Research Program
on Digital Constitutionalism
Project Aristotle

India

Country Report

December 2021

Authors

Ankit Kapoor, NLSIU Legal Services Clinic
Anshita Agrawal, NLSIU Legal Services Clinic
Arushi Tiwari, NLSIU Legal Services Clinic
Gurfateh Singh, NLSIU Legal Services Clinic
Harshita Thakral, NLSIU Legal Services Clinic
Rhea Prasad, NLSIU Legal Services Clinic

Institute
for Internet &
the Just Society

project
Aristotle

Research Program on Digital Constitutionalism **Project Aristotle**

India

Country Report

Authors
Ankit Kapoor, NLSIU Legal Services Clinic
Anshita Agrawal, NLSIU Legal Services Clinic
Arushi Tiwari, NLSIU Legal Services Clinic
Gurfateh Singh, NLSIU Legal Services Clinic
Harshita Thakral, NLSIU Legal Services Clinic
Rhea Prasad, NLSIU Legal Services Clinic

December 2021

Inquiries may be directed to digitalgovdem@internetjustsociety.org

DOI: 10.5281/zenodo.5792106

About us

The Institute for Internet & the Just Society is a think and do tank connecting civic engagement with interdisciplinary research focused on fair artificial intelligence, inclusive digital governance and human rights law in digital spheres. We collaborate and deliberate to find progressive solutions to the most pressing challenges of our digital society. We cultivate synergies by bringing the most interesting people together from all over the world and across cultural backgrounds. We empower young people to use their creativity, intelligence and voice for promoting our cause and inspiring others in their communities. We work pluralistically and independently. Pro bono.

Project Aristotle is the flagship project of the Digital Constitutionalism cycle of the Institute for Internet and the Just Society. Together with our international partners, we publish a research guide on what a structure of governance for the digital realm can look like when it is informed by interdisciplinary country-specific legal and policy research and analysis. We believe that delving deep into these bodies of knowledge, as shaped by a people within a particular national context, has much to offer in response to the pressing questions posed by the digital ecosystem.

INTRODUCTION

India is amongst the largest and fastest-growing markets for digital consumers. The public and private sectors are both driving digital growth. Emerging digital ecosystems are reshaping different sectors and a need for mutual response from all the stakeholders is reflected. This report aims to understand and analyse the emerging trends in the digital sphere and the role that constitutional tools can play in terms of regulating the digital platforms. The first section of this report seeks to explore the governance of the internet in India through the lens of rule of law and the role of the public in innovation and cooperation within the digital sphere. The second section of this report looks into the human and constitutionally guaranteed rights and their intersection with the digital ecosystem. The rights of minorities, need for regulation and moderation are also examined in this regard. The third section of this report discusses cardinal issues surrounding privacy, information security and the use of personal data. Ethical, economic and social considerations are looked into when examining issues pertaining to personal and non-personal data. Lastly, the fourth section of this report discusses intermediary regulation by placing it in the Indian landscape and exploring the content and information available online at a global level. It explores the role of guidelines in the digital sphere and the boundaries of regulating different types of content made available online. The report provides important insights into the Indian digital regime and highlights the role and importance of constitutional tools in ensuring that the digital sphere is transparent, accessible and equitable.

A. Digital Constitutionalism and Internet Governance

Digital Constitutionalism can be taken to mean the influence of constitutional tools on the governance of digital platforms by state and non-state actors. The definition explicitly mentions[1] non-state actors because the traditional constitution is limited to the relationship between the state and the citizens. Non-state actors, by laying down policies and regulations, play a key role in governing digital platforms alongside state actors. *Article 12*[2] *of the Indian Constitution* does not cover private entities within the definition of 'State'. The judicial interpretation of the same in recent cases, however, has stressed on the 'function test', i.e., an entity will fall within the ambit of *Article 12* in case it performs the functions of a state.[3] With private transnational entities becoming increasingly powerful and diverse, the question that arises is whether they already qualify under the function test. Not only are they engaged in regulation but also creation of rights. For instance, with Facebook planning to launch its own cryptocurrency, 'libra',[4] the assertion that tech giants are clearly outside the ambit of *Article 12* becomes hard to accept. Nonetheless, the need for a mixed governance structure is necessary. In India, this becomes even more important as social media platforms are gradually redefining the relationship between state and the citizenry by giving their own interpretations of the Indian Constitution. The recent clash between Twitter and the Indian government reflects how online platforms are becoming extremely political and influential nowadays.[5]

Digital Constitutionalism and the Rule of Law

Rule of law is one of the cardinal principles of constitutional law in India. The main postulates of rule of law, i.e., supremacy of the law, equality before law, and predominance of legal spirit are enshrined in the Indian Constitution. Supremacy of law is guaranteed under *Article 13(1) and (2)*[6] wherein any law made by the state, if

[1] The Constitution of India 1950, art 12.

[2] "In this part, unless the context otherwise requires, the State includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the Government of India."

[3] *BCCI v. Cricket Association of Bihar* (2016) AIR 1993 SC 892.

[4] Ashit Kumar Srivastava, 'Digital Constitutionalism and Personal Data Protection' (The Daily Guardian, 21 October 2020) <https://thedailyguardian.com/%EF%BB%BFdigital-constitutionalism-and-personal-data-protection/> accessed 20 March 2021.

[5] Lucas Henrique, 'Digital Constitutionalism and the Right to Protest Online- A Political Perspective of Digital Dissent from India's Experience with Content Moderation' (*ICONnect*) <://www.iconnectblog.com/2021/04/digital-constitutionalism-and-the-right-to protest-online-a-political perspective-of-digital-dissent-from-indias-experience-with-content-moderation/> accessed 12 April 2021.

[6] 13 (1) All laws in force in the territory of India immediately before the commencement of this Constitution, in so far as they are inconsistent with the provisions of this Part, shall, to the extent of such inconsistency, be void.

inconsistent with or violative of the rights under *Part 3 of the Constitution*, will be considered void. Equality before the law is guaranteed under *Article 14*[7] expressly wherein the state is absolutely barred from passing any law which is discriminatory. Predominance of the legal spirit is reflected in *Article 21*[8] of the Indian Constitution, wherein no person shall be deprived of life or liberty except in accordance with the procedure established by law. Cases like *Chief Settlement Commissioner of Punjab v. Om Prakash*[9], *Secretary of State of Karnataka and Ors. v. Umadevi*,[10] and *Kesavananda Bharati v. State of Kerala*,[11] reflect that the rule of law has become central to the Indian legal system; the primary touchstone through which state actions are judged. It, therefore, becomes important to ground Digital Constitutionalism also in the values of rule of law.

The first principle of rule of law talks about supremacy of the law which entails that no government or entity is above the law. An important prong of this principle is transparency of actions to prevent autocratic and whimsical decision-making and ensure compliance with the rules. This principle, when extended to Digital Constitutionalism, can bring about beneficial changes. For instance, the terms of services of Facebook were so vague that it allowed unfettered discretion to Facebook to terminate user accounts and moderate posts as it deemed fit.[12] This was later amended in 2009 to make it more concise. Even after the change, Facebook still retains substantial control over its user profiles as the terms still remain wide enough.[13] Hence, incorporating a more transparent policy system can be expected to limit the arbitrary actions of the digital platforms and make them more accountable. For instance, more specific guidelines with particular instances for removing content should be adopted. This will ensure that digital platforms do not circumvent transparency requirements through liberal interpretation of their guidelines.

The second principle of rule of law is equality, an extension of which is the legitimate expectation doctrine. It means that users should be treated equally, irrespective of their ideological, cultural, sexual or political ascriptions. Most of the digital platforms, however, moderate their content without disclosing specific reasons which undoubtedly raises assumptions of unequal treatment. For instance, LinkedIn's terms states that "We are not obligated to publish any information or content on our Service and can remove it with or without notice."[14] This sort of behavior results in platforms applying differential treatment to people of varying political ideologies, race, or sex. Even for the few platforms that promise to only remove content that violates explicitly stated rules, there is a great deal of uncertainty about how those rules are to be interpreted. For example, when it comes to display of nudity, it is unclear whether the image has to be sexual in nature and to what degree is skin-show not qualified as nudity.[15] Thus, digital platforms should apply the principle of equality and predictability in framing their terms to remove ambiguity. This will ensure that users are certain of the consequences of their actions and that all users are treated similarly in similar scenarios. Further, these terms should be drafted in simple English to ensure all users can access and understand the terms and conditions.

The third and necessary principle of rule of law is predominance of legal spirit which develops an enforcement mechanism for the above two principles. In digital governance, this principle can be applied in at least two forms. First, policies and terms should clearly specify the process through which any action may be taken by the platform regulators. Second, in case a user is aggrieved, a clear process of redressal should be set up

---

(2) The State shall not make any law which takes away or abridges the rights conferred by this Part and any law made in contravention of this clause shall, to the extent of the contravention, be void.

[7] "The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth."

[8] "No person shall be deprived of his life or personal liberty except according to procedure established by law."

[9] 1968 SCR (3) 655.

[10] AIR 2006 SC 1806.

[11] AIR 1973 SC 1461.

[12] Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 Social Media Society.

[13] ibid.

[14] 'User Agreement' (LinkedIn, 11 August 2021) <https://www.linkedin.com/legal/user-agreement> accessed 15 August 2021.

[15] 'Non-consensual Nudity Policy' (Twitter, November 2019) <https://help.twitter.com/en/rules-and-policies/intimate-media> accessed 16 July 2021.

with an unbiased authority that can review the same. Currently, there is hardly any platform that establishes any formal internal dispute resolution mechanism. Even the external dispute resolution process, which is litigation or arbitration, is not user-friendly. Almost all terms require users to resolve disputes in the platform's home jurisdiction which can be costly for users and can discourage them to approach redressal agencies. These, along with other examples, clearly create a deterrence effect on users to approach authorities with their disputes. This results in lack of faith in the legal system which promises to protect the rights of all citizens.

Since the fundamental rights recognised in *Part 3 of the Indian Constitution* only bind the state, the platforms are in a way immune to its violations. To address this, when the platforms do not make rules in consonance with the rule of law, the government should take it upon itself to align their actions with the laws of the land. The Union Minister for Information Technology recently stated that platforms must function with the laws of the land.[16] He added that a private company could not "put their own spin on our constitution."[17]*The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* have been enacted for the purpose of securing "transparency, accountability and rights of users related to digital media"[18]. The rules have widened the scope of intermediary oversight by introducing due diligence[19] and code of ethics[20] standards for them. While these steps address pressing issues for which the law was enacted, if observed closely, the law shifts the powers with the digital media to the government. Under the new IT rules, the government has the power to summarily take down content from digital platforms on vague grounds, and without so much as giving the publisher a hearing. This step has been criticised to be violative of "freedom of the press".[21] Thus, the government, while trying to limit the powers of digital platforms, has ended up creating an oversight mechanism which gives it unlimited power. This is against the concept of the rule of law, or in other words, the idea of good governance.

Digital Constitutionalism for the People, by the People, and of the People

In order to create a model *for* the people, users' interest should be given predominance over profit-maximising motives of digital platforms. Any policy or term that compromises users' privacy or any other right like freedom of speech should be immediately deemed unconstitutional. This would invite the same, or at least similar, consequences as would in a physical world. Digital platforms need to be made more accountable and their actions should be tested on the touchstone of constitutional doctrines. Further, obtaining individual consent should also be the norm. A data controller should give individuals the chance to choose (opt-in/opt-out) to provide their personal information, and take individual consent only after providing notice of its information-gathering practices. Only after consent has been taken, should the data controller collect, process, use, or disclose such information to third parties. Also, after the personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should follow the proposed National Privacy Principles.[22] This, as of now, is not done in India by any platforms.

Furthermore, the digital ecosystem must be safe, secure and universally accessible. The Indian Supreme Court has ruled the internet to be a fundamental right in the context of the prolonged internet suspension in Jammu and Kashmir.[23] The judges believed that lack of internet access hampers availing basic amenities such as

---

[16] A Surya Prakash, 'Centre's new IT rules were much-needed to ensure online platforms are subject to law of the land' (*The Indian Express*, 27 February 2021) < https://indianexpress.com/article/opinion/columns/digital-space-social-media-regulation-govt-control-it-act-7206572/> accessed 28 March 2021.

[17] ibid.

[18] Press Information Bureau (Ministry of Electronics & IT, Government of India) < https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749> accessed 19 March 2021.

[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Part II.

[20] ibid, part III.

[21] DheerajMishra, 'RTI Reply Busts Centre's Claim that 'Elaborate Public Consultations' Preceded IT Rules' (*The Wire*, 17 April 2021) <https://thewire.in/government/it-rules-ministry-information-broadcasting-media-ott-platform-rti-request> accessed 22 April 2021.

[22] Justice AP Shah Committee Report (Planning Commission) <http://planningcommission. nic.in/reports/genrep/rep_privacy.pdf> accessed 2 July 2021.

