The Dialogue®
INFORM ENGAGE IDEATE

KONRAD ADENAUER STIFTUNG

RESEARCH PAPER

REGULATION IN THE INTERNET AGE

BALANCING DIGITAL SAFETY AND HUMAN RIGHTS

RESEARCH PAPER

REGULATION IN THE INTERNET AGE
BALANCING DIGITAL SAFETY AND HUMAN RIGHTS

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue® has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Konrad-Adenauer-Stiftung (KAS) is a political foundation rooted in the principles of freedom, justice, and solidarity, closely associated with the Christian Democratic Union of Germany (CDU). KAS aids Germany in meeting its global responsibilities by promoting democracy, the rule of law, and a social market economy through its more than 100 international offices.

In 2005, KAS initiated the Rule of Law Programme Asia in Singapore to collaborate with Asian countries on rule of law development. The program focuses on Constitutional Law, Democracy Promotion, Procedural Law, Human and Minority Rights, Good Governance, Corruption Prevention, Judicial Independence, Environmental Law, and Tech Law/AI Ethics. Its primary aim is to advance the rule of law through regional seminars, dialogue, political exchanges, research, and training activities.

For more information
https://thedialogue.co | https://www.kas.de/en/rule-of-law-programme

Suggested Citation

Saxena, G. & Sharma, V. (2024, August) Research Paper: Regulation in the Internet Age - Balancing Digital Safety and Human Rights. The Dialogue® and KAS Rule of Law Programme Asia.

Catalogue No

TD/PR/RP/0824/02

Publication Date
September 16, 2024

KONRAD ADENAUER STIFTUNG

Dear Reader,

In today's rapidly evolving technological landscape, the need for robust safeguards has never been more evident. While the internet offers unparalleled opportunities, it also presents a myriad of challenges, ranging from cyberbullying to misinformation and privacy breaches. To navigate these complexities effectively, comprehensive digital safety strategies are imperative, particularly from a legal standpoint.

Furthermore, the discussion surrounding human rights in the digital sphere is paramount. As the United Nations asserts, human rights apply equally online and offline, emphasizing the need for a rights-based approach to online governance. In this digital age, online platforms wield considerable influence over individuals' expression and access to information, underscoring the importance of ensuring that legal frameworks prioritise human rights protections online making this project extremely timely and important.

This report, titled "Regulation in the Internet Age: Balancing Digital Safety and Human Rights," is the result of a collaborative effort between Konrad-Adenauer-Stiftung's Rule of Law Programme Asia and The Dialogue. This report explores the evolving legal and regulatory frameworks surrounding online safety in India and their implications for users' digital human rights, with a special focus on freedom of expression, privacy and consent and safety. It delves into case studies and presents key recommendations aimed at safeguarding online spaces while upholding fundamental human rights.

By addressing the intersection of digital safety and human rights, the report seeks to foster meaningful dialogue, drive policy reform, and inspire collaborative action to strengthen human rights in the digital space. The KAS Rule of Law Programme Asia extends its gratitude to the two researchers from The Dialogue, Garima Saxena and Vaishnavi Sharma, for their invaluable work in making this report possible.

The KAS Rule of Law Programme Asia's commitment to promoting the rule of law underscores the importance of ensuring that legal frameworks governing safety and legal protection and uphold human rights in the digital space. We hope for this report to ignite meaningful dialogue, spur policy reform, and foster collaborative action aimed at strengthening legal frameworks for human rights in the digital realm beyond India and the South Asian region.

Stefan Samse

Director, KAS Rule
of Law Programme Asia

Archana Atmakuri

Digital Communications Manager,
KAS Rule of Law Programme Asia

The Dialogue®
INFORM ENGAGE IDEATE

Dear Reader,

We are pleased to present our latest report, “Regulation in the Internet Age: Balancing Digital Safety and Human Rights. This report is the result of a collaborative effort between Konrad-Adenauer-Stiftung’s (KAS) Rule of Law Programme Asia and The Dialogue.

This research explores the complex landscape of online safety regulations in India, analysing their impact on digital human rights. In an era where billions engage with the internet daily, our work addresses the critical challenge of protecting users from online harms while preserving fundamental freedoms. The report focuses on the evolving legal and regulatory frameworks for online safety in India, examining the unintended consequences of these frameworks on users' digital rights, and offers recommendations for balancing safety and rights in the digital space.

The Dialogue, as a research-driven think tank at the forefront of technology policy, brings a unique and informed perspective to this complex topic. Our established track record in India's technology policy domain, recognised both nationally and internationally, forms the foundation for the insights and recommendations presented in this report. This collaboration with KAS enhances the depth and breadth of our analysis. We combine our expertise in technology policy with their focus on rule of law principles, aiming to provide a comprehensive perspective on the challenges and opportunities in regulating the digital sphere.

We hope this research will contribute significantly to the ongoing discourse on digital safety and human rights. Our findings and recommendations will, we believe, be valuable in shaping policies that effectively protect users from online harm while safeguarding essential freedoms.

Kazim Rizvi
Founding Director, The Dialogue

Contents

Abstract

The internet has become an integral part of modern life, transforming the way we communicate, conduct business, access information, and interact with others. In an era where billions of people worldwide actively engage with the internet, the importance of digital safety has risen to the forefront; users encounter online harms amidst the vast opportunities for global connectivity and empowerment offered by the digital landscape. While offering significant opportunities for global connectivity and empowerment, this digital landscape poses serious challenges such as cyberbullying, deepfake, misinformation and privacy breaches, prompting policymakers to craft comprehensive digital safety strategies. These strategies must strike a balance between safeguarding against online harms and upholding fundamental human rights like freedom of speech and privacy.

The effectiveness of these efforts relies on the development of evolving legal frameworks capable of addressing the nuanced complexities of the digital age without impinging on individual freedoms or stifling innovation. However, current laws often fall short, either by being outdated or overly broad, thereby risking the entrenchment of societal biases and enabling online harms. Moreover, the absence of transparent and fair processes for addressing these issues exacerbates power imbalances between users and digital platforms or state entities.

