

## Digital Constitutionalism: Navigating Governance in The Technological Era

Lekshmi Viswanath

Assistant Professor, Government Law College, Dharmapuri, India

### Article History

Received: 12-Nov-2024  
Revised: 21-Dec-2024  
Accepted: 25-Jan-2025  
Published: 31-Jan-2025

### Keywords

Digital Constitutionalism  
Digital Era  
Digital Technology  
Digital Rights framework  
Constitutional framework

### Abstract

The arrival of the digital era has modernized the realm of anthropoid connection, communication, and information exchange. However, the rapid progress of technology has raised significant worries regarding digital rights, data privacy, and cyber security. These concerns need the implementation of constitutional protections. In this context the concept of 'Digital Constitutionalism' arise proposing a framework that integrates principles of constitutional law with the challenges and opportunities presented by digital advancements. Digital Constitutionalism seeks to establish norms and principles that govern the digital realm, ensuring the shield of essential rights such as privacy, freedom of expression and equality in the digital age. This article delves into the Indian Constitution's approach towards examining the issues posed by the digital sphere. In this article the main framework emphasizes on adapting the existing constitutional principles to encompass digital rights, ensuring that legal protections remain relevant and effective in safeguarding citizen's right in an increasing digitalized world. It explores the laws and legal frameworks in place, as well as their effectiveness in tackling the complexities of this domain.

### Corresponding Author:

Dr Lekshmi Viswanath

Assistant Professor, Government Law College, Dharmapuri, India  
proflekshmi Viswanath@gmail.com

This article is under the [CC BY- NC-ND](#) licenses

Copyright © Journal of Law and Legal Research

Development, available at [www.jllrd.com](http://www.jllrd.com)



## 1. INTRODUCTION

In the modern world, the encroachment of technology has directed to a time of unparalleled connection, fundamentally changing the way individuals communicate, exchange information, engage in commerce, and participate in governing processes. The rapid progress of Information and Communication Technology in this digital era has completely transformed every aspect of human existence. The widespread use of digital platforms, the internet, and the advent of innovative technologies like as big data, artificial intelligence and the internet of things (IOT) have brought about unprecedented levels of ease, efficiency, and innovation<sup>1</sup>. Nevertheless, this digital revolution has also presented several issues and concerns,

including around the preservation of digital rights, data privacy, and cyber security. Digital rights are the expansion of the rights and freedoms that persons have in the physical world to the digital domain. Within this framework, the notion of digital rights comprises a range of elements, such as the freedom to express oneself, the ability to access information, the entitlement to privacy, and the liberty to participate in online activities without any sort of restriction or surveillance. The ability to freely express one's opinions, share information, and engage in debates on digital platforms has become a fundamental aspect of contemporary society, influencing public discourse, activism, and the interchange of ideas<sup>2</sup>. Nevertheless, the unregulated dissemination of information in the digital realm has also sparked apprehensions surrounding the violation of individual privacy

<sup>1</sup> De Gregorio G. *Digital constitutionalism across the Atlantic. Global Constitutionalism*. 2022 Jul;11(2):297-324..

ISSN: 3048-5045; Vol 02 Issue 01; Jan-2025; Pg-15-20

<sup>2</sup> Suzor N. *A constitutional moment: How we might reimagine platform governance. Computer Law & Security Review*. 2020 Apr 1;36:105381.

and safeguarding of data. Data privacy has become a crucial concern in the digital realm, as individuals produce and exchange an excessive quantity of personal data through their online actions. This data is frequently gathered by diverse groups, such as government agencies, corporations, and other users who are worried about its utilization, storage security, and the possibility of it being exploited or misused. Data privacy is a critical feature that involves safeguarding individuals' personal data and their right to govern and protect it from unauthorized access or misuse. In addition, the digital environment is filled with cyber security issues<sup>3</sup>. The linked structure of the digital system, although providing great benefits, also exposes flaws that may be exploited by malevolent individuals. Cyber dangers encompass several malicious activities, including hacking, identity theft, data breaches, ransomware attacks, and cyber espionage. In the digital age, ensuring the security of digital infrastructures and information systems has become a crucial and topmost priority.

