new compliance duties. For example, Rule 4(2) says that the first person to get information must be able to be traced, and Rule 3(1)(b) says that illegal content must be taken down within 36 hours (MeitY, 2021). Critics say that these steps give the president more power without putting in place protections of need or proportionality (Atlantic Council, 2021).

The EU and the UK, on the other hand, have adopted accountability measures instead of bans. In 2023, “the Irish Data Protection Commission fined TikTok €379 million for breaking the GDPR's rules about children's data rights”. The company had to change the default settings to fix the problem (Data Protection Commission, 2023). This shows a big difference: India chose to ban TikTok, while the EU changed the way TikTok works to protect children's rights within a constitutional framework.

The conclusion of the case study is that India's TikTok ban effectively claimed digital sovereignty but did not show many clear benefits for child protection. The intervention moved

ISSN: 2582-6433

users to less-regulated platforms by taking away a service without giving them enough protection or clear control. This made safety concerns worse instead of better.

COMPARATIVE ANALYSIS AND DISCUSSION

The European Union, the United Kingdom, and India exemplify distinct paradigms of platform governance: rights-based proportionality, regulator-led enforcement, and sovereignty-driven prohibition. Each model is based on its own constitution and has various effects on kid protection and platform responsibility.

The EU model bases commitments on basic rights and fairness. “Article 25 of the GDPR says that "data protection by design and by default" (EUR-Lex, 2016). Article 34 of the Digital Services Act (DSA) says that Very Large Online Platforms must do systemic risk assessments. Article 37 makes independent annual audits necessary, while Article 45 gives the Commission the right to levy fines of up to 6% of global turnover (European Commission, 2022). The Irish Data Protection Commission fined TikTok €379 million in 2023 for illegally processing children's data and ordered changes to the default settings (Data Protection Commission, 2023)”. This is an example of rights-centered accountability. The UK approach turns policy aims into legal obligations. The Online Safety Act 2023's Section 11 sets up a "duty of care," and Section 68 gives Ofcom the power to make codes of practice that everyone must follow. Ofcom's 2025 guidance told platforms to set up "highly effective" age-verification mechanisms. This was a clear way to make sure that the UK government and Ofcom were serious about enforcement (UK Government/Ofcom, 2023; Ofcom, 2025). While the specifics seem promising, early research reveals that youngsters are still being exposed to hazardous content at a high rate. This shows that enforcement is more of a problem than legislative ambition (The Guardian, 2025).

The Indian approach favors independence and leaving the market. India banned TikTok and fifty-eight other applications on June 29, 2020, because they posed dangers to sovereignty and public order, according to Section 69A of the IT Act (Press Information Bureau, 2020). The restriction moved almost 200 million users (Kumar, 2023) to indigenous apps like Moj, which had 80 million monthly active users within a few months (Taddi, 2024). But these alternatives typically didn't have the same level of moderation, which means that risks were moved instead of lowered (Brookings Institution, 2023). The IT Rules 2021 made intermediary liability even bigger by adding requirements for traceability (Rule 4(2)) and quick takedown duties (Rule

ISSN: 2582-6433

3(1)(b)) (MeitY, 2021).

In a comparative synthesis, the EU shows that rights protection is based on proportionality, the UK shows that measured compliance is possible, and India shows that sovereignty is maintained by prohibition. The data indicates that child safety is greatest enhanced when accountability frameworks mandate risk assessments, algorithmic openness, and enforced design modifications; conversely, prohibitions lacking corrective protections only shift damages.