[23] *Foundation of Media Professionals v. Union Territory of J&K* (2020) SCC online SC 453.

healthcare, education, etc.[24] India has been a signatory to the *Convention on the Rights of Persons with Disabilities* since 2007.[25] *Article 9 of the Convention of the Rights of Persons with Disabilities* requires the states to ensure that persons with disabilities can access information, communication and technology systems (ICT).[26] To implement the convention, India enacted the *Rights of Persons with Disabilities Act* in 2016.[27] Regarding online platforms, the act states that all content available in audio, print and electronic media must be in an accessible format.[28] However, online applications remain largely inaccessible and often impossible to use for persons with disabilities. The government of India has recognised this need and has come up with *Guidelines for Indian Government Websites (GIGW 2009)*, *National Policy on Universal Electronics Accessibility (2013)* and the *Rights of Persons with Disabilities Act 2016* as mentioned earlier.[29] These said guidelines and legislations require compliance with web accessibility standards and provision of public information and resources in accessible electronic format. Only when digital spaces are inclusive and all-encompassing can it be actually said to be in compliance with the rule of law.

A constitutional model by the people can be advanced by introducing a system of voting by users or a representative group of users. Multistakeholder and participatory governance is imperative.[30] At present, there is no system of representation of users in the policy-making of the digital platforms. Users usually do not have a say in the process of updating terms. Thus, there should be a co-voting mechanism in place where a group of users are selected who represent the views of all. This step requires the inclusion of all vastly demographically differing groups to ensure adequate representation from all communities. On sensitive issues like censoring rules, minority views also need to be given some weightage to democratise the process for all. This system will by no means eliminate the dominance digital platforms exercise, but it will reorganise the skewed power imbalance to a certain degree. India is a country with diverse cultures and as many as 22 official languages. However, currently, a majority of the government websites are in English, except a few which have content either in Hindi or one of the regional languages. Thus, while government websites are accessible, they are not usable for all. There is a need for putting the government website information in regional languages.[31] The discussion on making online platforms more inclusive, representative and equal in India has largely focused on ensuring that the platforms are accessible for all, including persons with disabilities. The same has proven to be helpful and invited discussion to make online platforms more accessible. However, the discussion about ensuring adequate representation of individuals from different communities, genders and ethnicities has not emerged. Subsequently, there has been very little effort to ensure adequate representation on online platforms.

Making Digital Constitutionalism *of* the people requires platforms to be less exclusive and more competitive. Currently, however, there are a few big monopolistic companies which comprise a majority of the digital marketplace. Thus, the composition of online space has become exclusive, giving dominance to a few players in the market. This requires regulation by the government to promote more inclusivity and visibility of

---

[24] Murali Krishnan, 'Internet a fundamental right, review suspension: Supreme Court on J&K communication shutdown' (*Hindustan Times*, 22 August 2021) <https://www.hindustantimes.com/india-news/access-to-internet-fundamental-right-review-suspension-supreme-court-rules-on-communication-shutdown-in-kashmir/story-M9IocBfOPADxEeiAbHh6MK.html > accessed 25 March 2021.

[25] United Nations Convention on the Rights of Persons with Disabilities.

[26] Article 9 "To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and in rural areas. These measures, which shall include the identification and elimination of obstacles and barriers to accessibility, shall apply to, inter alia:
(a) Buildings, roads, transportation and other indoor and outdoor facilities, including schools, housing, medical facilities and workplaces;
(b) Information, communications and other services, including electronic services and emergency services."

[27] Rights of Persons with Disabilities Act 2016.

[28] Rights of Persons with Disabilities Act 2016, s 42.

[29] National Informatics Centre, Ministry of Electronics and Information Technology, *Guidelines for Indian Government Websites* (Version 2.0, 2019).

[30] Lex Gill, Dennis Redeker & Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2005) Berkman Klein Center for Internet & Society Research Publication 2015-15 <https://dash.harvard.edu/handle/1/28552582> accessed 4 April 2021.

[31] National Informatics Centre, Ministry of Electronics and Information Technology, *Guidelines for Indian Government Websites* (Second edn. 2018).

other players. This requires the state to take radical steps for promoting competition in the digital space. The most important change we need is competition-expanding regulations that address the problems that antitrust cannot solve.[32] Competition and consumer choice will help to address many of the problems we face with digital platforms today. In the face of increased competition, platforms will be forced to comply with the regulations, ensure transparency and promote user-friendly policies. Furthermore, a democratic culture is not democratic because people get to vote on what the culture should be like. It is democratic because people get to participate in the creation of such culture through mutual communication. A Digital Constitutionalism model for the people entails that the platforms allow users full exercise of their rights of free speech and access to information. This would mean that digital platforms strictly stay within the limits of censoring policies and refrain from tone policing, moderating conversations, etc.

Digital Cooperation

There has been a precipitous increase in interdependence on technology in day-to-day activities because of technological advancements like mobile connectivity, low-cost computing, etc. Such efficiency, innovation and speed of the digital ecosystem can expand opportunities for everyone. However, the same technologies can be misused. The existing mechanisms for cooperation and governance of the digital ecosystem have failed to effectively address such issues. To address this, the Secretary-General of the United Nations (UN) appointed a panel to consider the question of 'digital cooperation' in 2018.[33] The report compiled by the panel emphasised the need for multilateralism and cooperation between all stakeholders, including but not limited to civil societies, academics, technologists, and the private sector participants. Similarly, there is a need for bringing more diverse voices such as those from traditionally marginalised groups, like women, youth, indigenous people, rural populations and older people. The same report noted that there is no single approach to digital cooperation. Since technology is constantly evolving, the issues constantly evolve and require changes. However, it suggested that the practice should be to use all available tools, thereby, making dynamic choices.

Two possible architectures for global digital cooperation have been suggested in this regard by the panel.[34]First, the Internet Governance Forum Plus (IGF Plus), which would build on the existing Internet Governance Forum which was established by the World Summit on Information Society. The IGF Plus would build on the strengths of the existing mechanism and come up with actionable outcomes which can be addressed by working on policies and norms of direct interest to stakeholder communities. The current limited participation of government and business representatives, especially from small and developing countries, can be addressed by introducing discussion tracks in which governments and other stakeholders can address specific concerns. Second, a distributed co-governance architecture which would comprise of three elements - digital cooperation, network support platforms which host and enable dynamic formation and functioning of multiple digital cooperation and a digital commons architecture. Both these suggestions have the potential for developing not only the policy aspect of digital cooperation but also the participatory and enforcement mechanism of the same.

Open-Source Intelligence and Untapped Potential in India

Open-Source Intelligence is a process by which information that is collected by professionals from publicly available data is analysed and disseminated. It is an effective mechanism for intelligence operations and for purposes of ethical hacking. In India, OSINT's full potential still remains untapped. There are three spheres where the potential of open-source intelligence (OSINT) can be maximised. First, the military, as information provided by the government is not the sole source through which the public secures information about military affairs. OSINT is a tool for gathering data on the same. For instance, OSINT played a key role in the recent case of India's

---

[32] Gene Kimmelman 'The Right Way to Regulate Digital Platforms' (*Shorenstein Center*, 7 October 2019) <https://shorensteincenter.org/the-right-way-to-regulate-digital-platforms/> accessed 12 April 2021.

[33] Report of the UN Secretary-General's High-level Panel on Digital Cooperation, United Nations, *The age of digital interdependence*, (2018).

[34] ibid.

tense relations with China over the northern border matter.[35] Thus, in future, OSINT can be harnessed by government agencies to deal with terrorism and security matters and get opinions from experts by spending less resources than they actually do. There is a need for certain regulations on information that can impact national security or can cause serious damage to a community of people. Issues concerning individual data privacy should be addressed, and the existing laws towards ensuring the right to privacy must be strengthened.[36] Second, OSINT can uncover a lot of hidden, sensitive or even potentially classified information without having to resort to hacking or any other illegal activity. Information and communication technology systems are continuously attacked by criminals aiming at disrupting the availability of the provided services.[37] Forensic digital analysis can incorporate OSINT to complement the digital evidence left at an incident.[38] Third, it is now possible to collect user interactions, messages, interests and preferences to extract implicit (or tacit) knowledge through sentiment analysis. The evidence accumulated from social media is far-reaching and widely advantageous. Such collection and analysis could be applied, for instance, to marketing, political campaigns or disaster management.

Digital Innovation and Digital Constitution

The need for digital innovation cannot be overemphasised. The rights that are traditionally conferred are not enough to cater to users in the digital space. Factors like borderless reach, vastness of information and anonymity of individuals distinguishes physical spaces from digital spaces and prompts the need to recognise cyber-rights. In India, the need for innovation in online spaces was acknowledged after the spur of the Aadhaar privacy incident.[39] The *Aadhaar and Other Laws (Amendment) Bill 2018* had raised an uproar in the country for ignoring privacy concerns of individuals.[40] Among other several privacy issues, the primary one was that it allowed private entities to access individual's personal data like biometrics. While declaring privacy to be a fundamental right, the Supreme Court recommended constituting a committee to look into the nuances of the same.[41] Consequently, a 10-member committee was established, headed by the retired Supreme Court Justice B.N. Srikrishna, to identify issues regarding personal data protection and to draft a data protection law for India.[42] Subsequently, Justice BN Srikrishna Committee drafted the *Personal Data Protection Bill, 2018* which introduced a new set of rights in India, furthering the goal of a fair digital economy.[43] These include, right to confirmation and access that enables the data principal to seek confirmation of what data has been processed by the data fiduciary and the processing activities undertaken; right to correction that enables the data principal to correct, update and complete any data that needs to be modified; right to data portability that enables the data principal to obtain and transfer their data to other entities; and the right to be forgotten which refers to the ability of an individual to limit, delink, delete, or correct the disclosure of the personal information on the internet that is misleading,

---

[35] Thejus Gireesh, 'The Rise of Open Source Intelligence: Impact to the security and public discourses' (*Centre for Land Warfare Studies*, 28 December 2020) <https://www.claws.in/the-rise-of-open-source-intelligence-impact-to-the-security-and-public-discourses/> accessed 15 April 2021.

[36] ibid.

[37] Javier Pastor-Galindo and others, 'The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends' (2020) 8 IEEE Access <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8954668> accessed 8 April 2021.

[38] John Breedon, 'How Agencies Can Use Open Source Intelligence to Close Cybersecurity Loopholes' (*Nextgov*, 27 November 2019) <https://www.nextgov.com/emerging-tech/2019/11/how-agencies-can-use-open-source-intelligence-close-cybersecurity-loopholes/161580/> accessed 8 April 2021.

[39] Suhrith Parthasarathy, 'A renewed attack on privacy: Aadhaar Bill' (*The Hindu*, 9 January 2019) <https://www.thehindu.com/opinion/lead/a-renewed-attack-on-privacy/article25943864.ece> accessed 8 April 2021.

[40] The Aadhar and Other Laws (Amendment) Bill 2018.

[41] *K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012

[42] Pawan Singh, 'Making Digital Rights Count in India' (*Australia India Institute*, 15 November 2018) <https://www.aii.unimelb.edu.au/publications/very-short-policy-brief/making-digital-rights-count-in-india/#_ftnref1> accessed 8 April 2021.

[43] ibid.

embarrassing, or irrelevant.[44] Together, these rights are expected to provide a stronger framework of rights available to all on digital platforms. The results of these rights are yet to be seen in the upcoming years but they seem promising nevertheless. They are especially helpful for the disadvantaged as they face more data-vulnerability owing to lack of access to information and control over data.[45] While there are no specific frameworks or recommendations that have been made with regard to a global Digital Constitution, entities such as the United Kingdom,[46] the European Union,[47] Japan[48], etc. have implemented a harmonised data protection law by overcoming the existing difficulties. This was done by placing certain requirements for data protection probability. The aim was to protect and empower the citizens' data privacy and reshape the way organizations approach data privacy. In the European Union, independent public authorities were established in each member state which serve as the regulatory body for interactions with businesses and citizens.[49] It provides for transfer of personal data to third countries based on the condition that the said countries protect the data as it would be in the European Union.

B. Human and Constitutionally Guaranteed Rights

The right to access online platforms and the internet is a human right in itself which is intrinsically connected to a broad number of other human and constitutionally-guaranteed rights. In the recent decades, considering the gig economy, businesses, infrastructure and educational requirements,[50] it is observed that access to the internet is important to facilitate the promotion and enjoyment of several rights such as education and work to name a few.[51] As held in the *K.S. Puttaswamy judgement*,[52] the right to access the internet is a right that enables most of our fundamental rights. This includes the right to freedom of speech and expression; freedom of peaceful assembly and association and the right to life under *Article 21* which includes the right to education, health, the right to livelihood, the right to dignity and the right to privacy.[53] However, in the *Anuradha Bhasin judgement*,[54] it was pointed out that though the internet is a crucial means of achieving other constitutionally protected rights, the right to the internet itself does not constitute a fundamental right. Therefore, for people who don't have access to the internet in India, their means of exercising their fundamental rights becomes limited. A welcome step in this regard would be the recognition of digital rights as fundamental rights but that has not yet been envisioned in the Indian constitutional scheme. Before we examine these rights more closely, it is important to understand to whom they are available.

---

[44] Vinod Joseph and Deeya Ray, 'India: The Right to be Forgotten- Under the Personal Data Protection Bill 2018' (*Mondaq*, 12 November 2019) <https://www.mondaq.com/india/privacy-protection/860598/the-right-to-be-forgotten--under-the-personal-data-protection-bill-2018> accessed 5 April 2021.

[45] Praavita, 'Aadhaar Doesn't Work. Supreme Court's Judgment Cannot Change this Reality by Denying the Facts' (*Scroll.in*, 30 September 2018) <https://scroll.in/article/896374/aadhaar-doesnt-work-supreme-courts-judgement-cannot-change-this-reality-by-denying-the-facts> accessed 30 March 2021.