In the context of India, a nation seeing fast growth in its digital presence and a flourishing digital economy, these concerns become increasingly relevant. The Indian Constitution is a crucial document that governs the country and establishes its legal framework. It plays a vital role in addressing concerns related to digital rights, data privacy, and cyber security. The provisions of the Constitution, especially those concerning vital rights and Directive principles, are essential in defining the boundaries of these issues within the country's legal framework. This research study seeks to analyze the Indian Constitution's reaction to these problems and evaluate the effectiveness of its provisions in dealing with the complications brought about by the digital era. The analysis will examine the constitutional framework, legal precedence, and current legislation to assess how India deals with digital rights, data privacy, and cyber security concerns within its constitutional scope. Furthermore, this paper will pinpoint deficiencies and propose areas of study for a more all-encompassing strategy to protect digital rights and privacy, while strengthening cybersecurity measures in India.

### **1.1 Digital Constitutionalism in India-An Overview and its grey areas**

Constitutionalism is intricately linked to digital technology, comprising both physical and abstract components that facilitate the exercise of human liberties and talents. Given the expectation that digital technologies will continue to be the primary catalyst for global changes in the future, the development of Internet governance is poised to have a substantial impact on this association. The management of the Internet is progressing towards division, division, and a combination of different approaches. These tendencies pertain not just to the governance of the technological infrastructure. Additionally, they play a part in transforming the structure of liberty and authority in the digital realm, promoting a fresh function for constitutionalism in the era of digital technology<sup>4</sup>. Digital constitutionalism refers to the concept of applying the principles of modern constitutionalism to the digital world. Digital constitutionalism is having a significant

impact on our society. It does not undermine the fundamental principles of current constitutionalism, but instead seeks to preserve its essential ideals in a way that is more suitable for the unique characteristics of the digital society. Current societal changes are continuously testing the traditional structures of constitutional law. The digital revolution has brought about significant changes to our personal lives, our interactions with others, and society as a whole. These changes are occurring within a framework of constitutional standards that were originally designed for traditional, non-digital societies. Nevertheless, the constitutional ecology is not inactive. The current constitutional framework must be revised or adapted to more effectively accommodate the changes brought about by the digital era. The enhanced authority of governments that, by using digital technology, have acquired more dominion over the lives of their populace. In the present day, traditional constitutional ideas are no longer capable of addressing all the complexities of the digital society. The form of constitutionalism inevitably undergoes further transformations. Additional constitutional layers are incrementally incorporated into the existing ones. New principles are arising to express the core ideals of constitutionalism in response to the challenging problems of modern society<sup>5</sup>. Yet, this does not undermine the initial constitutional framework established on the principles of democracy, the supremacy of law, the division of powers, and the safeguarding of human rights. Digital constitutionalism is trying to perpetuate the constitutional principles in the digital society, whereby preserving the contemporary constitutionalism.

The threat that these digital technologies bring is cannot be left unseen. The escalating hazards arising since the manipulation of our individual data enabled by the use of digital technologies are illustrative. Furthermore, the increasing importance of digital technology in modern culture has given a significant aggregate of power to non-state entities, such as large multinational corporations and worldwide organizations that own, exploit, or control this technology. This has had a negative impact on traditional constitutional actors, such as nation states. The advent of digital technologies not only affect the fundamental rights but also creates an imbalance in providing private entities a more dominant position. Tech Companies have significant influence on the daily lives of an unprecedented number of individuals. The likelihood and intensity of non-state actors infringing upon our fundamental rights is increasing. However, the prevailing mechanisms of power balancing, which primarily concentrate on the interaction between people and nation-states, do not adequately address this situation. In this paper the Author 's tries to analyse the concept digital rights and thereby providing a framework to work in tune with the Constitutional principles.

### **1.2 Digital Rights framework in Constitution of India**

The digital Revolution has greatly broadened the scope within which freedom of speech and expression functions. In India, the understanding and implementation of these basic rights in the digital realm have undergone significant development, along

<sup>3</sup> Masur, P. K. (2020). *How online privacy literacy supports self-data protection and self-determination in the age of information. Media and Communication*, 8(2), 258-269.