To address these challenges, this paper seeks to explore and analyse the evolving legal and regulatory frameworks concerning online safety in India. It also examines their resulting unintended consequences on the digital human rights of users, including the rights to free speech, privacy, and access to information, among others. Based on the analysis, the paper presents critical recommendations aimed at safeguarding online spaces from harm while ensuring that citizens can exercise their fundamental human rights in digital spaces.

Chapter 1:
Introduction

1.1 Context-Setting

As of 2024, the internet boasts a user base exceeding 5 billion people worldwide, with nearly 94.2 percent of them actively engaging on social media platforms each month.[1] On average, individuals spend close to 7 hours daily online, engaging in various activities such as work, entertainment, communication, and commerce.[2] This surge in human activity across websites, apps, and platforms has unlocked remarkable social and economic opportunities. Online spaces have served as catalysts for global movements, facilitated remote work, amplified marginalised voices, and fostered entrepreneurial endeavours. However, alongside these benefits, the proliferation of digital technology has introduced its share of challenges and complexities, particularly concerning safety in the digital sphere. Instances of digital harms and threats, including cyberbullying, harassment, misinformation, and online surveillance, have become increasingly prevalent, jeopardising users' rights and well-being. According to the 2023 Global Online Safety Survey conducted by a prominent tech company, which polled over 16,000 parents, teens, and other adults across 16 countries, including India, 69 percent of respondents reported experiencing online risks in the past year.[3]

In response to these challenges, policymakers and government entities have acknowledged the paramount importance of digital safety as a fundamental pillar in fostering inclusive and healthy societies in the Internet age. This acknowledgement has prompted a notable shift towards adopting a more comprehensive approach to digital safety, which encompasses various aspects, including speech and content regulation, data protection and privacy measures, cybersecurity protocols, digital literacy initiatives, and consumer protection efforts, among others. Pursuing this approach involves implementing a combination of legislation, regulatory and policy frameworks, and enforcement mechanisms.

However, amidst these endeavours, policymakers confront the formidable challenge of striking the delicate balance between ensuring safety online and upholding human rights such as the right to speech, privacy, and access to information. This challenge entails navigating complex and often competing interests. On the one hand, there exists a pressing need to address the proliferation of harmful content and activities online, thereby safeguarding individuals from various forms of digital harm, including cyberbullying, hate speech, and online exploitation. On the other hand, it is imperative to preserve and protect the fundamental rights of individuals, including their right to express themselves freely and their right to privacy, ensuring that regulatory interventions do not inadvertently infringe upon these rights. Regulatory interventions may, at times, unintentionally stifle innovation and compromise the Internet's democratising potential. This, in turn, may also prove counterproductive to digital safety itself and self-defeating in the long run. In essence, upholding digital rights cannot be an externality to online safety; they must be inextricably fused as elements to cultivate a digital landscape that is safe, secure, inclusive and conducive to human dignity and democratic values.

1.2 Defining the Problem

Legal frameworks aimed at governing digital spaces have emerged as a crucial determinant of the extent to which online spaces can be made safe and equitable. However, outdated or inadequate laws can act as barriers to progress and hinder individuals' ability to exercise their fundamental rights online, paradoxically enabling online harms, entrenching societal biases, and impeding users from exercising fundamental human rights like freedom of expression and privacy.[5] The practical application of vaguely defined or overly broad laws can significantly impact individuals' ability to engage meaningfully and equitably online. Restrictive policies may unintentionally create barriers or a chilling effect, preventing equal participation. For example, laws prohibiting hate speech, misinformation, or vaguely defined 'obscene' content online run the risk of being defined and applied in an overbroad way that infringes on legitimate free expression, access to

1. Digital Around the World, DATAREPORTAL, https://datareportal.com/global-digital-overview#:~:text=A%20total%20of%205.35%20billion,12%20months%20to%20January%202024.
2. Digital Around the World — DataReportal – Global Digital Insights, DATAREPORTA – Global Digital Insights. https://datareportal.com/global-digital-overview#:~:text=A%20total%20of%205.35%20billion,12%20months%20to%20January%202024.
3. Digital Safety, Global Online Safety Survey, https://www.microsoft.com/en-us/DigitalSafety/research/global-online-safety-survey.
4. For instance, in the recent past, the Indian government has encouraged several legislations on improving the use and impact of the internet like amendments to Information Technology Act, 2000 ("IT Act"); the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; etc.
5. Jacob E. Gersen & Eric A. Posner, Timing Rules and Legal Institution, 121 HARVARD L.R. , 543–589 (2007).

information, and freedom of the press.[6]

Moreover, many extant domestic laws and regulations lack adequate due process protections, transparent criteria, and fair appeal mechanisms. The lack of procedural safeguards creates an asymmetry of power between users and state agencies as well as platforms, making it difficult for individuals to seek equitable recourse in cases of inappropriate censorship or rights violations. At times, in the pursuit of enhancing online monitoring capabilities to detect illegal activities and abusive behaviour, privacy and data protection can be compromised through unchecked surveillance[7] authorities or mandates for tech companies to implement insecure infrastructure like encryption backdoors, thereby undermining digital privacy as well as safety.[8]

This is further complicated by the blurring lines between online and offline spaces, raising questions about how to adapt existing legal frameworks to the digital age.[9] For example, while offline harassment may be addressed through existing laws and regulations governing harassment, assault, and intimidation, these behaviours can become more pervasive, persistent, and anonymous when they occur online. This presents unique challenges of application and interpretation for law enforcement and legal systems.[10] Beyond their direct impacts, legal frameworks play a pivotal role in shaping broader social norms, cultural attitudes, and the boundaries that are understood around digital rights and acceptable online conduct.[11] The language and legal framing used to define issues such as online harassment, hate speech, data privacy, or content moderation hold immense power in influencing societal perceptions and biases. Moreover, legal codes and judicial precedents couched in discriminatory language may enable biased applications that reinforce the systemic marginalisation of individuals in digital spaces as well as offline. For instance, laws around policing indecent online content have often been interpreted in a discriminatory manner, reflecting prevailing cultural attitudes toward sex, gender identity, and morality.[12]