[46] The United Kingdom Data Protection Act 2018

[47] Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[48] Amended Act on Protection of Personal Information 2020.

[49] Y. D'Mello, 'How did we get here? A brief history of the GDPR' (*Aithority*, 3 May 2018) <https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/> accessed 30 March 2021.

[50] Jayna Kothari, Guaranteeing Indian Rights' (*The Hindu*, 31 December 2019) <https://www.thehindu.com/opinion/op-ed/guarantee-internet-rights/article30435736.ece> accessed 26 March 2021

[51] ibid.

[52] *K.S. Puttaswamy (Privacy-9J.) v. Union of India* (2017) 10 SCC 1

[53] Kothari (n 50)

[54] *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637

Any individual who has access to the internet has the potential to be classified as a 'netizen' and is granted this wide ambit of human and constitutionally guaranteed rights.[55] However, there is a distinction between a user of the internet and a netizen. A netizen is an individual who contributes to the development and growth of the internet and actively endeavours to make the internet a better place. Being a netizen implies an active engagement in making the internet a social and intellectual resource.[56] Bad actors or cyberthreat actors do not classify as netizens because they do not seek to promote and foster the growth of the internet. Rather, they are "states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cybersecurity awareness, or technological developments to gain unauthorised access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks."[57] An example of this would be the employment of internet bots by the government to further their propaganda.[58] Since bad actors or cyber threat actors do not classify as netizens, they are therefore not granted the wide ambit of human and constitutionally guaranteed rights available to internet users.

In India, while the rights of internet users have been enshrined in the constitution and espoused in judicial decisions, there is no statutory framework to protect and bolster these rights. We will examine the rights of various sections of society and whether India has adequate measures in place to protect these rights. We will also examine the interface between online and offline spaces and how public order is regulated on online platforms. Lastly, we will examine the role of social media councils and their possible efficacy in monitoring human rights in this era of Digital Constitutionalism.

Protecting the Rights of Minorities

Online environments are increasingly mirroring and amplifying the violence and discrimination that minorities face offline. It thus becomes imperative for social media platforms to design approaches that are responsive to the needs of minorities. Most intermediaries, such as social media platforms or companies providing services via websites, require the user to agree to their 'terms of service' (ToS). The ToS contains clauses that prohibit the user from using the company's services for illegal purposes, such as violation of copyright, financial fraud, extortion and child pornography, which can extend to legal protection against the violations of privacy of users. However, the ToS rarely mention any human rights abuses, especially those based on gender, sexuality or related issues.[59] Although some platforms like Twitter specifically mention human rights abuses (such as incitement against particular groups, hateful imagery)[60] the implementation of these policies is often less stringent. Recently, Twitter updated its policy to include "language that dehumanises people on the basis of race, ethnicity and national origin".[61] However, this measure seemed tokenistic as Twitter declined to comment on how their content moderators are trained or provide any information about how their artificial intelligence engines identify potentially problematic content.[62] This reflects the reluctance by companies to engage directly with human rights issues and rather only have liability for legal obligations with regards to the country of operation.

Bright-line policies of social media platforms on anonymity, etc. can also lead to privacy violations and have a disproportionate impact on minorities. For example, women who have anonymous online profiles, perhaps to escape abusive partners, harassers or disassociate from content shared about them, can suffer due to

---

[55] Micheal Hauben and Ronda Hauben, *Netizens: On the History and Impact of Usenet and the Internet* (1st edn, Wiley-IEEE Computer Society Pr 1997)

[56] ibid.

[57] 'Cyber Threat and Cyber Threat Actors' (*Canadian Centre for Cyber Security*, 18 November 2020) <https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors> accessed 25 March 2021

[58] Neerad Pandharipande, 'Amid anti-CAA protests, this coder amplified anti-establishment voices by taking down 1.6 lakh bots that disrupted Twitter trends' (*Firstpost*, 15 January 2020) <https://www.firstpost.com/india/amid-anti-caa-protests-this-coder-amplified-anti-establishment-voices-by-taking-down-1-6-lakh-bots-that-disrupted-twitter-trends-7898331.html> accessed 25 March 2021

[59] See FAQs: https://www.genderit.org/onlinevaw/faq/

[60] See: https://help.twitter.com/en/rules-and-policies#twitter-rules

[61] Reuters, 'Twitter expands hate speech rules to include race, ethnicity'(*The Hindu*, 2 December 2020) <https://www.thehindu.com/sci-tech/technology/internet/twitter-expands-hate-speech-rules/article33237705.ece> accessed 25 March 2021

[62] Ibid.

anonymity policies. Their profiles are reported as being "fake" and as a result women have to end up disclosing their identity rather than engaging in action against their harassers.[63] This creates unignorable privacy concerns. Further, the requirement to disclose official state-sanctioned identity documents has also resulted in discrimination and harassment towards transpeople, particularly those whose anonymity is critical for their safety and/or whose chosen names are central to their dignity and autonomy.[64] Such social media 'outing' of queer individuals can have disastrous ramifications. For example, in Tanzania, there is a surveillance squad that identifies and targets same-sex couples via social media and arrests them.[65] Greater attention is needed to ensure that policies are upholding the international human rights principles of non-discrimination and equality, and are taking into account contextual factors, such as language, culture, and power dynamics. It is clear that increased transparency is needed in a number of areas to better safeguard freedom of expression against arbitrary content removals and to better understand how the content viewed online is being moderated.[66] The use of digital media also creates the need to protect the rights of children and arrive at an appropriate digital age of consent.

The Indian government introduced the *Personal Data Protection Bill, 2019*, in the Lok Sabha on December 11, 2019, and it has subsequently been sent for review to a joint parliamentary committee. *Chapter IV*, *Section 16 of the Bill* deals with personal and sensitive personal data of children. It requires that a data fiduciary verify the age of a child and obtain the consent of his or her parent or guardian before processing their data.[67] The bill provides that the exact verification process will be specified through subsequent regulations. However, a pertinent point in this regard is that the verification process could make the data of the children available to the data fiduciary. Therefore, care must be taken to ensure that this data is not misused.[68] Further, there are many issues associated with having a blanket age of consent. The current digital ecosystem has adopted technological tools that have enabled children to grow and gain a better understanding of the digital space. Adolescents, who are generally termed as children, between the ages of 16 to 18, often have a comprehensive understanding of their activities online that is comparable to that of adults. Regulatory frameworks which do not take this into consideration end up having a negative impact on the interests of people in this age group. In 2016, approximately 44 million children in India were between the age of 16 and 18.[69] It is important that our laws do not restrict their ability to make use of the digital resources available to them.[70] Therefore, a plausible alternative is to adopt a graded approach to consent such that children below the age of 14 will need parental consent and children aged 14-16 years won't. Grading age of consent allows data fiduciaries to recognise that different age groups have different levels of development as well as different levels of recognising problems. Further, efforts must be made to protect the data of children. The Data Protection Authority should mandate age-appropriate standards and codes for online platforms. Some examples of this are: platforms should spell out why children's data is being collected in a way that the child can understand, the default setting should be private and companies should be prohibited from using nudge techniques to influence children to change their privacy settings.[71] These should be adopted in furtherance of child rights and the protection of children from exploitation, while also ensuring that their freedom of speech and expression is not unduly curtailed. A model like that of the Children's Ombudsman

---

[63] 'Providing a gender lens in the digital age: APC Submission to the Office of the High Commissioner for Human Rights' Working Group on Business and Human Rights' Association for Progressive Communications (*APC*, November 2018) <https://www.ohchr.org/Documents/Issues/Business/Gender/APC.pdf> accessed 25 March 2021

[64] Shepherd, Nicole. (2016) Big Data and Sexual Surveillance https://www.apc.org/sites/default/files/BigDataSexualSurveillance_0_0.pdf

[65] BBC News. (2018). "Tanzania: Anti-gay crackdown in Dar es Salaam." https://www.bbc.com/news/world-africa46048804

[66] 'EROTICS: An exploratory research project into sexuality and the internet' (*APC*, 6 August 2020) <https://www.apc.org/en/project/erotics-exploratory-research-project-sexuality-and-internet> accessed 24 March 2021

[67] Personal Data Protection Bill 2019, s 6

[68] Rajesh Bansal and Arjun Kang Joseph, 'Reconciling a child's right to privacy and autonomy' (*Hindustan Times*, 18 December 2019) <https://www.hindustantimes.com/analysis/reconciling-a-child-s-right-to-privacy-and-autonomy/story-FbpCPhr377diNTkawu5x6K.html> accessed 27 March 2021

[69] Bansal and Joseph (n 68)

[70] Bansal and Joseph (n 68)

[71] Soumyarendra Barik, '#NAMA Children and Privacy on the Internet: Should There Be a Blanket Age of Consent For Using Online Services' (*Medianama*, 18 December 2020) <https://www.medianama.com/2020/12/223-online-age-of-consent/> accessed 21 March 2021

can possibly be employed in the Indian landscape in furtherance of these rights and freedoms. A Children's Ombudsman is an independent authority constituted to protect the rights and freedoms of children. In India, such an institution would help in protecting children in their use of the digital space.

Regulating Online Spaces

In India, public order in the digital space is often defined by situations of disorder in the offline world. Recently, the Twitter account of The Caravan, a leading investigative journalism magazine was withheld.[72] The news agency ANI soon reported that around 250 accounts had been withheld by Twitter in India upon request from the Ministry of Electronics and Information Technology (MeitY) under *Section 69A of the Information Technology Act, 2000 (IT Act)*.[73] The accounts withheld by the social media platform included accounts of persons tweeting and retweeting in support of the ongoing farmers' protest against the newly introduced farm laws by the central government.[74] The recently notified *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (the Intermediary Rules) which pertain to Digital Media and the IT Act mandate additional compliances for intermediaries which increases their costs. Intermediaries are required to have a self-regulation mechanism while also being subject to oversight[75] by the Ministry of Information and Broadcasting (MI&B).[76]

There are many doubts regarding the independence of the self-regulating mechanism, because in reality it is functioning under the aegis of the MI&B.

Another disturbing development is the Ministry of Home Affairs's cybercrime volunteers program. In this program, volunteers can flag content online which the ministry can takedown. The grounds on which content can be flagged are arbitrary and vague.[77] Therefore, the volunteers can easily be influenced by their own beliefs and ideologies. This essentially creates a system of cyber vigilantism.[78]

This sort of a lateral surveillance program with unverified volunteers violates the *Shreya Singhal judgement* which prohibited the undue and arbitrary government curtailment of the online freedom of speech and expression.[79] As evinced from these developments, the government has lost out on the opportunity to improve upon the democratic rights of internet users.[80] As discussed earlier, jurisprudence is progressing to recognise the right to access the internet as a fundamental human right or at least a right that is essential to achieve other fundamental rights, The newly introduced barriers can have a chilling effect on this right and while there is a need to regulate the online space, the manner and substance of the current regulations beg urgent judicial review.

The government has also imposed internet shutdowns and curtailed the access and use of the internet to limit democratic free speech. *The Temporary Telecom Suspension Rules* were introduced by the Department of Telecommunications in 2017 under the colonial-era *Indian Telegraph Act*.[81] The said rules were envisioned to be used by the central/state governments and districts in case of public emergencies and to ensure safety. They also mention that no government department, except the Ministry of Home Affairs or a state's home affairs department can issue these orders. Recently, there was an amendment[82] which put a 15-day time limit on the validity of the order issued under the said rules. Every order for suspension of telecom service is reviewed by a

---

[72] Shambhavi Sinha and Nirmal Mathew, 'Why the New IT Rules Beg Urgent Judicial Review' (*The Wire*, 2 March 2021) <https://thewire.in/government/digital-platforms-intermediary-it-rules-india-freedom-of-speech-internet-control> accessed 26 March 2021

[73] Sinha and Mathew (n 73)

[74] Sinha and Mathew (n 73)

[75] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rules 10-12.

[76] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rules 10-12.

[77] 'What is Unlawful Content' (*National Cyber Crime Reporting Portal)* <https://cybercrime.gov.in/Webform/about_unlawful_content.aspx> accessed 26 March 2021

[78] Sinha and Mathew (n 73)

[79] Sinha and Mathew (n 73)

[80] Sinha and Mathew (n 73)

[81] Ministry of Communications, (Department of Telecommunications) Notification G.S.R. 998(E) dated 07.08.2017.

[82] Temporary Telecom Suspension Rules (Amendment) 2020.

review committee. The rules, however, do not provide specific grounds under which a shutdown can be ordered. They merely state that such an order can be issued in cases of public emergency or public safety. *Section 69A of the Information Technology Act* is relevant as well. It allows the central government and courts to order blocking of certain websites.[83] Similarly, *Section 144 of the Code of Criminal Procedure, 1973* has been used by the governments to impose internet blackouts.[84] The said section empowers authorities to issue directions to maintain public order in urgent cases of nuisance or apprehended danger. Internet shutdowns in India have taken place for varying reasons. The reasons for the same largely include a preventive strategy to deal with various law and order maintenance situations at "disturbed" areas.[85] There are other reasons that have been cited as well however. For instance, in states like West Bengal and Gujarat,[86] the state's board of secondary education and the state government's home department have previously introduced a curfew-style internet blackout during the secondary school examinations for up to nine days and have also used shutdowns as a measure to control cheating in exams.[87]

The aforementioned instances highlight the fact that the government, rather than protecting the constitutional rights of netizens, blatantly abuses them. It is also pertinent to note that the United Nations has considered cutting off users from internet access, regardless of the justification provided, to be disproportionate and a violation of *Article 19, paragraph 3 of the International Covenant on Civil and Political Rights*.[88] It has called upon states to ensure that access to the internet is maintained at all times, including during times of political unrest.[89]Further, from shirking requirements of due process to increasing executive control over the use of the internet, the government has ignored the ethos of the constitution and the decisions of the courts in landmark judgements like *K.S. Puttaswamy* and *Shreya Singhal*. In such a situation, it becomes important to envision an alternate model to monitor human rights online.