Wimmer, M., & Moraes, T. G. (2022). *Quantum computing, digital constitutionalism, and the right to encryption: perspectives from Brazil. Digital Society*, 1(2), 12.

<sup>5</sup> Babie, Paul T., and Arvind P. Bhanu. 2022. "The Form and Formation of Constitutionalism in India" *Laws* 11, no. 2: 33.

with the emergence of difficulties and legal explanations. Social media platforms play a important role in influencing public conversations by providing a space for users to voice their thoughts, exchange information, and participate in debates. The widespread use of these platforms, however, has resulted in difficulties with the regulation of material, including issues such as hate speech, dissemination of false information, and the distinction between free speech and content that incites violence or encourages discrimination. Regulators and judicial agencies have faced a challenging issue in finding a balance between allowing expression and implementing appropriate content regulation on these platforms. The conflict between upholding freedom of speech and controlling potentially dangerous or rights-violating information has resulted in cases of internet censorship. India has encountered instances of content removal, website blocking, and government instructions to social media companies to delete particular content due to concerns regarding national security, public order, or defamation. The delicate balance between safeguarding freedom of expression and curbing potentially harmful content has been the subject of legal disputes and public discussions. The development of data privacy legislation in India has been a reaction to the growing digital presence and the necessity to safeguard personal data. Prior to the implementation of dedicated data protection laws, data privacy problems were mostly dealt with under the Information Technology Act of 2000. The Information Technology Act, 2000 (IT Act) is the main law in India that deals with Electronic Commerce, digital signatures, and Cybercrime. However, it has extensive measures that are expressly committed to data privacy. Section 43A of the Information Technology Act included the requirement for bodies corporate to implement judicious security performs and processes for handling sensitive private data or information. The Information Rules of 2011 further specified that these measures must be in place and imposed liability in cases of negligence leading to wrongful loss or gain. The IT Act deals with a range of cyber-related matters, such as unauthorized access, hacking, data theft, and cybercrimes. Sections 43, 43A, 66, and 66B to 66F of the law specifically cover computer offenses, their corresponding sanctions, and procedures for dealing with cyber threats<sup>6</sup>.

The historical setting of the adoption of the Indian Constitution on January 26, 1950 is highly significant in influencing the governance and legal structure of the country. The constitution of India, established with the direction of Dr BR Ambedkar and a team of visionary thinkers, is widely recognized for its progressive and inclusive characteristics, establishing the foundation for a democratic and secular Republic. Although conceptualized during a very distinct age, in the present era of technology, the concepts and fundamental rights outlined in constitutions remain significant and provide guidance in dealing with modern difficulties, especially those related to the digital realm. The basic rights, which are written in Part III of the Indian

Constitution, serve as the foundation for the rights that are granted to Indian people. Originally designed to safeguard rights in the physical domain, these rights have undergone broad interpretations and implementation in the digital sphere<sup>7</sup>. Article 19 of the Indian Constitution ensures six essential freedoms, which encompass the rights to freedom of speech, freedom of expression, freedom of assembly, freedom of association, freedom of movement, and freedom of profession. In the digital era, the scope of freedom of speech and expression, as defined by Article 19, has considerably expanded. Through the initiation of the internet and social media platforms, individuals have gained the ability to openly and unrestrictedly share their thoughts and opinions. Nevertheless, these developments also present difficulties with the governance of material, namely addressing concerns of misinformation and the delineation between free speech and hate speech or defamation. The implementation of Article 19, which ensures the right to freedom of expression, in the digital domain has resulted in legal precedents shaping the creation of policies and laws that seek to find a middle ground between the freedom of speech and the necessity to tackle concerns like content moderation, online harassment, and misinformation. The Issue of free speech can be seen from M.F Hussain Controversy (2006) to the latest Digital Media Regulations<sup>8</sup>.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 is formulated for monitoring digital media platforms. The recently implemented Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, also known as the IT Rules 2021, aim to achieve two primary goals are augmenting the accountability of social media platforms (X, Instagram, Facebook, etc.) in order to mitigate their potential for mismanagement and exploitation, and empowering social media users through the establishment of a three-tier mechanism for efficiently addressing complaints. The IT Rules 2021 have been formulated under the jurisdiction provided by section 87(2)<sup>9</sup> of the IT Act and supersede the previous Information Technology (Intermediary Guidelines) Rules, 2011 (referred to as 'the IT Rules 2011')<sup>10</sup>. The Code of Ethics applies to publishers of digital media, such as news and current affairs content providers and OTT platforms. The IT Rules 2021 have received extensive condemnation for their undemocratic and unconstitutional nature. Various courts, comprising the High courts of Madras, Kerala and Bombay and Delhi, as well as the Supreme Court, are currently reviewing the constitutionality of these rules. An interim ruling was just issued by the Madras High Court, marking the latest stage in this ongoing battle. Although other courts have issued temporary orders in cases inspiring the Intermediary Rules, the Madras high court's judgment is the first one specifically related to Part II of the Rules, which governs digital intermediaries.