1.3 What can be done?

Evolving legal and regulatory paradigms governing digital domains must strive to balance competing aspects adequately – instituting meaningful safeguards and accountability measures around online harms while robustly upholding human rights principles of free expression, due process, privacy, access to information and non-discrimination. Prioritising nuanced, rights-respecting frameworks grounded on evidence-based policymaking, inclusive governance processes, and binding accountability measures is necessary to realise the internet's full potential as a safe, open, empowering space for all people to access information, engage in discourse and exercise fundamental freedoms equitably.[13] In this context, the European Union's Digital Services Act (DSA) emerges as a pivotal development, representing a comprehensive approach to online governance that mirrors the ideals of digital constitutionalism. This Act not only addresses the dissemination of illegal content and the challenges posed by misinformation but also underscores the protection of fundamental rights, ensuring platforms operate with greater transparency and accountability.[14]

6. Sarah Shirazyan, et al., How to Reconcile International Human Rights Law and Criminalization of Online Speech: Violent Extremism, Misinformation, Defamation, and Cyberharassment, STANFORD LAW SCHOOL, (Sept. 30, 2020), https://law.stanford.edu/publications/how-to-reconcile-international-human-rights-law-and-criminalization-of-online-speech-violent-extremism-misinformation-defamation-and-cyberharassment/.
7. Daniel J. Power et al., Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide, 4 JOURNAL OF BUSINESS ANALYTICS, 155–170 (2021).
8. Robert E. Endeley, Who needs an encryption backdoor: Why Americans want security over privacy., 1 AMERICAN JOURNAL OF SCIENCE AND ENGINEERING, 21–28 (2020).
9. Nirbhay Thakur, Indian courts see online violence against women as 'less real' than offline crimes: Study, INDIAN EXPRESS (November 7, 2023), https://indianexpress.com/article/cities/delhi/indian-courts-violence-women-offline-crimes-study-9016885/.
10. Shruti Shreya & Garima Saxena, #BreakTheSilo: Streamlining Gender Safety in the Digital Space, THE DIALOGUE (October 17, 2023), https://thedialogue.co/policy-framework-breakthesilo-streamlining-gender-safety-in-the-digital-space/
11. Kenworthey Bilz & Janice Nadler, Law, Moral Attitudes, and Behavioral Change, OXFORD HANDBOOK OF BEHAVIORAL ECON. & LAW (2014), https://experts.illinois.edu/en/publications/law-moral-attitudes-and-behavioral-change.
12. Genevieve Smith & Ishita Rustagi, When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity, STANFORD SOCIAL INNOVATION REVIEW (March 31, 2021), https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity#.
13. The Governance of Inclusive Growth, OECD (2015), https://www.oecd.org/governance/ministerial/the-governance-of-inclusive-growth.pdf.
14. Giancarlo Frosio & Christophe Geiger, Towards a Digital Constitution How the Digital Services Act Shapes the Future of Online Governance, STANFORD SOCIAL INNOVATION REVIEW (February 20, 2024), https://verfassungsblog.de/towards-a-digital-constitution/

Laws should also acknowledge the evolving social mores and ethical considerations that have historically informed discourse and jurisprudence around issues like online harassment, hate speech, non-consensual exploitation, and platform governance. A more thoughtful, inclusive approach to legal terminology, scope and application can contribute to shaping future policies and court rulings in ways that better accommodate the diverse perspectives, experiences and disproportionate risks marginalised groups face, thereby creating more inclusive and safer spaces online.

Viral Deepfakes and Disproportionate Chilling Effect

In November 2023, a deepfake video featuring an Indian actress went viral on social media,[15] bringing to light the regulatory and enforcement gaps within the extant regulatory landscape concerning information technology laws. Deepfakes, which leverage artificial intelligence to manipulate media and create convincing yet entirely fabricated content, particularly target women and other marginalised sections.[16] With the proliferation of artificial intelligence technologies, the global misuse of technology to produce such malicious content has become a pressing issue, underscoring the need for concurrent ethical standards, privacy safeguards, and supervision frameworks with the rapidly evolving field of artificial intelligence. Recognising the severe harm posed by deepfakes, the Indian government has issued advisories on AI that emphasise ethical deployment and accountability, aiming to strike a balance between innovation and societal well-being.[17]

Shreya Singhal and Freedom of Speech and Expression

The case of *Shreya Singhal v. Union of India*[18] is a landmark judgement in Indian constitutional law jurisprudence concerning freedom of speech and expression on the Internet. This case originated from a challenge to the constitutional validity of Section 66A of the Information Technology Act, 2000, which criminalised certain types of online speech. The petitioner mounted the constitutional challenge after two women were arrested for posting comments critical of the shutdown of Mumbai following the death of politician Bal Thackeray. The petition argued that Section 66A was vague and overbroad, thus infringing the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Indian Constitution.

The Supreme Court of India heard the case and extensively examined the provisions of Section 66A. The Court held that the language used in Section 66A was vague and ambiguous, leading to its misuse and abuse. The provision criminalised a wide range of speech, including legitimate expression of dissent and criticism, thereby chilling freedom of speech and expression on the internet.