Social Media Councils - The Way Forward?

Article 19 is an internationally recognised body that endeavours to preserve the freedom to speak and the freedom to know by engaging with stakeholders on a global and regional level. In order to regulate human rights online, this organization has envisioned Social Media Councils (SMC) as a possible way forward. Essentially, a SMC is a body that lays down appropriate human rights standards for content moderation online. However, there are several factors that arise in envisioning SMC's as an appropriate model for Digital Constitutionalism. The first is which standard of human rights should be adopted by the SMC and the second is what sort of role the SMC should occupy. Ideally, the SMC should adopt an internationally accepted standard for online content moderation with a certain margin of flexibility. However, the problem with adopting an international standard is that it may not account for India-specific issues like caste. Additionally, it must be decided whether SMC's should have an adjudicatory or an advisory role. In an advisory role SMC's would provide general guidance and be an open forum for discussions and recommendations. This is preferable to an adjudicatory role and provides more freedom to intermediaries to take independent decisions.[90]

---

[83] Information Technology Act 2000, s 69A .

[84] Code of Criminal Procedure 1973, s 144.

[85] Shikhar Goel, 'Internet Shutdowns: Strategy to Maintain Law and Order or Muzzle Dissent?' (2018) 50(42) EPW <https://www.epw.in/engage/article/internet-shutdowns-strategy-maintain-law> accessed 26 March 2021

[86] TNN, 'To beat exam cheats, Gujarat to block mobile internet today' (*Times of India*, 28 February 2016) <https://timesofindia.indiatimes.com/india/to-beat-exam-cheats-gujarat-to-block-mobile-internet-today/articleshow/51173461.cms> accessed 26 March 2021

[87] Shadab Nazmi, 'Why India shuts down the internet more than any other democracy' (*BBC News*, 19 December 2019) <https://www.bbc.com/news/world-asia-india-50819905> accessed 26 March 2021

[88] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27

[89] ibid.

[90] Pierre Francois Docquir, 'The Social Media Council: Bringing Human Rights Standards to Content Moderation on Social Media' (*Centre for International Governance Innovation*, 28 October 2019) <https://www.cigionline.org/articles/social-media-council-bringing-human-rights-standards-content-moderation-social-media> accessed 28 March 2021

The scope of the SMC is another matter of debate. Perhaps in the Indian context, it would be preferable to have SMCs at the local level to account for linguistic, ethical, social and racial diversity within the Indian diaspora.[91] Another possible solution to regulating human rights online is the development of sophisticated AI software that can detect human rights violations and report them accordingly. However, such a technology-based solution would still require some amount of human oversight and it may take decades before such sophisticated software can be developed.[92]

In the Indian landscape, perhaps a homegrown model could be adopted where the National Human Rights Committee constitutes an adjunct wing to specifically look at human rights in the online space. These are merely suggestions to regulate human rights online in this era of Digital Constitutionalism but the Indian government is yet to take any concrete steps in this direction.

C. Privacy, Information Security, and Personal Data

To enforce its obligations under *UNCITRAL Model Law on E-Commerce*, the Parliament enacted the *Information Technology Act, 2000*.[93] In the absence of any specific data protection law, the provisions enacted under this act alongside the rules constitute the primary law on data protection. After rejecting the need to pass a legislation, the Ministry of Electronics and Information Technology framed the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011*. The primary objective was to protect India's lucrativeness to foreign business parties, and thus the scope of data protection obligations on body corporates were defined and clarified.[94] Accordingly, the scope of personal and sensitive personal data were largely tantamount to global standards.

The *2011 Rules* defines 'personal information' as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."[95] *Rule 3* recognises 'sensitive personal data or information' as a subset of personal data or information. It exhaustively defines sensitive personal data to include (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise. The proviso to this rule declares that any information that is freely available or accessible in public domain or furnished under the *Right to Information Act, 2005* or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Under *Section 3(28) of the Personal Data Protection Bill*, 'personal data' means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling. *Section 3(36) of the Bill* defines 'sensitive personal data' as such personal data, which may, reveal, be related to, or constitute (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under *Section 15*. *Sections 33-34* also mention critical personal data, without actually defining it. *Section 91(1)* empowers the central government to frame policies for the digital economy, in so far as they do not govern personal data. The explanation to *Section 91(2)* defines non-personal data (NPD) as the data other than personal data.

---

[91] ibid.

[92] Council of Europe Commissioner for Human Rights, 'Unboxing Artificial Intelligence: 10 steps to protect Human Rights' (*Council of Europe*, 14 May 2019) <https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights> accessed 28 March 2021

[93] Information Technology Act 2000, preamble.

[94] Rahul Matthan, *Privacy 3.0: Unlocking our Data Driven Future* (Harper Collins 2018), 99-109.

[95] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules 2011, rule 2(1)(i).

The Kris Gopalakrishnan Report (the Report) extensively discusses the aspects of NPD. However, it suffers from three primary flaws. First, it does not clearly establish the relationship between personal and non-personal data,[96] and instead treats them fallaciously as a dichotomy.[97] There is also a possibility of overlap between personal and non-personal data since the term inferred data falls within the scope of both the Report and the *PDP Bill, 2019*.[98] Second, there is vagueness over the scope of private NPD. For instance, when NPD is derived from the personal data of an individual or community, it is unclear how ownership of such data is attributed to a third-party private entity. Third, their port is inadequate vis-a-vis community rights as it fails to address the potential conflict between and among different communities. It also fails to recognise the implications of big data and machine learning on the anonymization of community NPD. These advances obscure a precise understanding of classification criteria for both analytics and members of these communities, with the latter often even lacking knowledge of the existence of such classification.[99]

Ethical, Economic and Social Considerations When Regulating Non-Personal Data

The Report, under paragraph 3.6-3.7, recognises the emerging trend of businesses and organizations using AI techniques to collect and analyse user data and generated content. However, this usage of these techniques is asymmetry concentrated among the market incumbents, thus creating an imbalance in the digital industry. The extent of imbalance is compounded in the Indian context given that it is among the top consumer markets owing to its large volume of smartphone users and fractured levels of internet penetration. Thus, if this imbalance is unchecked, it could lead to insurmountable market power in favour of said incumbents over emerging start-ups, MSMEs, the government, and private citizens. Thus, this socio-economic context necessitates regulation aimed at maximising overall welfare.

To protect data principals, the Report, under paragraph 4.5(iii), applies the concept of 'sensitivity' to NPD too, with the objective of protecting national security or preventing collective groups harm. The rationale behind this, as explained in paragraph 4.5(iv), is the presence of modern anonymization techniques that prevent perfect irreversibility of anonymised NPD. If re-identified, the extent of harm is greater if the underlying personal data is sensitive. Thus, greater protection is accorded to NPD derived from sensitive personal data. This empowers data principals to obtain relief if there is any harm from re-identification of their sensitive personal data. Thus, this protection is mindful of the ethical implications of technology.

Cognizant of the socio-economical and ethical implications, the Report, under paragraph 4.6(iii)-(iv), notes that the concept of 'consent for personal data' is unimputable for NPD because the conditions of 'specific' and 'capable of being withdrawn' are unsatisfied. However, consent can still act as a safeguard in limited situations. First, data principals must consent to anonymization of their data during collection to retain even limited agency. Second, there should not be any blanket consent for unlimited usage and sharing of collected personal data. This is especially since the entities that subsequently receive such NPD are not obligated to register its receipt and intended use.

The Report's position on open-access to metadata has an adverse ethical implication on the surveillance architecture. Under paragraph 7, it states that said access spurs unprecedented innovation and growth in the digital economy. However, there are no limitations to the usage of said data for sovereign purposes, and no oversight or counterbalancing balance. Moreover, this assertion is entirely unsupported by empirical evidence.[100]

---

[96] 'SFLC.in's Comments on Non-Personal Data Governance Framework' (2020) SFLC <https://sflc.in/sites/default/files/2020-09/mygov_160001782547894471.pdf> accessed 28 March 2021.

[97] 'Consultation on the Non-Personal Data Governance Framework, 2020' (2020) GSMA ASIFMA, 5-6 <https://www.asifma.org/wp-content/uploads/2020/09/gfma-response-to-meity-npd-consultation-final-v20200911-clean.pdf> accessed 28 March 2021.

[98] GSMA ASIFMA (n 62) 6.

[99] 'Submission of Comments on Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) NLUD Center for Communication Governance, 40 <https://ccgdelhi.org/wp-content/uploads/2020/09/CCG-NLU-Comments-to-MeitY-on-the-Report-by-the-Committee-of-Experts-on-Non-Personal-Data-Governance-Framework.pdf> accessed 28 March 2021.

[100] NLUD Center for Communication Governance (n 64) 27.

Conversely, there is a lack of clarity over the scope of NPD including unstructured data. If included, this overburdens businesses by complicating ease of doing business and may even deter foreign investment.[101]

Encryption Backdoors

Section 69 of the IT Act, 2000 authorises the central and state governments to intercept, monitor or decrypt communications in the interest of national security, sovereignty, defence and for preservation of public order or investigation of an offence. Under *Rule 3 (5), the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009* (2009 Rules), service providers and subscribers are obligated to assist government agencies with accessing data by decryption or interception. Under *Rule 9*, the scope of decryption is quite broad, extending over "any information as is sent to or from any person or class of persons or relating to any particular subject"' Moreover, *Rule 23* requires records pertaining to decryption orders be destroyed within a prescribed period of six months, which significantly diminishes the scope for review of the government's exercise of such unilateral power. Arguably, end-to-end encrypted platforms are outside the scope of these rules since under *Rule 2(g)(i)* and *Rule 13(3)*, 'decryption assistance' is defined as assistance to allow access, to the extent possible, to encrypted information, where the intermediary has control over the decryption key. However, the architecture of end-to-end encryption precludes the intermediary with such access.

Under *Section 79 of the IT Act*, an intermediary is exempted from liability if inter alia they observe due diligence and other guidelines, stipulated by the government, while discharging their duties. Under *Rule2(v)* read with *Rule4(2) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (2021 Rules)*, a significant social media intermediary providing message services has to enable identification of But such order can only be passed on the grounds of "investigation, prosecution, and punishment of an offence related to the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, or public order, rape, sexually explicit material, or child sexual abuse material." Moreover, no significant social media intermediary is required to disclose the contents of any message during such compliance. However, this may be overridden by the provisions of the *2009 Rules*, which contain powers to make demands for the message content. Used together, these provisions empower the government to break any type of end-to-end encryption to gain knowledge of message content too.[102] But there are constitutional challenges to these provisions.[103]

Dr. V Kamakoti, Professor of Computer Science at IIT Madras, had proposed to the Madras High Court two proposals on operationalising traceability. The rationale behind this was the utility of traceability for law enforcement and free speech.[104] However, Dr. Manoj Prabhakaran,Professor of Computer Science at IIT Bombay, responded to this proposal in court by highlighting that this proposal would erode user privacy and prove to be ineffective for its purpose. He argued that traceability is not a demonstrable deterrent as is apparent from the ubiquity of fake news on social media platforms and that it has limited utility until untraceable messaging services become widely available in the market. Further, he argued that phone numbers have little identification value and equally, tracing the originator of content does not have any practical value because of the room for impersonation and little scope for mitigation. He argues that previous proposals demonstrating the compatibility between traceability and end-to-end encryption have all been vulnerable to spoofing. This is when the message originator

---

[101] GSMA ASIFMA (n 62) 8.

[102] 'Deep dive: How the intermediaries' rules are anti-democratic and unconstitutional' (*Internet Freedom Foundation*, 27 February 2021) <https://internetfreedom.in/intermediaries-rules-2021/> accessed 28 March 2021.

[103] Notably, the constitutionality of Section 69 and the 2009 Rules has been challenged before the Supreme Court, in Internet Freedom Foundation & Another v Union of India (WP (C) No 44/2019, on the ground of violating the right to equality, privacy, and freedom of expression. This matter will be taken up by the Supreme Court in Facebook Inc. v Union of India (TP (C) 1943-46/2019), along with 3 cases on encryption and traceability (mandatory linking of government issued ID card to social media accounts) that were initially instituted before the Madras, Bombay, and Madhya Pradesh High Court, respectively. Moreover, the constitutionality of IT Rules, 2021 has been challenged before (1) the Delhi High Court in the Foundation for Independent Journalism v. Union of India and Sanjay Kumar Singh v. Union of India; and (2) before the Kerala High Court in Live Law Media Private Limited v. Union of India.