Limitations of the EU and UK Approaches

Although the European and British frameworks represent a marked advancement over prohibitionist strategies, both exhibit shortcomings that justify refinement. The GDPR and DSA's rights-based structure in the Union shows a high level of constitutional understanding, but enforcement is still a big problem. National authorities, especially the Irish DPC, have extensive investigative backlogs that leave minors vulnerable even when violations are acknowledged (European Data Protection Board, 2023). This gap gets worse because of too much dependence on ex post monetary consequences. Penalties often come years after the harm was done, and the complicated requirements of proportionality analysis and systemic risk assessments put too much pressure on smaller providers, which some people say makes dominant platforms even stronger (Brookings Institution, 2023). Empirical data indicates that addictive design elements and detrimental content persist in proliferating, despite formal adherence, prompting inquiries regarding the efficacy of paper-based requirements as protective measures (The Guardian, 2025). The British regime, though distinct, is not immune to critique. Ofcom's legal duty of care requires "highly effective" age-assurance, but some experts say that strong verification may need intrusive data collection or biometric checks, which would go against the privacy it is supposed to safeguard (Amnesty International, 2021). At the same time, Ofcom's broad discretion could lead to the removal of too much legal but controversial content, which could have a chilling impact on expression. There are also worries about whether one regulator can really keep an eye on compliance across thousands of businesses. Surveys conducted post-enactment validate that children's exposure to explicit content persists extensively, highlighting the disparity between legislative intent and actual results (The Guardian, 2025). The framework advanced in this study seeks to address these deficiencies by synthesising proportionality, algorithmic transparency, and privacy-preserving child-safety obligations within a single coherent model. Unlike the Union’s fragmented,

ISSN: 2582-6433

reactive approach, it emphasises ex ante design modifications and continuous audits; unlike the British reliance on regulator-led discretion, it embeds privacy-respecting verification standards to mitigate surveillance risks.

Policy Recommendations

Effective regulation of digital platforms must reconcile constitutional rights, technological realities, and enforceable safeguards. A comparative reading of recent enforcement suggests a three-tiered regulatory strategy: procedural safeguards rooted in proportionality, technical and transparency obligations, and graduated enforcement mechanisms responsive to risk levels.

First, regulators should institutionalise mandatory proportionality and impact assessments before invoking extreme measures such as blocking orders. Section 69A of IT Act authorises the central government to block digital services "in the interest of sovereignty and integrity of India" but does not require publication of proportionality analyses or judicial pre-clearance. The 2020 TikTok ban illustrates the risks of such opaque executive action, which disrupted a market of over 200 million users without demonstrable child-safety gains (Press Information Bureau, 2020; Kumar, 2023).

Second, platforms must be subjected to binding design and audit obligations. The Digital Services Act requires systemic risk assessments (Art. 34), independent audits (Art. 37), and empowers the European Commission to issue corrective orders (European Commission, 2022). "The Irish Data Protection Commission's 2023 €379 million fine against TikTok, confirmed by the European Data Protection Board, compelled structural redesign of default settings to protect minors, demonstrating that sanctions and audits can reshape practices without recourse to bans (Data Protection Commission, 2023; EDPB, 2023)".

Third, child safety requires privacy-preserving age assurance mechanisms. The UK Online Safety Act 2023 (s.11) introduced a statutory duty of care, and Ofcom's 2025 guidance mandates "highly effective" age verification standards. Crucially, these obligations must be benchmarked against measurable key performance indicators (KPIs) such as reductions in harmful exposure rates (UK Government/Ofcom, 2023; Ofcom, 2025). Fourth, enforcement capacity should follow a graduated model. Corrective redesign orders and audits should precede monetary fines, which in turn should precede market exit orders reserved for unremediable systemic risks. The EU's current Digital Services Act proceedings against major

ISSN: 2582-6433

platforms illustrate the utility of phased enforcement and iterative compliance (European Commission, 2024).

Finally, regulators must institutionalise cross-border cooperation. Given the transnational nature of digital harms, mutual assistance between supervisory authorities, harmonised data-transfer safeguards, and joint enforcement protocols are essential to ensure remedies remain effective across jurisdictions (Amnesty International, 2021). Collectively, these measures preserve constitutional safeguards while ensuring that platform accountability mechanisms remain enforceable, proportionate, and effective in protecting children in the digital age.