15. Main accused in Rashmika Mandanna deepfake video case arrested, says police, The Indian Express (January 20, 2024) https://indianexpress.com/article/cities/delhi/rashmika-mandanna-deepfake-video-accused-arrest-delhi-police-9118870/.
16. Aja Romano, New deepfakes research finds they're mainly used to degrade women, VOX (October 7, 2019), https://www.vox.com/2019/10/7/20902215/deepfakes-usage-youtube-2019-deeptrace-research-report.
17. Ministry sends social media platforms advisory on deepfakes, The Hindu, (December 26, 2023), https://www.thehindu.com/sci-tech/technology/deepfake-concerns-government-issues-advisory-to-all-social-media-platforms-to-comply-with-it-rules/article67677002.ece; Mixed response to advisory on Deepfakes; government to notify tighter IT rules in a week, The Hindu (January 17, 2024), . https://www.thehindu.com/sci-tech/technology/deepfakes-in-india-mixed-response-to-advisory-government-notify-tighter-it-rules-in-a-week/article67747422.ece.
18. Shreya Singhal v. Union of India, (2013) 12 SCC 73, Writ Petition No. 167 of 2012.

The court emphasised the importance of protecting freedom of speech and expression in a democracy, particularly in the context of the Internet, which has become a vital medium for communication and expression. It recognised that while reasonable restrictions on freedom of speech are permissible under the Indian Constitution, these restrictions must be narrowly tailored and must serve a legitimate purpose, such as protecting public order, decency, or morality.

Article 19(1)(a) of the Indian Constitution guarantees people the freedom of speech and expression. The judgement also prevents the state from arbitrarily using its power to restrict freedoms mentioned in Article 19 and provides clear guidelines for future legislation pertaining to reasonable restrictions on fundamental rights and freedoms. However, while the provision has been struck down from the law, several cases have been initiated using the section to initiate cases against individuals.[19]

Revenge Porn and no space for Privacy and Consent

While Non-consensual Dissemination of Intimate Images (NCDII) is not a modern phenomenon and dates back to decades before the advent of the Internet, there has been an exponential rise in offences in the past few decades, as the advancement in digital technology and the Internet have enabled individuals to make such content available to a wide public.

In India, while the growing concern over the NCDII case, including revenge porn and sextortion cases, has caught the executive's attention, tracking perpetrators and holding them liable continues to be a concern. Furthermore, the issue is only exacerbated when, despite having appropriate laws such as section 66E of the IT Act (which gives due regard to privacy and consent violations), the courts have, in several instances, applied sections such as Section 67 and 67A of the IT Act (which concern obscenity). Such arbitrary application of the law relegates critical privacy and consent concerns to the shadows and, as a result, restricts the remedies available for victims.

Consider the case of Manoj Dattatray Supekar v. State of Maharashtra 2016 SCC OnLine Bom 15449, where the perpetrator, a man, videotaped sexual acts and non-consensually forwarded the clips to the victim's relatives and husband. Despite constituting a clear privacy and consent violation, authorities booked under section 67A (which criminalises sexually explicit media) rather than section 66E.

19. Gauri Kashyap, Section 66A: The Dead Lw That Still Haunts India, Supreme Court Observer (July 26, 2021), https://www.scobserver.in/journal/section-66a-the-dead-law-that-still-haunts-india/.

Chapter 2:

Examining the Legal Dynamics of Online Safety and Human Rights

The legal landscape surrounding online safety and human rights is complex, involving multiple laws and regulations that aim to balance the protection of individuals with the preservation of digital freedoms. This section examines the specific legal provisions governing aspects of digital safety, their implications on digital rights, and the challenges they pose to ensuring a safe and inclusive digital environment.

Relevant Law	Impact
Information Technology Act, 2000	**Broad Language and Subjectivity:** The issue of broad and subjective legal definitions, particularly regarding 'obscene' or 'sexually explicit' content, under the IT Act 2000, has profound implications for digital expression/ The ambiguity surrounding these terms can lead to selective enforcement, often at the expense of artistic content, advocacy for women's rights, and the expression of diverse sexual identities.[20] This creates a chilling effect, stifling free speech and suppressing diverse voices under the guise of protecting public morals or decency.[21] For instance, while Section 66A was initially introduced with the intention of safeguarding individuals, especially women, its broad scope inadvertently facilitated a wider clampdown on digital expression. Instances of application of this legal provision reveal patterns where individuals engaging in seemingly benign behaviours, like posting a meme or liking a controversial post, found themselves ensnared by law.[22] This phenomenon underscored a critical oversight in the legislation's design, which did not fully anticipate or mitigate against such expansive interpretations and applications. Furthermore, the eventual ruling in the landmark Supreme Court case of Shreya Singhal v Union of India, which struck down Section 66A as unconstitutional, highlighted the judiciary's recognition of these issues. However, reports of continued misuse post-ruling,[23]

20. Vrinda Bhandari & Anja Kovacs, What's sex got to do with it? Mapping the impact of questions of gender and sexuality on the evolution of the digital rights landscape in India, INTERNET DEMOCRACY PROJECT (January 20, 2021), https://internetdemocracy.in/reports/whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india. Vallishree Chandra & Gayathri Ramachandran, The Right to Pornography in India: An Analysis in Light of Individual Liberty and Public Morality. 4 NUJS LAW RevIEW 323 (2011).
21. Srirak Plipat, Creativity Wronged: How Women's Right to Artistic Freedom Is Denied and Marginalised, Freemuse (2018), https://freemuse.org/media/fabnhqia/freemuse-report_creativity-wronged_how-womens-right-to-artistic-freedom-is-denied-and-marginalised_online-version.pdf.
22. No more prosecutions under Section 66A, says Supreme Court, THE HINDU (October 12, 2022), https://www.thehindu.com/news/national/no-more-prosecutions-under-section-66a-says-supreme-court/article66002464.ece.
23. Krishnadas Rajagopal, SC 'shocked' over trials under Sec 66A of IT Act, BusinessLine (July 5, 2021), https://www.thehindubusinessline.com/news/its-shocking-people-are-still-booked-and-tried-under-section-66a-of-information-technology-act-sc/article35145694.ece.
Julie Posetti & Nabeelah Shabbir, The Chilling: A global study of online violence against women journalists, INTERNATIONAL CENTER FOR JOURNALISTS (November 2, 2022), https://www.icfj.org/sites/default/files/2022-11/ICFJ_UNESCO_The%20Chilling_2022_1.pdf. 13 infamous cases in which Section 66A was misused, India Today (March 25, 2015), https://www.indiatoday.in/india/story/section-66a-cases-how-it-curbed-245739-2015-03-24