[104] Aditi Agarwal, 'Kamakoti's proposals will erode user privacy, says IIT Bombay expert in IFF submission' (*Medianama*, 27 August 2019) <https://www.medianama.com/2019/08/223-iff-response-kamakoti-submission-traceability-2/> accessed 28 March 2021

has no control over the person forwarding the message, its frequency, and subsequent fora of dissemination.[105] Most importantly, the negative impact of compromising encryption on privacy and security is immense and inevitable, and far outweighs any perceived benefit.[106] A traceability mandate creates new risks to communications security that makes it a very intrusive measure that is unlikely to be the least intrusive approach. It completely undermines anonymity, which is essential to the ability to communicate without fear of retribution. Moreover, compromised anonymity also creates a chilling effect on free speech.[107]

Encryption permits the creation of a safe space for users' right to privacy and freedom of expression and protects them from becoming vulnerable to unfettered surveillance and malicious or repressive actors. It preserves communicational privacy, reflected in the ability to restrict access to communications; intellectual privacy, which is the freedom to develop ideas without being monitored; and informational privacy, resting on the elements of secrecy, anonymity and control. The importance of encryption is therefore amplified in jurisdictions such as India where the surveillance regime lacks adequate checks and balances.[108] Repressive governments often use surveillance to monitor citizens' actions,[109] and encryption offers a degree of freedom from such surveillance.[110] Traceability would empower repressive regimes with the ability to ascertain who interacted with a particular message that expressed dissent or encouraged protest, irrespective of the context in which they did so.[111] More importantly, the shield of anonymity empowers the voiceless to speak up openly and publicly by eliminating their fear of prosecution.[112] The creation of a backdoor necessarily means the end of end-to-end encryption because platforms need to break existing protocols by fundamentally altering their architecture that has been built through rigorous cybersecurity testing over the years.[113] This weakens anonymity for both the targeted message originators and every user within the communication system.[114]

Compliance with Privacy Statute During Crises and Using Regulatory Sandboxes

There are excessively broad exemptions under the *PDP Bill, 2019*. *Sections 4-11 of the PDP Bill, 2019* establish safeguards in the collection and processing of personal data, such as consent. The requirement of only consent is omitted, under *Section 12(d)-(f)*, for grounds such as medical emergencies, public health crisis, disasters, or breakdown of public order. However, the central government can override other safeguards too through its broad powers under *Section 35*. This is particularly concerning given the inadequate counterbalancing mechanisms, which legitimises unbridled surveillance.[115] The government needs to simply pass a written reasoned order on broad grounds such as national security, foreign relations, or law and order. These exceed the scope

---

[105] 'Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?' (*Internet Freedom Foundation*, 25 February 2021) <https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/> accessed 28 March 2021

[106] Agarwal (n 105)

[107] Agarwal (n 105)

[108] 'India's Surveillance State' (2014) SLFC.in Surveillance Report <https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> accessed 28 March 2021.

[109] Bedavyasa Mohanty, ''Going Dark' in India: The legal and security dimensions of encryption' (*Observer Research Foundation*, 13 December 2016) <https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption/> accessed 28 March 2021

[110] Ibid.

[111] Aroon Deep, 'Encryption and issues related to Misinformation' (*Medianama*, 15 June 2020) <https://www.medianama.com/2020/06/223-encryption-misinformation/> accessed 28 March 2021

[112] Rahul Matthan, 'Traceability is Antithetical to Liberty' (*Ex Machina*, 3 March 2021) <https://exmachina.substack.com/p/traceability-is-antithetical-to-liberty> accessed 28 March 2021.

[113] 'Deep dive: How the intermediaries' rules are anti-democratic and unconstitutional' (*Internet Freedom Foundation*, 27 February 2021) <https://internetfreedom.in/intermediaries-rules-2021/> accessed 28 March 2021.

[114] Matthan (n 113).

[115] Renjith Mathew, 'Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study' (*SCC*, 22 May 2020) <https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#_ftnref28> accessed 28 March 2021.

envisaged in the *PDP Bill, 2018*, which was limited to 'security of the state'.[116] The addition of 'public order' is particularly concerning given its wider scope and lower threshold of invocation. The government can easily justify the invocation of this ground by easily satisfying the test of 'expedience', which is extremely deferential since it is difficult to restrict.[117] The exemptions are also disproportionate since the government is empowered to exempt the application of the entire bill to all agencies for all functions.[118] Such overbroad exemptions are not always required for all agencies for all functions, and there is no rationale for omitting basic safeguards like fair and reasonable processing under *Chapters I, IX-XIV of the Bill*. There is also no independent high-level oversight mechanism or periodic review, alongside a lack of judicial review over the government's exemption decisions.[119]*Section 35* also provides the government criminal immunity, which frustrates the operation of other statutory remedies even if the government is found guilty.[120]

Under *Section 40(1) of PDP Bill, 2019*, the Data Protection Authority (DPA) is empowered to create sandboxes for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest. The DPA's power to sanction sandboxes is bound by safeguards under *Section 40(4)*. First, they cannot grant renewals to the sandbox more than twice, subject to a total period of thirty-six months. Second, data fiduciaries must specify the adopted safeguards alongside compensatory mechanisms. Third, the scope of provisions under *the PDP Bill, 2019* which can be exempted (these are: *Sections 4, 5, 6, and 9*) are specified.

Despite these welcomed safeguards, there are still issues with *Section 40*. First, there is no clarity on the nature of the sandbox offered. In practice, there are data and regulatory sandboxes. Data sandboxes serve as a secure area where only a copy of the company's or participant companies' data is located for scaling the fiduciaries' datasets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions.[121] Second, there also exists an absence of consumer protections. This blanket vacation of consumer protections, instead of their addition, is uncommon and should be rectified. While *Section 40(4)* contains some safeguards, regulators must ensure that data principals' rights are extended rather than curtailed in the sandbox. This requires the stipulation of a clear redressal mechanism and that all participants ensure protection of data principal obligations before they exit the sandbox.[122]Third, the objectives are unclear as well. The stated objective is merely 'supporting innovation for public interest'. This vagueness creates situations where regulators are handicapped in assessing the feasibility, potential outcomes, and collateral effects of operations in the sandbox. There is also uncertainty in the interaction with the sandboxes offered by other sectoral regulators. For instance, the proposed sandbox under the DPA may overlap with the RBI's fintech sandbox. The adverse consequence here includes regulatory arbitrage or over-regulation, if regulatory perimeters are not clearly defined.[123]

Principles and Regulations Governing the Operation of Intelligence Agencies Online

---

[116] Aditi Agarwal, '#NAMA: Issues Around Surveillance In The Personal Data Protection Bill, 2019' (*Medianama*, 29 January 2020) <https://www.medianama.com/2020/01/223-nama-issues-surveillance-personal-data-protection-bill-2019/> accessed 28 March 2021.

[117] Ibid.

[118] Agarwal (n 117).

[119] Rishab Bailey, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman, 'Comments on the draft Personal Data Protection Bill, 2019' (*The Leap Blog*, 3 April 2020) <https://blog.theleapjournal.org/2020/04/comments-on-draft-personal-data.html> accessed 28 March 2021.

[120] Agarwal (n 117).

[121] Amber Sinha, Elonnai Hickok, Pallavi Bedi, Shweta Mohandas and Tanaya Rajwade, 'An Annotated Version of the Personal Data Protection Bill 2019: Comments and Recommendations' (2020) The Center for Internet & Society, 3 <https://cis-india.org/internet-governance/annotated-version-of-comments-to-the-personal-data-protection-bill-2019> accessed 28 March 2021.

[122] 'Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019' (2020) Dvara Research, 14 <https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf> accessed 28 March 2021.

[123] ibid.

The standard for infringing upon the fundamental right to privacy was established by the Supreme Court in *K.S. Puttaswamy v Union of India (2017)*, namely legality, necessity, and proportionality.[124] In *K.S. Puttaswamy v Union of India II (2019)* (Aadhaar judgement)[125] it was held that proportionality is satisfied when:(a) the interference has a legitimate goal; (b) it must constitute a suitable mean of achieving the goal; (c) there must not be any less restrictive but equally effective alternative; and (d) the measure must not have a disproportionate impact on the rights holder. Any activity by an intelligence agency must satisfy this standard. Government surveillance in India can be legitimised under either *Telegraph Act, 1885* or *Section 69*, *IT Act, 2000*.

Under the *Section 5*, *Telegraph Act*, *1885*, the central or state government can intercept in two circumstances. First, when there is a 'public emergency' or 'in the interest of public safety'. Second, when it is necessary or expedient to do so, which includes inter alia a broad list from sovereignty and integrity of India to friendly relations with foreign states. Under *Section 69*, *IT Act*, *2000* there is an expansion of the grounds of interception. It adds the excessively broad and vague grounds of 'defence of India' and 'investigation of any offence'. There is also no condition that interception can only occur in the case of public emergency or in the interest of public safety. Even *Section 69B*, *IT Act*, *2000* permits monitoring and collecting data for enhancing cybersecurity,[126] or for preventing the spread of any computer contaminant in India. The main difference between *Section 69B* and *Section 69* is that while the latter requires the interception/monitoring/decryption of only information generated, transmitted, received or stored through a computer resource, *Section 69B* specifically provides a mechanism for all metadata through a computer resource for the purpose of combating threats to "cyber security". This is particularly relevant because metadata allows the generation of 360-degree profiles of users.[127]

The procedural safeguards differ under the *Indian Telegraph Rules*, *1951 (the Telegraph Rules)* and the *IT Act*, *2000* and its *2009 Rules*. They are broadly expressed in terms of: (1) the competent issuing authority and scope for exemptions: *Rules 419A*, *Telegraph Rules* requires the order to be issued by the secretary in the Ministry of Home Affairs or secretary to the state government in-charge of the home department, as the case may be. But in unavoidable circumstances, orders can be issued by an officer not below the rank of a joint secretary, who has been authorised by either the Union or State Home Secretary, as the case may be. Since the *IT Act* is a union legislation, *Section 69* and *Section 69B* only empowers the Secretary to the Ministry of Home Affairs and the Secretary of the Department of Information Technology respectively; (2) existence of an oversight mechanism: *Rule 419A*, *Telegraph Rules* mandate the creation of a Review Committee with the Cabinet Secretary as its chairman and the Secretary to the Government in charge of Legal Affairs and the Secretary to the Department of Telecommunications as its members. This committee's oversight powers also extend to the orders issued under *Section 69* and *69B*, *IT Act*, *2000*. The requirement is for orders under either statute to be placed before this committee within 7 days of issuance. The committee itself is obligated to meet at least once every two months to validate the orders, and can even revoke orders or destroy copies of intercepted messages; (3) disclosure requirements: *Under Rule 419A*, *Telegraph Rules* and the *IT Rules*, *2009*, service providers are required to maintain the secrecy and confidentiality of the intercepted information and directions for interception. But there is no specific prohibition on disclosing the number of surveillance orders issued in aggregate.[128] Additionally, *the IT Rules*, *2009* also require a stipulation of the reasons and duration of interception orders alongside a prohibition of disclosure to unauthorised persons;[129] and (4) existence and type of remedies: for unlawful interception, *Section*

---

[124] (2017) 7 SCC 157

[125] (2019) 1 SCC 1

[126] The term 'cyber security' has been defined in section 2(nb), IT Act as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction."

[127] 'Explainer: WhatsApp Privacy Policy Changes' (*Internet Freedom Foundation*, 11 January 2021) <https://internetfreedom.in/explainer-whatsapp-privacy-policy-changes-2021/> accessed 19 August 2021.

[128] 'State of Privacy India' (*Privacy International*, 26 January 2019) <https://privacyinternational.org/state-privacy/1002/state-privacy-india> accessed 28 March 2021.

[129] Rishab Bailey, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman, 'Use of personal data by intelligence and law enforcement agencies' (2018) Data Governance, 7 <https://www.datagovernance.org/files/research/BBPR2018-Use-of-personal-data.pdf> accessed 28 March 2021.

24, *Telegraph Act* stipulates a penalty of up to Rs 500 and imprisonment of up to one year. Under the *IT Rules*, *2009*, unlawful interception is prohibited, but since there is no specific penalty, the catch-all penalty under *Section 45*, *IT Act*, *2000* applies, which is fines not exceeding Rs. 25,000.

From the above analysis, it is clear that present surveillance systems in India suffer from two main limitations. First, the legal framework is designed to confer broad mandates to intelligence agencies, without adequate legal and procedural safeguards for protecting civil liberties. The Review Committee is designed ineffectively since its composition ensures that the authority issuing the interception order and the one which exercises oversight share the same incentives. There is total non-transparency since in practice service providers interpret the requirement of secrecy to extend to aggregate information regarding interception orders.[130] Second, it is blind to the reality of the state's capacity in carrying out surveillance functions. This issue is compounded due to the large volumes of surveillance data that are collected, and the insights that are gathered from them.[131] These concerns are exacerbated given the emergence of modern technologies that increase both the extent and frequency of surveillance as well as the covertness of undertaking it. This was epitomised in the context of the Pegasus Spyware, which is a zero-contact spyware that uses the device's cameras and microphones for surveillance.[132] The central government's inadequate response, in terms of not issuing a comprehensive response or constituting a specialised public body for enquiry, in spite of the scale and nature of harm impugned against it demonstrates the lack of any practical safeguards for surveillance.[133]

D. Intermediary Regulation

Online social media platforms reflect a growing need for intermediary regulation. Different kinds of harmful behavior and practices over the internet have called for urgent attention and regulation. There are three broad categories of legal harm for which some statutory duty of care and positive monitoring obligations stand concomitant.[134] International conventions and national guidelines outline harms with a clear definition (such as terror content, child-sexual exploitation, hate crime and incitement of violence, harms with less clear definition (cyberbullying, coercive behavior, hate crimes, incitement of violence), and underage exposure to legal content.[135] These harms manifest themselves on social media platforms, customer feedback sections, open public forums, online communities, listing sites, cloud hosting providers, messaging services and search engines.[136] A general definition of an online harm may be a content or activity which violates certain parameters of care, and harms certain persons with varying degrees of severity. The United Kingdom in 2019 released an *Online Harms White Paper* which set out appropriate actions to prevent bullying, insulting, intimidating and humiliating behavior.[137]Particularly, it highlighted certain damaging content that included sexual exploitation and

[130] 'State of Privacy India' (*Privacy International*, 26 January 2019) <https://privacyinternational.org/state-privacy/1002/state-privacy-india> accessed 28 March 2021.