<sup>6</sup> Pavan Duggal Cyber law – AN exhaustive section wise commentary on the Information Technology Act, 3<sup>rd</sup> Edition 2023.

<sup>7</sup> Macpherson, E., Borchgrevink, A., Ranjan, R., & Vallejo Piedrahíta, C. (2021). Where ordinary laws fall short: 'riverine rights' and constitutionalism. *Griffith Law Review*, 30(3), 438-473.

<sup>8</sup> Sharma, T. (2023). The Changing Face of Free Speech: A Study of Article 19 In the Digital Age in India. *International Journal of Law and Social Sciences*, 78-88.

<sup>9</sup> Which gave the central government the power to frame rules to block content under the grounds mentioned in Section 69A of the IT Act. Such grounds are Sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above

<sup>10</sup> Dhruv Manchanda and Priyam Raj Kumar, 'The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021: Impact On Digital Media' Mondaq (2021).

The Bombay High Court, in the cases of Agij Promotion of Nineteenonea Media Pvt. Ltd. Vs. Union of India<sup>11</sup> and Nikhil Mangesg Wagle Vs. Union of India<sup>12</sup>, has temporarily halted the enforcement of Rule 9(1) & 9(3) of the IT Rules, 2021. These rules required online news publishers and online curated content publishers (commonly known as OTT) to follow a specific 'Code of Ethics' set by an external authority. The High Court determined that these two sub rules were clearly in violation of the basic freedom to speech and expression. Furthermore, the Court concluded that the central government did not have the authority to create these Rules under the parent legislation, namely the IT Act. It was also contended that IT Rules debased the constitutional privileges to liberty of speech and manifestation and the Supreme Court's decisions in K.S Puttaswamy v. Union of India<sup>13</sup> and Shreya Singhal v. Union of India<sup>14</sup>. Rule 9 of the IT Rules prima facie infringed the constitutional guarantee to freedom of speech granted by Article 19(1)(a), by requiring publishers to comply with the Norms. The public interest litigation was initiated by TM Krishna, a Carnatic musician, and a second petition was filed by the Digital News Publishers Association (DNPA), which consists of thirteen media outlets, along with journalist Mukund Padmanabhan. The petitioners argued that the IT Rules, 2021 are in violation of Articles 14 and 19 of the Constitution of India. The Madras high court bases its decisions on the criteria established by the IT Act for limitations on freedom of communication and expression, as outlined in the Supreme Court's significant ruling in the case of Shreya Singhal v. Union of India (173). In the case of Shreya Singhal, the court determined that any regulation attempting to limit freedom of expression may only be considered valid if it is directly connected to one of the eight specific topics outlined in Article 19(2). According to Article 19(2), the right to freedom of speech and expression can be limited in order to protect the sovereignty and integrity of India, ensure the security of the state, maintain friendly relations with foreign countries, preserve public order, uphold decency or morality, or address contempt of court, defamation, or incitement to commit a crime. In its ruling, the Madras High Court cites the Shreya Singhal case to discuss the test applied to Rule 3(1)(b)(x), which prohibits intermediaries from issuing blatantly false and untrue information with the intention to deceive or harm others for financial gain or to cause harm. The Madras high court has observed that initially, these limitations appear to exceed the boundaries of Article 19(2). The court has also recognized the influence of the regulations on individuals, noting that there is a legitimate concern that a subtle signal or approval from the relevant authorities may lead to the platform existence unavailable to a citizen. It is crucial to emphasize that while expressing these first concerns regarding Rule 3, the court did not essentially suspend its implementation.