Relevant Law	Impact
	particularly by local enforcement and judiciary, reflect a persistent challenge in ensuring that legal updates are comprehensively communicated and understood across all levels of law enforcement. **Lack of Consent and Privacy provisions for sexual and bodily autonomy:** While Section 66E provides for a model provision against non-consensual dissemination of intimate images (NCDII), pointedly factoring in privacy and consent concerns in its language, it is seldom used for that specific purpose. The effectiveness of the provision is limited by the broader legal framework within which it operates, which often prioritises issues of obscenity and public morality over individual rights to privacy and consent.[24] Sections 67 and 67A, which deal with the transmission of obscene material and material containing sexually explicit acts or conduct in electronic form, respectively, are particularly significant in this regard. These sections are frequently critiqued for their broad and subjective interpretation[25], which can lead to the suppression of lawful sexual expression under the guise of protecting decency and morality. This approach fails to recognise the importance of consent and the autonomy of individuals over their bodies, thus repressing any sort of sexual expression and denying any value which may come from it unless it passes the domestic obscenity tests.[26] **Decryption and the Right to Privacy:** Section 69[27] aimed at protecting national security and public order, raises concerns about the potential infringement of individuals' right to privacy. The requirement to provide decryption keys or assistance in decrypting information might compromise the privacy and confidentiality of personal or sensitive data stored or transmitted digitally. The Supreme Court of India in *Facebook Inc. v Union of India,*[28] in an order dated 24th September 2019, had stated that easy availability of decryption could defeat fundamental rights and that it should be relied on only in special circumstances, ensuring that the privacy of an individual is not invaded.

24. Vaishnavi Sharma, Understanding Non-Consensual Dissemination of Intimate Images Laws in India with Focus on Intermediary Liability, 14 NUJS Law Review 4 (2021), https://nujslawreview.org/2022/03/26/understanding-non-consensual-dissemination-of-intimate-images-laws-in-india-with-focus-on-intermediary-liability/
25. Sunil Abraham, Shreya Singhal and 66A: A Cup Half Full and Half Empty, 50 EPW 12 (2015), https://www.epw.in/journal/2015/15/commentary/shreya-singhal-and-66a.html
26. Gautam Bhatia, Obscenity and Pornography, Offend, Shock, or Disturb: Free Speech under the Indian Constitution, OUP (April 21, 2016), https://academic.oup.com/book/2791/chapter-abstract/143310578?redirectedFrom=fulltext
27. Section 67; Section 67A; Section 69A and Blocking Rules; Section 69 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
28. Facebook Inc. v Union of India, (2022) 15 SCC 532, TP (C) 1943-46/2019 (Diary No.32478-2019).

Relevant Law	Impact
	Blocking Powers and Expression and Economic Participation: The enforcement of Section 69A of the Information Technology Act, which permits the State to block access to online content deemed illegal, also emerges as a critical point of discussion. While aimed at safeguarding national security and public interests, the application of this section has raised concerns about its broader implications, particularly for marginalised communities. The 2020 ban on certain Chinese platforms is a significant instance where the state's exercise of its powers under Section 69A had unintended, disproportionate effects on less privileged sections of Indian society.[29] For many in these communities, these platforms provided not only a space for self-expression and public validation but also opportunities for content creation and income generation.[30] This reflects the inherent conflicts within digital governance: the challenge of balancing the state's security interests with the individual rights to freedom of expression and economic participation.
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	**Arbitrary Takedown Practices:** While the IT Rules, 2021 primarily aim to address the growing online harms and enhance the accountability of the platforms, several provisions contained therein pose challenges to free speech and expression and privacy. These provisions act as a barrier for marginalised individuals to represent themselves and discuss issues relevant to their experiences authentically online.[31] While these rules aim to protect users, they also risk inadvertently leading to over-censorship or selective enforcement, which can silence the very voices they intend to protect. For opinionated and outspoken women,[32] this can mean a greater likelihood of their content being flagged, reported, or removed under broad content moderation policies, potentially stifling their expression and participation in online discourse. Such takedown practices become all the more concerning when considering Rule 3(2), which obligates intermediaries to remove media portrayals which are 'sexually explicit', either on a complaint lodged by the individual themself or lodged on their

29. Devadasan, V., The phantom Constitutionality of Section 69A: Part i, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (October 22, 2022), https://indconlawphil.wordpress.com/2022/10/22/the-phantom-constitutionality-of-section-69a-part-i/.
30. Ahaskar, A. (2020, August 2). Indian tiktok influencers scramble for earnings, followers after App Ban. mint. https://www.livemint.com/companies/news/indian-tiktok-influencers-scramble-for-earnings-followers-after-app-ban-11596345861028.html.
31. Büchi, M., Festic, N., & Latzer, M., The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda, BIG DATA & SOCIETY 9(1), (2022), https://doi.org/10.1177/20539517211065368.
32. Why Is the Internet Still An Unsafe Place for Opinionated Women? - IWMF. Why Is the Internet Still an Unsafe Place for Opinionated Women? - IWMF. https://www.iwmf.org/2018/03/why-is-the-internet-still-an-unsafe-place-for-opinionated-women/; Online rape threats, abuse and vicious attacks: The price that Indian women in politics pay for being opinionated-India Newst. FIRSTPOST (August 16, 2018), https://www.firstpost.com/india/online-rape-threats-abuse-and-vicious-attacks-the-price-that-indian-women-in-politics-pay-for-being-opinionated-4980171.html.