[131] Bailey (n 130) 4-5.

[132] Nandagopal Rajan, 'Explained: Pegasus uses 'zero-click attack' spyware; what is this method?' (*The Indian Express*, 3 August 2021) <https://indianexpress.com/article/explained/zero-click-attacks-pegasus-spyware-7411302/> accessed 19 August 2021.

[133] Apar Gupta and Vrinda Bhandari, 'Many snooping questions: Official response to Pegasus must be clearer. Plus, system of authorising surveillance is flawed' (*The Times of India*, 19 July 2021) <https://timesofindia.indiatimes.com/blogs/toi-edit-page/many-snooping-questions-official-response-to-pegasus-must-be-clearer-plus-system-of-authorising-surveillance-is-flawed/> accessed 19 August 2021.

[134] Mark Owen and Louise Popple, 'Online harms: the regulation of internet content' (*Taylor Wessing*, 1 October 2019) <www.taylorwessing.com/download/article-online-harms.html#> accessed 30 March 2021

[135] ibid.

[136] ibid.

[137] Department of Digital, Cultural, Media and Sport And Home Office, 'Online Harms White Paper' (*GOVUK*, April 8th, 2019) <https://www.gov.uk/government/consultations/online-harms-white-paper> accessed March 30 2020

abuse,[138]terrorist content,[139] cyberattacks,[140] and hate speech.[141] The Indian Supreme Court had struck down *Section 66A of the Information Technology Act, 2000*, which prohibited speech causing "annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will", as unconstitutional.[142] One of the crucial points in the judgement remained that it is difficult to absolutely define, and subsequently apply, statutory prohibited activities. This lack of boundaries risks arbitrariness in content takedowns. Intermediary guidelines may often be at the expense of users' rights, and intermediaries have no choice but to be amenable, lest they lose protection from third party liability.

The drafting, dissemination and enforcement of community guidelines call for participation of all stakeholders, much like legislature drafting and public policy.[143] Since India is an active statistical, research and analytical partner of OECD committees and subsidiaries,[144] referring to the OECD regulatory checklist, the Indian government demands certain key caveats which include the requirement that all accounts must be created and operated in official capacity only; a responsiveness criteria to be defined and a dedicated team to be put in place to monitor and respond as a social media demands 24x7 interactions; a congruence between responses on social media and traditional media; adherence to relevant provisions of *IT Act 2000* and *RTI Act*.[145] It also calls for a framework of regulation which respects the government-intermediary dynamics, the challenges which online platforms have to face and the values they propagate.[146] However, the ground reality confronts inconsistencies abound. Facebook refused to take down a damaging, doctored video of the United States House Speaker Nancy Pelosi in 2020, merely flagging to do even that properly with the content which was watched and shared for over two million times.[147]In 2019, the People's Union for Civil Liberties, filed a petition in the Indian Supreme Court, where it implored the court to take cognizance of the fact that the *Section 66A*, *IT Act*, a provision which was struck down in *Shreya Singhal*, has been used to register thousands of FIRs across states. The persistence of *Section 66A* criminalised messages on platforms deemed "offensive" on vague grounds, having a chilling effect on free speech.[148]

Pertinently, online platforms have enormous capacity for information dissemination and their users reciprocate with a similar appetite for consumption. A study suggests that falsehoods spread faster, deeper and farther as compared to other categories of information.[149] The Rohingya Massacre, the US Capitol Riots, lynching incidents in India are a few instances which revealhow vile social media can be when used as a destructive machinery. To hold the internet intermediaries vicariously liable in the event of every online offence is unpragmatic. The *Information Technology (Intermediaries Guidelines) Rules 2011* did not specify any consequences

---

[138] U.S. Department of Justice, 'Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse' (*US Department of Justice*) <www.justice.gov/opa/press-release/file/1256061/download> accessed 30March 2021

[139] United Nations Office on Drugs and Crime, 'The use of the internet for terrorist purposes' (*UNODC*) <www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> accessed 30 March 2021

[140] IBM Services, 'What is a cyber attack?' (*IBM*, 1 December 2020) < www.ibm.com/services/business-continuity/cyber-attack> accessed 30 March 2021

[141] Law Commission of India, *Hate Speech* (Law Com No 267, 2017)

[142] AIR 2015 SC 1523

[143] Ortwin Renn and others, 'Public participation in decision making: A three-step procedure' (1993) 26 Policy Sci 189

[144] THE OECD REFERENCE CHECKLIST FOR REGULATORY DECISION-MAKING (Organisation for Economic Co-operation and Development 2021) <https://www.oecd.org/gov/regulatory-policy/35220214.pdf> accessed 31 March 2021.

[145] Department of Electronics and Information Technology, Ministry of Communications & Information Technology Government of India, 'Framework & Guidelines For Use Of Social Media For Government Organisations' (2020).

[146] ibid.

[147] The Guardian, 'Facebook Refuses To Remove Doctored Nancy Pelosi Video' (*The Guardian*, 3 August 2020) <https://www.theguardian.com/us-news/2020/aug/03/facebook-fake-nancy-pelosi-video-false-label> accessed 31 March 2021.

[148] WRIT PETITION (CRIMINAL) NO. 199 OF 2013, Supreme Court

[149] Peter Dizikes, 'Study: On Twitter, false news travels faster than true stories' (*MIT News*, 8 March 2018) <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> accessed 30 March 2021

for non-compliance with regulation guidelines, but the *2021 Rules* envisage potential criminal prosecution under the provisions of the *IT Act* and the *Indian Penal Code*, in the event that safe harbor is withdrawn.[150]

Intermediary Regulation in the Current Indian Landscape

Intermediary platforms lend to the country's social, political, cultural and economic reality, making their proper regulation critical.[151] Government intervention which takes care of user rights and strikes a balance between preemptive and troubleshooting measures is imperative. The Ministry of Electronics and Information Technology (MeitY) notified the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*; *Part II* of which provides for due diligence by intermediaries, along with a redressal mechanism.[152] *Rule 3(1)* of the said rules deal with due diligence while *Rule 3(2)* provides for a grievance redressal mechanism to be adopted by an intermediary. However, an analysis of these rules reveals that they leave ample space for discriminatory behavior by authorities. Broad terms such as "significant social media intermediary" and "material risk of harm" bode well for arbitrariness.[153] Even though reasonable restrictions on internet news media exist, the rules seem to expand the grievance redressal mandate over to online news content. This could result in unnecessary roadblocks for online publishers and an attack on freedom of speech and expression.[154]Another troubling provision of the new rules require user data, even from deleted accounts, to be stored for six months. Stored data ought to be retained for the investigative purposes, this borderline surveillance exercise lacks proper regulation.[155]

The *PDP Bill* posits that users need to mandatorily verify their user IDs when they sign in to platforms. It is noteworthy that targeted advertisements provide the largest share of revenue for intermediaries, pursuant to which collection of user data is routine. It is an alarming blow to privacy and freedom of speech and expression that this data could now be traced to a verified user ID.[156] It is suggested[157] that the set of *2021 Rules* could adapt provisions which ensure better protection and accountability. These would include having a robust procedure surrounding data sharing with legal authorities, to keep the state from undertaking mass data surveillance.[158] Further, the stipulated period of storage must be limited and categories specified must follow from intelligible differentia.[159] Measures should be in place which call for accountability, sensitivity and practicality must be taken, at the intermediary level. Reminding the user to not do anything "illegal" with periodic terms and services notification will result in little improvement.[160] Additionally, an expert panel would be better suited to engage

---

[150] Tariq Khan, 'SAFE HARBOURS: A MIRAGE OF INTERMEDIARY PROTECTION' (*RGNUL Student Research Review*, 21 October 2020) <http://rsrr.in/2020/10/21/safe-harbours-and-intermediary-liability/> accessed 30 March 2021

[151] ibid.

[152] 'Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (*Press Information Bureau*, 25 February 2021) <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1700749#:~:text=Amidst%20growing%20concerns%20around%20lack,in%20exercise%20of%20powers%20under> accessed 30 March 2021.

[153] 'Deep dive: How the intermediaries' rules are anti-democratic and unconstitutional' (*Internet Freedom Foundation*, 27 February 2021) <https://internetfreedom.in/intermediaries-rules-2021/> accessed 30 March 2021.

[154] ibid.

[155] Jyoti Panday, 'The Supreme Court Judgment in Shreya Singhal and What It Does for Intermediary Liability in India?' (*Centre for Internet and Society*, 11 April 2015) <https://cis-india.org/internet-governance/blog/sc-judgment-in-shreya-singhal-what-it-means-for-intermediary-liability> accessed 28 March 2021

[156] Mathew (n 116).

[157] 'Deep dive: How the intermediaries' rules are anti-democratic and unconstitutional' (*Internet Freedom Foundation*, 27 February 2021) <https://internetfreedom.in/intermediaries-rules-2021/> accessed 30 March 2021.

[158] 'Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?' (*Internet Freedom Foundation*, 25 February 2021) <https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/> accessed 28 March 2021

[159] 'What is GDPR, the EU's new data protection law?' (GDPR) <https://gdpr.eu/what-is-gdpr/> accessed 30 March 2021

[160] Rishabh Dara, 'Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011' (*Google Policy Fellowship*, 2011) <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf> accessed 26 March 2021

directly with social media entities, instead of the ex-officio authorities of the Ministry of Home Affairs.[161] Lastly, the consent obtained from data subjects must be done in elaborate, yet lucid language. The netizen must not be kept in the dark about how their information is processed.[162] In *Shreya Singhal v. Union of India*,[163] the Supreme Court categorically held that any intermediary has to takedown unlawful content after receiving an order from the court or appropriate government. Thereafter, the government of India recently enacted *2021 Rules* which superseded the *2011 Rules*.[164] These rules have significantly broadened the scope of government oversight and control over online intermediaries and have also expanded the radar to include digital news and OTT streaming services under the *2021 Rules*.[165] The new rules are broad, stringent and threaten the safe harbour provisions recognised globally. They also put an obligation on intermediaries to be transparent about their grievance mechanism and release reports regarding any grievance made and how they have been solved.[166] These reports have to be released twice a year.

Understanding Problematic User-generated Content

There is no clear definition or understanding of user-generated content in India. However, the understanding of the same can be arrived at after breaking down the definition of user, user account and content. As per the *2021 Rules*, the term user refers to 'any person who accesses or avails any computer resource of an intermediary or a publisher for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information and includes other persons jointly participating in using such computer resource and addressee and originator.'[167] Further, user account is defined as 'the account registration of a user with intermediary or publisher and include profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher.'[168] Similarly, content is not clearly defined but can be understood to be any electronic record,[169] made available to users of computer resources through the internet or any other computer resource.[170] However, in addition to this, the Indian legal framework also mentions the 'originator of a content', which is quite relevant to understand the parameters determining user generated content. The originator of any content is only relevant in the case of false or misleading news. The originator of the content is any user, which could include a person but may also include accounts, pages, handles, who first communicated any information.

Addressing Fake News

The term fake news has been used very loosely in recent times. It is interchangeably applied in satire, biased news reporting, propaganda, etc. There is also no clarity on whether this term is applied to private communications, social media, online media or traditional print media.[171] Currently, words like inaccurate, false, misleading, biased, etc. are used to describe the term "fake news". However, it has been suggested that an exact term to identify the issue with a piece of content would allow us to create targeted as well as meaningful solutions

---

[161] ibid.

[162] ibid.

[163] Shreya Singhal v. Union of India [(2015) 5 SCC 1

[164] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

[165] Raghav Mendiratta, 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021' (*World Intermediary Liability Map*, March 26 2021) <https://wilmap.law.stanford.edu/entries/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> accessed 26 April 2021

[166] Torsha Sarkar, 'New intermediary guidelines: The good and the bad' (*Down to Earth*, 26 February 2021) <https://www.downtoearth.org.in/blog/governance/new-intermediary-guidelines-the-good-and-the-bad-75693> accessed 26 April 2021

[167] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 2(x).

[168] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 2(y).

[169] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 2(g).

[170] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 2(u).

[171] V. Vasudevan, '"Fake News" and the Constitution' (*Indian Constitutional Law and Philosophy*, 17 June 2020) <https://indconlawphil.wordpress.com/2020/06/17/fake-news-and-the-constitution/> accessed 9 August 2021

in place of using an umbrella term.[172] Most importantly,India does not have a "fake news" legislation yet and relies on the Indian Penal Code to address concerns relating to fake news.