CONCLUSION

The comparative evaluation of the regulatory frameworks in the EU, UK, and India indicates that platform responsibility is fundamentally a constitutional issue, as it dictates the equilibrium between state sovereignty, market freedom, and the rights of vulnerable users. The EU model shows how important it is to include proportionality, fundamental rights, and enforceable obligations of design in a supranational governance structure. The Digital Services Act and recent fines against TikTok are two examples of this (European Commission, 2022; Data Protection Commission, 2023). The UK method, based on the Online Safety Act 2023, turns moral aspirations into legal responsibilities of care with measurable results. However, it will only work if Ofcom has the resources to carry them out and enforce them (UK Government/Ofcom, 2023; Ofcom, 2025). The Indian example, on the other hand, shows how restrictions based on sovereignty can strengthen state power but typically move risks around instead of lowering them. This raises questions about due process and constitutional proportionality (Press Information Bureau, 2020; Kumar, 2023).

The overarching lesson is that safeguarding children in the digital era cannot be achieved solely through prohibition. It needs design requirements that can be enforced, audits that are open to the public, and protections that are based on proportionality and respect both user rights and governmental interests. In the future, governance needs to go beyond the simple option between regulation and prohibition. Instead, it needs to create a unified system of accountability that puts constitutional ideals into action while also being able to adjust with new technologies.

ISSN: 2582-6433

REFERENCES

1. Amnesty International. (2021). TikTok's "For You" feed risks pushing children and young people towards harmful mental health content. Amnesty International.
2. Atlantic Council. (2021). The problem with India's app bans. Atlantic Council.
3. Brookings Institution. (2023). TikTok bans won't guarantee consumer safety. Brookings.
4. Celeste, E. (2018). Digital constitutionalism: A new systematic theorisation. International Review of Law, Computers & Technology, 32(2–3), 76–99. https://doi.org/10.1080/13600869.2018.1475898
5. Data Protection Commission. (2023). DPC announces €379 million fine of TikTok. Data Protection Commission.
6. De Gregorio, G. (2022). The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law, 20(1), 41–70. https://doi.org/10.1093/icon/moac002
7. European Commission. (2022). The EU's Digital Services Act. European Commission.
8. European Commission. (2023). DSA: Very large online platforms and search engines. European Commission.
9. European Commission. (2024). Implementation report on the Digital Services Act. European Commission.
10. European Data Protection Board. (2023). Binding decision 2/2023 on TikTok and children's data.
11. EUR-Lex. (2016). Regulation (EU) 2016/679 (GDPR). EUR-Lex.
12. Information Technology Act, No. 21 of 2000, § 69A, Acts of Parliament, 2000 (India).
13. Kumar, A. (2023). The case of the TikTok ban in India. Media, Culture & Society. SAGE Journals. https://doi.org/10.1177/01634437231156230
14. Ministry of Electronics & Information Technology (MeitY). (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Government of India.
15. Ofcom. (2025). Statement on protecting children from harms online. Ofcom.
16. Press Information Bureau. (2020, June 29). Government bans 59 mobile apps (including TikTok). Government of India.
17. Reuters. (2025, January 17). US TikTok ban could echo India chaos as users seek options. Reuters.

ISSN: 2582-6433

18. Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. Social Media + Society, 4(3). https://doi.org/10.1177/2056305118787812
19. Taddi, V. V. (2024). Perception, use of social media, and its impact on adolescent mental health in India. PMC Journal.
20. TechCrunch. (2023). TikTok fined €379M in EU for failing to keep kids' data safe. TechCrunch.
21. The Guardian. (2025, August 18). Children's exposure to porn higher than before 2023 Online Safety Act, poll finds. The Guardian.
22. TIME. (2025, January 30). Here is what happened when India banned TikTok in 2020. TIME.
23. UK Government/Ofcom. (2023). Online Safety Act — explainer / Ofcom guidance. GOV.UK.
24. UNCRC Committee. (2021). General Comment No. 25 on children's rights in relation to the digital environment.