Relevant Law	Impact
	behalf by "any other person." As noted, such broad wording could endanger the safe spaces which cater to marginalised communities in their attempts to define their sexualities through expression which may be explicit.[33] The balance between protecting individuals from online harm and ensuring the freedom of expression is delicate and requires nuanced content moderation practices that recognise and safeguard the right to speak out, especially on issues challenging societal norms. **Encryption and Privacy Concerns:** Furthermore, Rule 4(2), which mandates enabling technical measures to identify the first originator of the information on its computer resource on significant social media messaging platforms, has been criticised due to its unavoidable implication of ending end-to-end encryption.[34] Despite the good intent, the purposes outlined in the Rule might be overbroad and may not meet the proportionality test laid down in the K.S. Puttaswamy v. Union of India judgement. As end-to-end encryption plays an important role in maintaining confidentiality in technologically enabled communications and protects user privacy in everyday scenarios, it is essential to maintain a balance between public interests and the rights of individuals to privacy.[35] It also allows women and LBGTQIA+ individuals to voice their opinions and express themselves freely using encryption-enabled anonymity.[36]
Bharatiya Nyaya Sanhita, 2023 (erstwhile, Indian Penal Code, 1860)	The government has introduced the Bharatiya Nyaya Sanhita (BNS) to replace the 163-year-old Indian Penal Code. The shift in focus of the law from punishment to justice, as indicated in the title, reflects a shift to a more holistic understanding of justice that goes beyond punishment.[37] The law offers inclusivity by legally recognising transpersons as a legal category, a demand long made by the trans community.[38] However, the law has omitted legal protection for adult males and trans persons against sexual violence.

33. Torsha Sarkar et.al., On the legality and constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, THE CENTER FOR INTERNET AND SOCIETY INDIA (2021), https://cis-india.org/internet-governance/legality-constitutionality-il-rules-digital-media-2021.
34. Burman, A. & Jha, P., Understanding the Encryption Debate in India, CARNEGIE INDIA (September 13, 2021), https://carnegieindia.org/2021/09/13/understanding-encryption-debate-in-india-pub-85261.
35. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
36. See Bromell, D., Regulating free speech in a digital age: Hate, harm and the limits of censorship, Springer Nature (2022), https://books.google.com/books?hl=en&lr=&id=OadeEAAAQBAJ&oi=fnd&pg=PR9&dq=Free+Speech+in+the+Digital+Age:+How+Encryption+and+Anonymity+Protect+Our+Voices&ots=Eb062pQv2G&sig=ol0D161g9QVyh2IpEmLVQ9K86gI; Encryption: essential for the LGBTQ+ community - internet society, INTERNET SOCIETY (June 21, 2021). https://www.internetsociety.org/resources/doc/2019/encryption-factsheet-essential-for-lgbtq-community/.
37. Section 4(1) (f) of Bharatiya Nyaya Sanhita, 2023 introduces community service as a form of punishment.
38. Section 2(10) of Bharatiya Nyaya Sanhita, 2023 categorises gender into three classes – man, woman, and transgender. Keswani, H. Cyberstalking: A critical study. Bharti Law Rev, 131-48 (2017), https://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf.

Relevant Law	Impact
	Exclusion of Men and Transpersons from Rape Definition: The introduction of the BNS represents a significant legal evolution, aiming to modernise and adapt India's penal code to contemporary standards of justice and inclusivity. By acknowledging transpersons as a distinct legal category, the BNS takes a progressive step towards inclusivity, addressing long-standing demands from the transgender community for legal recognition and rights. However, the continued gender-specific language in its provisions, particularly concerning rape, highlights a persistent gap in the law's approach to gender and sexual violence. This reliance on traditional gender roles and definitions, where the law explicitly designates offenders as male and victims as female, does not account for the realities faced by transgender individuals and others who do not fit within these binary categories. The omission of Section 377 from the BNS, which previously criminalised rape against adult men, exacerbates this issue further, leaving a significant portion of the population without adequate legal protection against sexual violence. This exclusion not only undermines the law's inclusivity but also neglects to address the diverse and complex nature of sexual violence in contemporary society, including online spaces where such violence can manifest distinctly. Furthermore, recent amendments have recognised some forms of technology-facilitated gender-based violence (TFGBV), primarily protecting women's rights through criminalisation and failing to reflect the nature of such violence and the degree of harm caused. This approach raises significant challenges in adequately protecting women's rights and addressing the full spectrum of harm caused by such violence. The nature of TFGBV encompasses a range of behaviours from online harassment to emotional manipulation and coercive control through digital means,[39] presenting unique challenges that existing legal provisions do not always effectively capture. This discrepancy can hinder legal authorities' ability to prosecute cases of TFGBV, as the current framework may not fully account for the nuanced ways in which digital violence can impact victims.[40] **Obscenity in Online Public Sphere:** The definition of obscenity in Section 292 is rooted in archaic notions and understanding of

39. TechnologyFacilitated GenderBased Violence: Preliminary Landscape Analysis, GLOBAL PARTNERSHIP (2023), https://assets.publishing.service.gov.uk/media/64abe2b21121040013ee6576/Technology_facilitated_gender_based_violence_preliminary_landscape_analysis.pdf; Ronald Crelinsten, What can we do to combat online Gender-Based violence?, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION (June 23, 2022), https://www.cigionline.org/articles/what-can-we-do-to-combat-online-gender-based-violence/.
40. Malavika Rajkumar and Shreeja Sen, The Judiciary's Tryst with Online Gender-Based Violence, IT FOR CHNAGE (2023), https://itforchange.net/sites/default/files/2190/The%20Judiciary%27s%20Tryst%20with%20OGBV_0.pdf.