The Supreme Court while dealing with the matters transferred from the High Courts and taking consideration of the case filed by Justice for Rights Foundation seeking stricter content guidelines for Over-The -Top (OTT) streaming platforms such as Amazon and Netflix, it was held that government should

not take any action against anyone who fail to comply with the laws. Undoubtedly, digital media is an immensely powerful contrivance for training one's freedom of speech and expression. Though, the escalating utilization of digital media for illicit activities has bolstered the Government's endeavours to regulate and restrict its dissemination<sup>15</sup>. While the abuse of digital media necessitates legal control, there are also valid concerns about the infringement of civil rights as an unavoidable outcome of censorship. It can be seen that Article 19(2) of the Constitution of India stick to the same old format rather in considering the need for bringing the need for Digital Constitutionalism in India. Article 21 of the Indian constitution encompasses the fundamental right to life and individual freedom. Over time, the Judiciary has read Article 21 and recognized the right to privacy. In the significant legal case of Justice KS Puttaswamy v. Union of India<sup>16</sup> (2017), the Supreme Court of India unequivocally affirmed that the right to privacy is an inherent and basic right enshrined under Article 21 of the Constitution of India. This ruling established a significant precedent recognizing the need of safeguarding data and privacy in the era of digital technology. The ruling established the basis for deliberations and legislative structures concerning the preservation and safeguarding of data privacy in India. Although these fundamental rights form the foundation for addressing digital rights in India, the understanding and implementation of these rights in the digital realm are still developing. The constitutional significance of these Fundamental Rights in the digital era is a topic of continuous legal and policy discussions, especially in regards to the delicate balance between free expression, privacy, and the necessity of regulation to guarantee responsible utilization of digital platforms. It is crucial to examine and modify these constitutional provisions to address the intricacies of the digital environment in order to guard the rights and privacy of Indian people in the digital era.

Given the advanced capabilities of social media and search engine websites in monitoring individual behaviour, the emerging field of digital constitutionalism aims to not only challenge government entities but also non-government entities such as Facebook and Google. Furthermore, the principles established in Article 21 on the concept of dignity in legal decisions may also be extended to the realm of informational privacy. These normative counteractions may be extended to oppose both the State and Non-State actor. Nevertheless, the broadening of normative counteraction necessitates a dual strategy, whereby Non-State actors such as Facebook and Google are seen as an integral component of the 'State', with 'State' according to the definition provided in article 12 of the Indian Constitution. If these corporations (Facebook, Google, etc.) are considered to be 'State', they should be equally responsible for safeguarding the dignity of individuals, just as the Government of India. Nevertheless, Indian Jurisprudence has not yet reached a level of development where it may acknowledge Non-State actors as being included in article 12 of the Constitution of India<sup>17</sup>.

<sup>11</sup> W.P. (L.) 14172 of 2021

<sup>12</sup> AIR ONLINE 2021 BOM 3175

<sup>13</sup> AIR 2017 SC 4161.

<sup>14</sup> AIR 2015 SC 1523

<sup>15</sup> Ajay Kumar, 'Digital Media Regulations in India: Some Reflections' in Pawandeep Kaur (ed), *Emergent Regulatory Governance: Key to* ISSN: 3048-5045; Vol 02 Issue 01; Jan-2025; Pg-15-20

*Indian Regulatory Laws 303-337 (Indu Book Services Pvt Ltd, New Delhi 2022).*

<sup>16</sup> (2017) 10 SCC 1, AIR 2017 SC 4161

<sup>17</sup> Ashit Kumar Srivastava, *Digital Constitutionalism and personal data protection*, The Daily Guardian, 2020.