Social media platforms are vulnerable to abuse by actors who may misuse the platform to spread misinformation and hateful, inappropriate content. Regulatory mechanisms are therefore required to align the utility of online platforms with the welfare of citizens, while safeguarding the right to free speech.[173] The misuse of such platforms can lead to economic, psychological and social forms of harm, both online and offline.[174] They can also lead to discrimination and violence.[175] As per a recently published index, Indian citizens are most likely to encounter misinformation online.[176] Fake news has resulted in episodes of violence and hatred. A recent example is of the early reporting of the pandemic in India which tended to generalise Indian Muslims as willful carriers of the coronavirus.[177] While there is no specific provision that addresses fake news, there are different provisions which together form the criminal jurisprudence of fake news in India. These include *Indian Penal Code* provisions on sedition, promotion of religious enmity, defamation, public mischief, criminal intimidation, etc.[178] Similarly, the *Information Technology Act* discusses cybercrime offences under *Chapter XI of the Act*.[179] One particular provision, *Section 66A* was earlier applied in cases pertaining to fake news, the same was struck down by the Supreme Court in the year 2015.[180] The Indian Ministry of Electronics and Information Technology (MeitY) has recognised and addressed the issue of potential misuse of platforms and touched upon the problem of disinformation.[181] However, despite such an elaborate statement, the term has not yet been adopted under the *IT Act* or any provisions of the penal code. As a consequence, there is a dearth of precedents available in cases pertaining to fake news. Fact-checking and restricting inflammatory/fake content has become a necessity. For instance, Facebook has been accused of "ideological bias" in India by both left-wing and right-wing groups.[182] So much so that the former union minister for Information Technology has labelled the website as "inherently biased" against people who support right-leaning ideology and has referred to it as the "latest tool to stoke internal divisions and social disturbances."[183] Further, a group of Facebook employees who identify themselves as Muslims wrote an open letter to the Facebook administration in 2020 demanding transparency in taking down

---

[172] ibid.

[173] A. Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change' (2021) Observer Research Foundation, Occasional Paper No. 296 https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/ accessed 27 March 2021.

[174] Annie Gowen and Manas Sharma, 'Rising Hate in India' (*The Washington Post*, 31 October 2020) <https://www.washingtonpost.com/graphics/2018/world/reports-of-hate-crime-cases-have-spiked-in-india/> accessed 28 March 2021

[175] J. Weinstein, *Hate Speech, Pornography, And Radical Attacks on Free Speech Doctrine* (Routledge 1999)

[176] Microsoft, 'Microsoft Releases Digital Civility Index on Safer Internet Day,' (*Microsoft News Center India*, 5 February 2019) <https://news.microsoft.com/en-in/microsoft-digital-civility-index-safer-internet-day-2019/> accessed 28 March 2021.

[177] J. Bajoria, 'Corona Jihad is Only the Latest Manifestation: Islamophobia in India has been years in the making' (*Human Rights Watch*, 1 May 2020) <https://www.hrw.org/news/2020/05/01/coronajihad-only-latest-manifestation-islamophobia-india-has-been-years-making> accessed 28 March 2021.

[178] Indian Penal Code 1860, ss 124A, 153A, 499, 425 and 503.

[179] Information Technology Act 2000, ch XI.

[180] (2015) 5 SCC 1

[181] Anirudh Sunilkumar, 'Government Defines 'Fake News' in Parliament; Says Social Media Being Used for Weaponisation of Information' (*Republic World*, 26 July 2018) <https://www.republicworld.com/india-news/general-news/government-defines-fake-news-in-parliament-says-social-media-being-used-for-weaponisation-of-information.html> accessed 28 March 2021

[182] Press Trust of India, 'Parliamentary panel to discuss Facebook issue on Wednesday' (*Economic Times*, 1 September 2020) <https://economictimes.indiatimes.com/news/politics-and-nation/parliamentary-panel-to-discuss-facebook-issue-on-wednesday/articleshow/77876060.cms?from=mdr> accessed 28 March 2021

[183] India Today Web Desk, 'Ravi Shankar Prasad writes to Mark Zuckerberg, accuses Facebook India of bias: Full text of letter' (*India Today*, 1 September 2020) <https://www.indiatoday.in/india/story/ravi-shankar-prasad-writes-to-mark-zuckerberg-accuses-facebook-of-bias-full-text-of-letter-1717521-2020-09-01> accessed 28 March 2021

content. The group also questioned why anti-Muslim and hateful content continued to find space on their platform.[184]

A four-step model is recommended for online platforms to counter fake news.[185] This includes (i) Identifying fake news as per the definitions or elements that address local terminologies as well. While upholding anonymity, the platform must flag it in a specific manner which communicates its problematic/unreliable nature to the end-user; and disallow proliferation. While the content may continue to exist online, it should not only be flagged but platforms should disable any type of proliferation further, which includes content's algorithmic prioritization. (ii) Any blatantly problematic content should not be promoted for interactions, i.e., such content should not be available on user feeds; issuing interaction warnings, since platforms employ interaction data, they must issue warnings to all end-users who have encountered problematic content before it was flagged or identified. (iii) All end-users who shared or promoted such content must be sent personal notifications on the respective platforms, about the problematic nature of the content. Similarly, the publishing end-user must be provided with necessary reasons for flagging or taking down the published content; and lastly, providing better recourse mechanisms in terms of reporting fake content, platforms should be user-friendly with timely action and response. (iv) Recourse against wrongful takedowns should be formalised and direct end-users to such mechanisms if their content is taken down. In addition to these steps, there is a growing need for general awareness being raised against fake news across social media platforms. Platforms have come up with creative mechanisms to explain the new features and functioning to their users over the past few years and the same mechanisms could be put to use in informing the users about potential fake news being circulated and how to act against it following the steps mentioned above.

There have been several platforms, experts and politicians who suggest government-led moderation of illicit content with different mechanisms to place checks and balances against arbitrary imposition.[186] However, the same has come under a lot of skepticism by human rights groups and activists as they are not confident or do not perceive the governmental intervention to be safe and unbiased because of potential scope for arbitrary imposition of bans, content moderation and internet shutdowns.[187]A hybrid system of government-led regulation and self-regulation currently exists in India with up to 17,444 websites being blocked for promoting obscene content until 2019 by the IT Ministry.[188] However, in this system, there has been very little space offered to the non-state actors and academics who may provide considerable assistance in filtering out fake and misleading information while ensuring that no biases or prejudices creep in. It is suggested by the authors that an objective criterion be developed which can adequately identify fake or misleading information being circulated by certain metrics such as authenticity, relevance, background source amongst others which can then be referred to the government regulators for blocking. Twitter had taken down 6,36,248 accounts in 2015-16 alone for disseminating extremist content worldwide.[189] The Covid-19 pandemic has resulted in another case study for

---

[184] ET Bureau, 'Muslim staffers at Facebook call for transparency in enforcing policies' (*Economic Times*, 22 August 2020) <https://economictimes.indiatimes.com/tech/internet/muslim-staffers-at-facebook-call-for-transparency-in-enforcing-policies/articleshow/77686338.cms> accessed 29 March 2021

[185] A. Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change,' (2021) Observer Research Foundation, Occasional Paper No. 296, <https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/> accessed 27 March 2021.

[186] Ajita Shashidhar, 'Think beyond sex and abuse': Netflix, Amazon Prime, other OTT platforms state at a new challenge' (*Business Today*, 11 November 2020) <https://www.businesstoday.in/latest/trends/story/govt-regulation-on-netflix-amazon-prime-to-hamper-freedom-of-storytelling-278382-2020-11-11> accessed 28 March 2021; Amrita Nayak Dutta, 'Javadekar notes absence of self-regulation by OTT platforms, says looking into suggestions' (*The Print*, 16 November 2020) <https://theprint.in/india/governance/javadekar-notes-absence-of-self-regulation-by-ott-platforms-says-looking-into-suggestions/545448/> accessed 29 March 2021

[187] A. Obhan and B. Bhalla, 'India: OTT Platforms Brought Under Government Regulation" (*Mondaq*, 19 November 2020) <https://www.mondaq.com/india/broadcasting-film-tv-radio/1007300/ott-platforms-brought-under-government-regulation> accessed 28 March 2021.

[188] Krishnanand Tripathi, 'More than 17,000 websites blocked for spreading obscene content, violating India values' (*Financial Express*, 13 February 2019) <https://www.financialexpress.com/industry/technology/the-list-of-websites-blocked-by-the-government-for-spreading-obscene-content/1486743/> accessed 29 March 2021

[189] BBC News, 'Twitter shuts 3,77,000 "terrorism" accounts' (*BBC News*, 22 March 2017) <https://www.bbc.com/news/technology-39351212> accessed 29 March 2021

Indian jurisprudence and regulating authorities; this can prove to be instrumental in filling the ethical-legal gap that currently exists. The prevalence of fake news and harmful online content necessitates amending our understanding of online harms and the ill-effects they carry. Scholars recommend accountability and transparency, consistency and collective will, respect for human rights and legal certainty to address this.[190] There is a need for continuous collaborative engagements within the online industry, along with state and non-state actors enabling the creation of voluntary multi-platform and multi-stakeholder initiatives. Some recommendations, in addition to the ones discussed above, are adequate definitions, legislative support, and improvement in social media infrastructure.

Revisiting the Global Intermediary Ecosystem

There is a need to balance the need for comprehensive legislations whilst also allowing for greater control for case or user-specific policy-making. This can be operationalised through a principles-based regulatory approach, wherein broad contours are expressed in the statute but specific 'codes of practice' are developed by regulators, acting under statutory empowerment.[191] However, this requires the immunities for regulators because the fear of ex-post facto sanction may hamper policy-making. Borrowing from corporate law, we can apply the standard of 'best judgement' to their actions. This ensures a rebuttable presumption of good faith and correctness to their actions.[192] But this extent of immunity must be contingent on transparency, where regulators are mandated to exhaustively list applicable regulations on their website and enforce only those.[193]

Regulators must shift towards regulating digital platforms through interventions in the design of the architecture of the platform or the internet so as to achieve intended regulatory outcomes.[194] There are at least three such useful architectural interventions that can be used. First, there is scope for enforcing contractual obligations through code. This ensures automated compliance in an impartial manner through hard-wiring performance into the platform. The potential for usage also extends to complex highly-scalable multi-party transactions that would have otherwise been impossible.[195] Second, the virality tools of digital platforms, which popularize the content, can be inverted such that it dampens offensive content instead of taking it down entirely. In fact, this is a more proportionate response since the availability of the content ensures platforms are not actually violating freedom of speech.[196] Third, regulators can develop prohibited content dashboards to operationalise a list of permissible and impermissible content, which platforms can then bake into their tools and filters.[197] This is similar to the 'doctrine of autoblock' developed by the Supreme Court in *Sabu Mathew George v. Union of India (2017)*. This required search engines to develop a list of keywords relating to pre-natal sex determination, and then pre-emptively block access to advertainments which contained these. This ex-ante

---

[190] A. Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change,' (2021) Observer Research Foundation, Occasional Paper No. 296, <https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/> accessed 27 March 2021

[191] Rahul Matthan, 'A Three Point Plan to Improve Tech Policy Formulation' (*LiveMint*, 16 July 2019) <https://www.livemint.com/opinion/columns/opinion-a-three-point-plan-to-improve-tech-policy-formulation-1563296823102.html> accessed 28 March 2021

[192] Rahul Matthan, 'Principle Based Regulations' (*Ex Machina*, 4 February 2021) <https://exmachina.substack.com/p/principle-based-regulations> accessed 28 March 2021

[193] ibid.

[194] Rahul Matthan, 'Contract as Code' (*Ex Machina*, 11 November 2020) <https://exmachina.substack.com/p/contract-as-code> accessed 28 March 2021

[195] ibid.

[196] Rahul Matthan, 'Moderating with Moderation' (*Ex Machina*, 28 October 2020) <https://exmachina.substack.com/p/moderating-with-moderation> accessed 28 March 2021

[197] Rahul Matthan, 'Gatekeepers at the Edge' (*Ex Machina*, 20 January 2021) <https://exmachina.substack.com/p/gatekeepers-at-the-edge> accessed 28 March 2021

approach imposes 'constructive knowledge' on the platforms, which is a more effective way of determining the responsibility of platforms, rather than case-to-case assessments.[198]

Analyzing Guidelines of Online Platforms

The specific guidelines for content moderation have been laid down in the *IT Rules, 2021*. Under *Rule 2(v)-(w)*, a distinction is made between a 'significant social media intermediary' and a 'social media intermediary' based on a notified threshold users of 5 million, to be notified by the government. Under *Section 79 of the IT Act*, an intermediary is exempted from liability if inter alia they observe due diligence and other guidelines, stipulated by the government, while discharging their duties. Subsequently, these due diligence guidelines for social media intermediaries were issued under *Rule 3* and some additional ones for significant social media intermediaries under *Rule 4 of the 2021 Rules*. Under *Rule 4(4)*, significant social media intermediaries are obligated to "deploy technology-based measures, including automated tools or other mechanisms to proactively identify information", whether explicit or implicit, depicting rape, child sexual abuse or conduct. It also extends to information which has been removed/disabled under *Clause (d) of Sub-rule (1) of Rule 3*, i.e., for violating the interests of the sovereignty and integrity of India: the security of the state; friendly relations with foreign states; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence, or information which violates any law for the time being in force.