Relevant Law	Impact
	obscenity, whereby such understanding is extrapolated to the digital realm, highlighting a significant tension between traditional legal standards and the dynamics of contemporary societal norms and digital expression.[41] This tension is exacerbated by the broad and subjective nature of what constitutes "obscenity," potentially leading to overreach in the application of these laws online. Such overreach threatens to chill free expression, particularly for marginalised communities and those discussing or exploring issues related to sexuality, gender, and identity in the digital public sphere. The fear of legal repercussions for content that may be deemed "obscene" under these broad definitions can deter individuals and platforms from engaging in or facilitating open discussions, thereby limiting the diversity of voices and perspectives in online spaces. Moreover, the introduction of Section 195 of the BNS, which criminalises the dissemination of false information potentially harming India's sovereignty, unity, integrity, or security, raises additional concerns regarding free speech. The provision's potential for broad interpretation could further restrict lawful expression, particularly in critiquing or discussing governmental policies and social issues, by equating criticism with harm to the state. This poses a risk to the fundamental right to freedom of expression as protected under Article 19(2) of the Constitution and highlights the delicate balance between ensuring national security and preserving democratic freedoms in the digital age.
The Bharatiya Nagrik Suraksha Sanhita, 2023 (erstwhile, Code of Criminal Procedure, 1873)	**Broad Latitude and Discretionary Powers:** The Bharatiya Nagrik Suraksha Sanhita (BNSS), 2023, preserves Section 144 from the Code of Criminal Procedure, 1873, reflecting a critical juncture in the ongoing discourse on governance, public safety, and civil liberties. Section 144, known for granting district magistrates extensive powers to issue orders in response to nuisances or perceived threats, has historically seen varied applications, often tipping towards excess and arbitrariness. This broad discretionary power has implications for restricting internet access, impacting education, livelihood, and the broader civic life of individuals.[42] The Supreme Court's directives in the *Ramlila Maidan Incident case*[43] underscore the principle that such sweeping measures should be a recourse of last resort, advocating for proportionality and restraint in the face of

42. Vrinda Bhandari, et.al.,The Use and Misuse of Section 144 CrPC, SSRN (2023), http://dx.doi.org/10.2139/ssrn.4389147.
43. In Re Ramlila Maidan Incident, (2012) 5 SCC 1.

Relevant Law	Impact
	potential overreach. This guidance is pivotal, especially in an era where digital rights and access to information are fundamental to exercising democracy and individual freedoms. The continued inclusion of Section 144 in the new legal framework without stringent safeguards and a clear demarcation of its bounds raises concerns about the possibility of undermining digital liberties under the guise of maintaining public order.
Indecent Representation of Women (Prohibition) Act (IRWA), 1986	**Protectionist Language and Morality:** The IRWA aims to combat the derogatory portrayal of women across media platforms, extending its reach to the digital realm. However, the Act's broad and ambiguous definitions of "indecency" and "indecent representation" leave much to subjective interpretation,[44] potentially aligning with outdated societal norms and moralities. This lack of specificity in the law can create significant challenges in enforcement, particularly in the fast-evolving landscape of online media, where the line between creative freedom and derogatory representation can be exceptionally thin.[45] This ambiguity may not only hinder the law's effectiveness in protecting women from demeaning portrayals but also inadvertently entrench societal stereotypes about sexuality. The broad interpretation of what constitutes indecency can disproportionately impact women, restricting their freedom of expression and reinforcing the notion that female sexuality is inherently objectionable. Moreover, the queer community, whose expressions of identity and sexuality often diverge from mainstream norms, may find themselves particularly vulnerable under such laws. Their creative and representational works could be unfairly targeted as indecent, stifling their voices and diminishing the diversity of perspectives available in the media.[46]
Protection of Women from Domestic Violence Act, 2005	**Lack of Remedies for Domestic Violence Survivors:** The lack of explicit recognition of technologically facilitated gender-based violence (TFGBV) in domestic and familial contexts within legal frameworks signifies a gap in addressing the full spectrum of domestic violence in the digital age. This oversight can significantly undermine the severity and impact of such abuses,[47] which leverage technology for coercion, surveillance, and control, diminishing the affected individuals' autonomy,

44. Bishakha Datta, Guavas and Genitals, A research study in Section 67 of the Information Technology Act, IT FOR CHANGE (2018), https://projects.itforchange.net/e-vaw/wp-content/uploads/2018/01/Smita_Vanniyar.pdf.
45. *Keeping women safe? Gender, online harassment and Indian law,* INTERNET DEMOCRACY PROJECT (2013), https://internetdemocracy.in/media/keeping-women-safe-gender-online-harassment-and-indian-law-2.
46. Arushi Sharma and Shivanshi Gupta, Criminology of cyberstalking: Laws in India and UK, 1(4) INDIAN JOURNAL OF LAW AND LEGAL RESEARCH (2022), https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/injlolw4&section=331; Debrati Halder, Cyberstalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives, 11(1) NATIONAL LAW SCHOOL JOURNAL (2015), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1307&context=nlsj.
47. Alison J. Marganski, Lisa A. Melander, Technology-facilitated violence against women and girls in public and private spheres: Moving from enemy to ally, THE EMERALD INTERNATIONAL HANDBOOK OF TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE, 623–641 (2021), https://doi.org/10.1108/978-1-83982-848-520211046.

Relevant Law	Impact
	self-worth, and safety. The absence of specific legal remedies for victims of TFGBV limits their ability to seek protection and justice, highlighting an urgent need for legal systems to evolve in response to the changing dynamics of domestic violence.[48]
National Education Policy 2020 (NEP)	**Educational Gaps in the Digital Era:** While the NEP does lay emphasis on gender sensitisation, the policy fails to incorporate Comprehensive Sexuality Education (CSE) into the school curriculum. This highlights a critical gap in the legal and educational approach to online safety and human rights. In an era increasingly dominated by digital communication, the absence of formal education on topics such as menstrual health, contraceptives, and broader aspects of sexuality can lead to misinformation and stigma, impacting students' rights to information and education on crucial health and social issues.[49] This gap in the NEP points to the broader challenge of ensuring that digital and educational policies are inclusive, intersectional, and comprehensive, reflecting the diverse needs of the population.