The Data Protection and Data Privacy (DPDP) Act in India which is in line with the European General Data Protection Regulation has faced scrutiny regarding its alignment with Article 21 of the Constitution of India, which guarantees the right to life and personal liberty. Article 21 of the Constitution includes the right to privacy but the current Data Protection and Data Privacy Act (DPDP) Act does not provide the adequate safeguards to protect this right, particularly in terms of data collection, processing, and sharing. The DPDP Act may not fully empower individuals (data subjects) with sufficient control over their personal data. This includes issues around consent, data portability, and the right to be forgotten, which are crucial for protecting individual privacy. The broad exemptions for government agencies from various provisions of the law in the Act can potentially lead to unchecked surveillance and misuse of personal data, undermining the privacy rights enshrined under Article 21. Even it can be seen that the data localization mechanism might infringe the privacy rights as it might make the Government to access personal data without adequate oversight. However, this raises a significant legal question for us to consider: is it feasible to use the criteria of a reasonable expectation of privacy to address the gaps in privacy law in India until a specific law is enacted or the present law can be reframed in tune with the Constitutional principles. But there still arises a dilemma that the latest DPDP Act 2023 if made stringent then again, the data driven bodies will be questioned for use of data. Thus, the issues of inadequate consent mechanism, excessive government exemptions and weak data breach notifications cannot be worked in alignment with Article 21 of the Constitution.

### 1.3 Government Initiatives in considering cyber threats

As technological advancements progress, the risks in the digital realm also increase. The fast process of digitizing many industries has presented hackers with fresh prospects to exploit weaknesses and pilfer important information. Government measures are vital in combating cybersecurity concerns in India, given the increasing prevalence of cyber-attacks.

The Indian government has implemented a range of programs and regulations to tackle cyber security threats. Such as

- The National Cybersecurity Policy 2013 is designed to safeguard information infrastructure in cyberspace, enhance the capacity to prevent and address cyber threats, and reduce risk<sup>18</sup>.
- The National Cyber Coordination Centre (NCCC) serves as a platform for acquiring and analyzing threat intelligence to assist the government's cybersecurity endeavors<sup>19</sup>.
- The Indian Cyber Crime Coordination Centre (I4C) was formed with the aim of combating cybercrime and enhancing law enforcement capacities in addressing cyber threats<sup>20</sup>.
- CERT-In (Indian Computer Emergency Response Team) CERT-In, which operates under the Ministry of Electronics and Information Technology, serves as a central body for managing cyber security incidents<sup>21</sup>.

<sup>18</sup> Available From: [https://www.meity.gov.in/writereaddata/files/downloads/National\\_cyber\\_security\\_policy-2013%281%29.pdf](https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf)

Although there have been efforts to address cyber security, there is still a need for ongoing development and enhancement of measures. The ever-changing landscape of cyber threats, such as advanced attacks, data breaches, and ransomware, requires a responsive and flexible approach from the government and relevant agencies to effectively combat emerging challenges in cyberspace.

The effort taken by the Government in enacting a law as well as such initiatives provide for protection of citizen information and upholding citizen right to free expression. But it is becoming a challenging task that surveillance measures and data collection by Government agencies can potentially infringe on individual's privacy rights. Even the surveillance is necessary to protect national security but such measures will be violative of fundamental rights is not used proportionately and with judicial oversight. The specific provisions in the National Security Policy 2013 which enumerates the clauses for monitoring and incident response which aims at intrusive surveillance practices, the capacity building and training process which focusses on extensive data collection and collaboration with private entities leading to sharing of personal data.

National Cyber Coordination Centre (NCCC) even works on monitoring internet traffic and extensive surveillance of digital communications. The main work initiated by this center pertains to censorship, which can lead to suppression of legitimate speech and expression. Thus, the main areas of monitoring without warrants, data sharing, indiscriminate blocking of websites affects the constitutional rights of people. Section 70B of the Information Technology Act 2000 speaks about the Indian Computer Emergency Response Team to serve as national agency for incident response. CERT – In has broad discretionary powers to act against perceived cyber threats, including issuing directives to service providers and intermediaries. The arbitrary and discriminatory enforcement of cyber security measures will violate the principle of equality before the law. Another major concern arises due to the actions taken under the cyber security policies which will bypass due process of result in unfair trials. Thus, a fair trial is guaranteed under Article 20 and 21 of the Constitution is not achieved due to the hasty enactments and initiatives for cyber protection in India.