However, the mandatory deployment of AI-based tools and their scope of usage is problematic. Presently, it is being used not only for sexual content but also for all the general conditions of moderation stipulated in *Rule 3(1)(d)*. Development of AI tools of censorship is replete with a host of risks, including the underdeveloped and imperfect nature of AI in the current state-of-the-art. AI tools learn by examining vast amounts of data, and the development of a censorship AI is likely to require social media intermediaries to store and examine large amounts of user-generated content that does not in any way relate to the kind of content sought to be censored. Additionally, coding biases in the development of AI often lead to discrimination, over-breadth and a lack of accountability and transparency. This is of particular concern since the AI seeks to control and monitor the exercise of a user's fundamental right to freedom of speech and expression. It is necessary to carefully consider whether AI ought to be allowed to regulate the fundamental rights of citizens.[199]

Role of Community Guidelines

It is evident that the community guidelines play an important role in moderating content and serves as the first source of reference when a complaint is made to remove objectionable content. But it is necessary that these guidelines are representative of the laws and demographics of the country. To fill the void, social media platforms must draft community guidelines based on the Constitution of India and laws of the land. The guidelines need to incorporate legal changes, judicial pronouncements but also adapt to the social dynamics of India. While assessing whether content posted by a user violates community guidelines, the content moderation team considers the situation in India and whether the post is violative of Indian laws. For example, the Facebook Oversight Board has representatives from India which interpret the community standards of Facebook in Indian context while moderating user generated content.[200] Similarly, a new article by Washington Post Journal reports that Facebook recently sent researchers to investigate the role of inflammatory content posted on its website in instigating sectarian violence.[201] The report also suggests that Facebook and Whatsapp have been used to spread hate, rumors and call for violence in February 2020 when the communal riots occurred in some parts of India. India is Facebook's largest market and the content moderation team have been concerned about flagging content of

---

[198] Varun Sen Bahl, Faiza Rahman andRishab Bailey, 'Internet intermediaries and online harms: Regulatory Responses in India' (2020) Data Governance Network Working Paper 6, 52 <https://datagovernance.org/files/research/BahlRahmanBailey_-_Paper_6-2.pdf> accessed 28 March 2021

[199] 'Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?' (*Internet Freedom Foundation*, 25 February 2021) <https://internetfreedom.in/latest-draft-intermediary-rules-fixing-big-tech-by-breaking-our-digital-rights/> accessed 28 March 2021.

[200] Meet the Board (Oversight Board) https://oversightboard.com/meet-the-board/ accessed on 30 July 2021

[201] Newley Purnell and Jeff Horwitz, 'Facebook Services Are Used to Spread Religious Hatred in India, Internal Documents Show' (*Wall Street Journal*, 23 October 2021) <www.wsj.com/articles/facebook-services-are-used-to-spread-religious-hatred-in-india-internal-documents-show-11635016354> accessed 25 October 2021.

groups associated with the ruling party due to fear of witch-hunting.[202] Facebook is aware about its role, but has not done enough to prevent the harm. Social media companies use sophisticated technology to actively regulate sexually explicit content, nudity, child pornography on their platforms but they have not done enough to prevent the spread of hate speech and misinformation that may lead to instigation of violence.

Every social media intermediary is bound by law to inform their users about the rules and regulations, privacy policy and user agreements for access or usage of its computer resource.[203] This includes information that the user may not host, display, upload, modify, publish, transmit, store, update or share. Social media platforms provide information on their websites but do little to educate users.

However, it is imperative to note, as highlighted by a report published by NYU Stern Centre for Business and Human Rights, that even as content moderation is pivotal to the functioning of Facebook, the task is delegated to underpaid, secondary actors in remote locations.[204] Facebook's outsourcing of content moderators who have little financial or health security is termed as 'grossly inadequate'. There remains a lack of juxtaposing the ambition to grow as a business, with a tactical strategy which ensures that content isn't being misused. The report also acknowledged that all social media platforms have problems similar to Facebook when it comes to content moderation.

Additionally, every social media intermediary is bound by law to inform their users about the rules and regulations, privacy policy and user agreements for access or usage of its computer resource.[205] This includes information that the user may not host, display, upload, modify, publish, transmit, store, update or share.

Regulating Sponsored Content Online

There have been talks between the industry, state and non-state actors of sharing the responsibilities between the stakeholders. However, limited action has been taken to counter the online harms that take place.[206] The existing online platforms have deployed very little resources to take down blatantly illegal content, a large reason for this is that the platforms lack real-time local responders who are well-versed in Indian languages.[207] Another reason is that the community guidelines for these online platforms are uniform across different countries and therefore, they have limited implementation value at a local stage. Parallel to this is the lack of definitions for understanding local online harms. Therefore, it is pertinent to have the government and tech platforms complement each other's information gatekeepers like the media and the politicians.

It is suggested that the final arbiter should comprise a mix of the stakeholders which include the industry, state and non-state actors. A move in this direction is the *Voluntary Code of Ethics* by social media platforms which was introduced by the Election Commission of India in 2019.[208] This involved the Internet & Mobile Association of India along with popular social media platforms like Facebook, Whatsapp, Twitter etc. which observed this code during the election and ensured that free and fair elections were conducted. This was to be done by undertaking information, education and communication campaigns, creating dedicated grievance redressal mechanisms, creating notification mechanisms to notify relevant platforms of potential violations of electoral

---

[202] Regina Mihindukulasuriya, 'Facebook research flagged "inflammatory content" against Muslims in India, says WSJ probe' (*The Print*, 24 October 2021) <theprint.in/tech/facebook-research-flagged-inflammatory-content-against-muslims-in-india-says-wsj-probe/755878/> accessed 25 October 2021

[203] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3.

[204] Paul M. Barett and J Grant Sims, '*False Accusation : The Unfounded Claim That Social Media Companies Censor Conservatives*' (*Centre for Business and Human Rights, NYU Stern*, February 2021) <https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/60187b5f45762e708708c8e9/1612217185240/NYU+False+Accusation_2.pdf> accessed 22 October 2021

[205] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rule 3.

[206] Megha Mandavia, 'Social Media to Join Hands to Fight Fake News, Hate Speech' (*The Economic Times*, 19 February 2020) <https://economictimes.indiatimes.com/tech/internet/social-media-to-join-hands-to-fight-fake-news-hate-speech/articleshow/74200542.cms> accessed 29 March 2021

[207] Z. Laub, 'Hate Speech on Social Media: Global Comparisons' (*Council on Foreign Relations*, 7 June 2019) <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons> accessed 28 March 2021

[208] 'Social media platforms present "voluntary code of ethics"' (The Hindu, 20 March 2019) <https://www.thehindu.com/elections/lok-sabha-2019/social-media-platforms-present-voluntary-code-of-ethics/article26593315.ece> accessed 29 March 2021

laws, ensuring that all political advertisements are certified and in accordance with applicable legal directions.[209] By building a consensus on important elements, the legislature can assist the online platforms to interpret and implement the law in a much more structured manner. A collective approach would discourage a certain set of elected individuals who may often be unaware and ignorant of the law and the digital realm in general and in adjudicating on what is acceptable speech along with avoiding faulty implementation. The Law Commission's report suggests that the scope of regulation should not be limited to "incitement of violence" but also prohibit advocacy of hate; and incitement to hostility or discrimination.[210] Another suggestion is that cohesive definitions should be introduced and should complement the adoption of voluntary codes amongst platforms, the same should update media code and Representation of the People Act against information manipulation during the elections.[211] There should be a strict prevention of potential over-criminalization; the legislature can identify and agree upon key elements to facilitate consensus-building and safety nets around ethical codes. Criminal law should not be the first response but the last resort when state or court intervention is imperative. Sponsored content and political ads should also be mandatorily fact-checked while maintaining directories of promoters, amount paid, and source. The use of inorganic amplification methods like bots to propagate hate agendas must be charged with fines. In cases of severe social impact, penal fines that are proportionate and consistent against repeat offenders must be employed.[212]

E. Conclusion

Despite some systemic hurdles, India has worked on creating a digitally empowered society by ensuring digital services, access, inclusivity, empowerment and bridging the digital divide over the past few years. The country boasts of having a digital profile comprising 1.23 billion Aadhaar cards (digital identification numbers), 1.2 billion mobile phones, 490 million internet subscriptions and a network of 312,000 Common Services Centres.[213]

This also means that there is a great need and scope for efficient digital governance, inclusivity and constant regulation. The issues highlighted in this report reflect certain human and constitutional violations along with ethical, economic and social considerations which need to be addressed. Nevertheless, it is believed that involving various stakeholders and implementing an informed framework can prove to be instrumental in addressing these concerns and making most of the potential that a digital India carries.

[209] Press Information Bureau, 'Voluntary Code of Ethics' by Social Media Platforms to be observed in the General Election to the Haryana & Maharashtra Legislative Assemblies and all future elections' (*Press Information Bureau*, 26 September 2019) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1586297> accessed 8 August 2021

[210] Law Commission of India, "Hate Speech" Law Commission of India, (Report No. 267, 2017).

[211] A. Lohani, 'Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change,' (2021) Observer Research Foundation, Occasional Paper No. 296, <https://www.orfonline.org/research/countering-disinformation-and-hate-speech-online/> accessed 27 March 2021

[212] ibid.

[213] Ministry of Electronics & Information Technology, *India's Trillion-Dollar Digital Opportunity*, Government of India (2019).

ANNEXURE

Questionnaire | Project Aristotle

a. Digital Constitutionalism and Internet Governance

1. What factors can be considered important to ground Digital Constitutionalism in traditional constitutional concepts?
2. How can we define Digital Constitutionalism?
3. What should be the core tenets of a Digital Constitution?
4. How can Digital Constitutionalism present a constitutional model for the people, by the people, and of the people?
5. How can online platforms be made more inclusive, representative, and equal?
6. What role should open-source intelligence (=OSINT: the discipline of assembling and analysing publicly available information) play in the future of our society?
7. Should the Digital Constitution be an integrative model, which draws upon and comprehensively presents standards for specific laws (e.g. antitrust, evidentiary standards etc.) as opposed to grounding ideals? If so, how should it fulfil the responsibilities of a pluralistic enterprise such as this as well as the specific needs of a pluralistic global society?
8. How can competition and antitrust laws of different jurisdictions protect the global market from big-tech domination, and is there a need to?
9. What is the role of regional/grassroots actors as well as inter-judicial cooperation/coordination in the digital ecosystem? Which other mechanism(s) might be more helpful?
10. Can the Digital Constitution present an anchor for the governance of the virtual world similar to a traditional constitutional model or will it always be in flux? Is there a need for constitutional innovation, and if so, in which areas (e.g. the right to be forgotten as a novel right)?
11. How is it possible to harmonise diverse national frameworks in order to achieve a global Digital Constitution?

b. Human and Constitutionally Guaranteed Rights:

1. Which human and constitutionally guaranteed rights do online platforms affect, and how?
2. Who can be defined as a netizen?
3. Who can be classified as a 'bad actor', and can 'bad actors' be netizens?
4. How can we embed within the digital ecosystem approaches which are responsive to the needs of minorities (e.g. ethnic minorities, racial minorities, gender minorities, religious minorities)?
5. How should the digital age of consent be arrived at and what should it be? In pursuance of which child rights should such an age be identified?
6. How should public order be defined for the digital space? Should situations of disorder in the offline world influence the definition and management of public order online, and if so why and when?
7. Should the state be allowed to impose internet shutdowns, slowdowns and communication throttles? What socio-legal rationale could be adopted by states in order to do so?
8. Could the Social Media Councils (SCMs) model, as introduced by Article 19, be reinterpreted on a larger scale, with the purpose of monitoring human rights, within the context of Digital Constitutionalism?

c. Privacy, Information Security, and Personal Data:

1. How do we define personal and non-personal data?
2. What should be the ethical, economic, and social considerations when regulating non-personal data?
3. Should there be a backdoor to end-to-end encryption/Should traceability be enabled to prevent and mitigate instances of online harms? What would the benefits and detriments of the same be?

4. How important is compliance with complex/technical/lengthy data protection and privacy statutes in events of crises (e.g. such as during pandemics, where time is essential)? In that regard, is there a need to provide regulatory sandboxes, and if so what could be the grounding philosophy to shape the rules of control for such ecosystems?
5. According to which principles and regulations should intelligence agencies operate online?

d. Intermediary Regulation:

1. How do we define online harms?
2. How should community guidelines for online platforms be drafted, disseminated, and enforced?
3. To what legal standards of accountability and transparency should online platforms be held, and in what capacity? Can you suggest any mechanisms (judicial, or otherwise) which might be capable of ensuring such a check on the functioning of these platforms?
4. Should online platforms be immune from liability from third-party, user generated content [refer to intermediary liability laws]?
5. What should the parameters to define problematic user-generated content be?
6. Should online platforms moderate 'fake news', and if so, why?
7. Should safe-harbour protections be offered to online platforms, given that the grant of such a protection will come at the cost of fundamental rights (e.g. privacy) of citizens? If affirmative, how should this balance be achieved? [Read with Questions in Part B.]
8. How does the global intermediary ecosystem shift from a post-hoc, harm-prevention lens to a proactive approach towards understanding and regulating technology?
9. Do the guidelines/policies of online platforms account for fallibility of the algorithm and the human content moderators, and if so, to what extent?
10. What role should community guidelines drafted by online platforms play in the governance of user-generated content? How should the terrain of conflict between community guidelines, public policy domestic contexts, and international human rights be negotiated upon?
11. Should the advertisement policies and sponsored content of online platforms adhere to certain standards (e.g. of whether they interfere with the political opinions and elections in a democracy)? If so, who should frame these policies, and who should be the final arbiter?

Institute
for Internet &
the Just Society