48. Megan O'Brian, Online violence: real life impacts on women and girls in humanitarian settings, HUMANITARIAN LAW AND POLICY BLOG (January 4, 2024), https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings. See Dana Floberg, The racial digital divide persists. FREE PRESS (December 13, 2018), https://www.freepress.net/blog/racial-digital-divide-persists.
49. Anureet Watta, Can we guarantee a good education to young girls in current India?, YOUTH KI AWAAZ (September 2, 2021), https://www.youthkiawaaz.com/2020/12/what-does-the-nep-2020-say-about-gender/.

Chapter 3:

Key Recommendations

Recommendation 1: Updating Legal Frameworks to Prioritise Human Rights

Legal frameworks governing aspects of digital safety should enshrine human rights as the cornerstone and should be updated to integrate privacy, freedom of expression, and due process into regulations, ensuring they protect fundamental rights while addressing safety concerns. Laws must also be adaptable, allowing for rapid updates or modifications in response to new threats or technological developments. This flexibility ensures that protections remain relevant and effective without becoming obsolete or overly restrictive as the digital ecosystem evolves.

The DSA in the European Union exemplifies a comprehensive approach to harmonising digital safety with the protection of human rights. This regulation aims to create a safe, predictable, and trusted online environment by setting a uniform standard for intermediary services. It addresses crucial issues such as disseminating illegal content and the societal risks of disinformation, all while ensuring that the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union are effectively protected.[50] The DSA's focus on preventing harm and fostering innovation provides a valuable model for other regions and nations aiming to update or create digital safety laws prioritising human rights.

Recommendation 2: Focusing on Evidence-Based Policymaking

Policies and measures should rely on credible, empirical research and data to ensure effectiveness and avoid unintended consequences. This approach promotes informed decision-making grounded in data-driven insights rather than anecdotal evidence or speculation. Furthermore, implementing ongoing monitoring and ex-post evaluations of the societal impacts of laws governing digital safety is essential. This continuous monitoring allows policymakers to assess both the intended and unintended consequences of new regulatory models governing digital spaces.

For example, the Italian government, in collaboration with the Italian National Institute of Statistics (Istat) and various NGOs, has heightened its focus on data collection and analysis with the introduction of Law No. 53 in May 2022.[51] This law mandates a systematic approach to gathering detailed and reliable data regarding the prevalence, nature, and patterns of violence against women. Such data provide a comprehensive understanding that enables policymakers and researchers to develop targeted interventions and informed policies.

Recommendation 3: Defining Roles and Preserving Flexibility

Clearly defining the roles, responsibilities, and liabilities of all stakeholders is crucial for effective governance of the Internet ecosystem and ensuring digital safety. This involves governments, internet service providers, online platforms, and individual users. By establishing clear expectations and delineating accountability, policymakers can promote transparency and clarity in the digital space. Furthermore, maintaining flexibility for innovation within the boundaries of human rights frameworks is essential. The internet is a dynamic and rapidly evolving environment with constant technological advancements and emerging challenges. Therefore, regulatory frameworks must be adaptable to accommodate these changes while upholding fundamental rights and principles.

50. Recital 9, Digital Services Act, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.
51 Experts of the Committee on the Elimination of Discrimination against Women Commend Italy on Gender Architecture, Ask About Human Trafficking and Gender Parity in Politics.United Nations, (February 1, 2024).
https://www.ungeneva.org/en/news-media/meeting-summary/2024/02/examen-de-litalie-au-cedaw-des-progres-legislatifs-sont-notes.

Recommendation 4: Promoting Digital Literacy

Integrating digital literacy programmes into formal education systems and community initiatives is integral to empowering individuals. These programmes should be designed to equip individuals with the skills needed to navigate the digital landscape safely and effectively. Ensuring the accessibility and inclusivity of these programmes is crucial for reaching diverse learning needs. Collaboration with educational institutions, non-governmental organisations (NGOs), and tech companies is essential for developing and implementing comprehensive digital literacy curricula.

A notable example in this regard is California's recent legislative action, which mandates media literacy education in public schools, addressing the urgent need for media literacy in this digital age.[52] The law requires schools to instruct students in a set of skills crucial for the digital age, including recognising falsified data, identifying fake news, and generating responsible internet content.

Recommendation 5: Promoting Multi-Stakeholder Collaboration

Effectively addressing the complex challenges of digital safety requires promoting multi-stakeholder collaboration. This involves bringing together diverse expertise and perspectives from government agencies, technology companies, human rights organisations, security experts, and other vital sectors.

52. Robin Buller, There's nothing more critical': California makes schools teach kids to spot fake news, The Guardian, (December 5, 2023), https://www.theguardian.com/education/2023/dec/05/california-media-literacy-class-schools-misinformation.

Authors

Garima Saxena

Senior Research Associate, The Dialogue®

Garima Saxena is a Senior Research Associate at The Dialogue. She pursued her undergraduate degree from Rajiv Gandhi National University of Law, Punjab. Her prime interest lies in how our society interacts with technology and its impact on individuals. She actively advocates for privacy and digital freedom through her work.

Vaishnavi Sharma

Research Associate, The Dialogue®

Vaishnavi Sharma serves as a Research Associate at The Dialogue, specialising in privacy and data governance research. She earned her undergraduate degree from Maharashtra National Law University, Mumbai, with a strong focus on constitutional law. Her primary areas of interest encompass fundamental rights, including freedom of speech and expression, assembly, and privacy, both in offline and online contexts.

thedialogue.co

@_DialogueIndia
@TheDialogue_Official
@The-Dialogue-India
@TheDialogueIndia

kas.de

@kas_rlpa
@kasiusla
@kas-rule-of-law-asia
@Konrad-Adenauer-Stiftung-Rule-of-Law-Programme-Asia