### 1.4 Deficiencies in the current Constitutional framework for Digital Rights in India

- There is no specific provision entirely dedicated to data privacy even though right to concealment is enshrined in the Article 21 of the Constitution of India. The lack of a dedicated data protection framework under the constitution leads to uncertainty in the legal safeguarding of personal data.
- The constitution written in the mid-20th century failed to foresee the rapid development of technology. Consequently, it may not sufficiently address or anticipate digital concerns, such as future technologies like Artificial Intelligence, as well as the complexities of data usage and protection in the digital realm.

<sup>19</sup> Available From: <https://i4c.mha.gov.in/>

<sup>20</sup> Ibid

<sup>21</sup> Available From: <https://www.cert-in.org.in/>

- Conspicuous a stability between the rights of individuals and the rules that govern them in the digital realm is an ongoing problem. Clearer criteria are needed to manage content in the digital domain without encroaching on fundamental rights.
- The lack of clear legal requirements, along with ambiguous current laws and the absence of particular legislation, impede the effective enforcement of measures related to digital rights, data protection, and cybersecurity.
- There is a lack of enough technical experts within law enforcement. Agencies provide a substantial obstacle in detecting and handling complex cybercrimes. Training and resources are important in effectively combating these problems.
- Successful execution requires Effective cooperation among diverse stakeholders, such as government entities, law enforcement agencies, commercial enterprises, and international organizations, is crucial for a unified strategy and the exchange of information.

## 2. CONCLUSION

The Indian legal system pertaining to digital rights, data privacy, and cyber security is intricate and need extensive measures to successfully confrontation the complications obtainable by the digital era. The existing legal framework does not have specific measures for safeguarding data privacy and finding a balance between free expression and responsible regulation, which reveals notable deficiencies. To effectively tackle digital concerns within the Indian constitutional framework, it is imperative to adopt a holistic strategy that acknowledges the importance of data privacy, technical neutrality, and the need to strike a stability between rights and duties. This strategy should

encompass legal changes, encompassing the development of targeted laws for digital rights, data privacy, and cyber security, in accordance with international standards and including the enhancement of capabilities within law enforcement authorities. Implementing and enforcing these reforms requires international coordination and public awareness efforts. In order to protect digital rights and maintain security measures in India, it is imperative for policy makers, experts, and the public to collaborate and establish a strong, flexible, and rights-oriented legislative framework. The Indian constitutional framework should adapt in parallel with technological progress, upholding the principles of private rights and a robust, cutting-edge security system. Digital constitutionalism as been analyzed is a global and ever-changing concept. To make the laws in tune with constitutional principles is a herculean task. This task can be achieved by active participation of both private entities, non-state actors and legislators. Our constitutional framework and the basic norms should not tamper at any cost in this new and challenging situation.

### *Conflict of Interest*

Conflict of interest declared none.

### *Funding*

The review presented in the article did not receive any external financial support.

### *Acknowledgements*

The authors would like to acknowledge that no external funding or assistance was received for this research, and therefore, no acknowledgements are necessary.

## 3. REFERENCES

- De Gregorio G. Digital constitutionalism across the Atlantic. *Global Constitutionalism*. 2022 Jul;11(2):297-324.
- Suzor N. A constitutional moment: How we might reimagine platform governance. *Computer Law & Security Review*. 2020 Apr 1;36:105381
- Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, 8(2), 258-269.
- Wimmer, M., & Moraes, T. G. (2022). Quantum computing, digital constitutionalism, and the right to encryption: perspectives from Brazil. *Digital Society*, 1(2), 12.,
- Babie, Paul T., and Arvind P. Bhanu. 2022. "The Form and Formation of Constitutionalism in India" *Laws* 11, no. 2: 33.
- Pavan Duggal Cyber law – AN exhaustive section wise commentary on the Information Technology Acr, 3<sup>rd</sup> Edition 2023.
- Macpherson, E., Borchgrevink, A., Ranjan, R., & Vallejo Piedrahíta, C. (2021). Where ordinary laws fall short: 'riverine rights' and constitutionalism. *Griffith Law Review*, 30(3), 438-473.
- Sharma, T. (2023). The Changing Face of Free Speech: A Study of Article 19 In the Digital Age in India. *International Journal of Law and Social Sciences*, 78-88.