IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ASSESSING THE IMPACT OF RECENT LEGISLATIVE REFORMS ON DIGITAL RIGHTS AND FREEDOMS IN INDIA: A CRITICAL ANALYSIS

Mansi Bajpai, LLM 1 year , Faculty of Juridical Sciences, Rama University, Kanpur

Mr. Rahul Singh, Assistant Professor, Faculty of Juridical Sciences, Rama University, Kanpur

ABSTRACT:

India has recently witnessed significant legislative reforms aimed at modernizing its criminal justice system. Among these reforms are three consequential bills: the Bharatiya Nyaya (Second) Sanhita, 2023 ("BNS"), Bharatiya Sakshya (Second) Bill, 2023 ("BSB"), and Bharatiya Nagarik Suraksha (Second) Sanhita, 2023 ("BNSS"). The main objective of these bills is to shift the legal framework from colonial-era practices focused on punishment to a modern welfare state approach centered on delivering 'justice'. These bills seek to achieve this object by overhauling foundational legislations governing criminal law and procedure in the country, with a particular emphasis on digitization and the incorporation of modern technologies. The primary aim of these bills are to make transition in legal framework of colonialism to welfare state.. i.e from the objective of inflicting punishment to the objective of providing 'justice'. However, these reforms have raised concerns regarding their implications for digital rights and freedoms, particularly in relation to privacy, free speech, and protection against self-incrimination. Findings suggest concerns regarding the broadening of executive powers, vagueness of provisions related to cybercrimes and sedition, and the challenges posed by the digitization of criminal procedures. The research underscores the importance of safeguarding fundamental rights amidst efforts to modernize the criminal justice system, emphasizing the need for transparency, public consultation, and oversight mechanisms to uphold democratic principles and human rights in India.

INTRODUCTION

"Every new time will give its law" [1]- Maxim Gorky

India has been undergoing significant legislative reforms in recent times, particularly within its criminal justice system. The introduction of the BNS[2], BSB[3], and BNSS [4]represents a pivotal juncture in the country's legal evolution. On December 25, 2023, the three bills received the President's approval, setting the groundwork for a new criminal justice system in India. These reforms aim to modernize archaic laws and adapt them to contemporary challenges. However, amidst the push for efficiency and accessibility, concerns have been raised regarding the potential impact of these reforms on digital rights and freedoms. As India embraces digitization and integrates modern technologies into its legal framework, questions emerge about the safeguarding of individual liberties in the digital age.

This research article undertakes a critical examination of the recent legislative reforms and their implications for digital rights and freedoms in India. By dissecting key provisions of the aforementioned bills, with a specific focus on privacy, free speech, and protection against self-incrimination, this study seeks to unveil the potential challenges and opportunities presented by the modernization of the criminal justice system. Through a qualitative analysis and synthesis of existing literature, this research endeavors to provide insights into the consequences of these reforms for individual liberties, democratic principles, and human rights.

Amidst the global discourse surrounding the complexities of the digital age, the Indian context serves as a pertinent case study for understanding the intricate interplay between law, technology, and individual rights. By critically evaluating the recent legislative reforms, this research aims to contribute to ongoing discussions regarding the role of technology in shaping legal frameworks and the imperative of upholding fundamental rights in the digital era. Ultimately, it underscores the necessity for deliberate consideration, transparency, and accountability in the pursuit of a justice system that remains faithful to democratic values and honors the dignity and rights of all individuals.

METHODS:

This research article utilizes a qualitative analysis approach to examine the provisions of the BNS, BSB, and BNSS bills, focusing on their implications for digital rights and freedoms in India. The analysis draws upon primary sources, including the text of the bills themselves, as well as secondary sources such as scholarly articles, legal analyses, and media reports. Additionally, insights from expert opinions and stakeholder perspectives are incorporated to provide a comprehensive assessment of the legislative reforms.

[1] Maxim Gorky
[2] Bharatiya Nyaya (Second) Sanhita,2023
[3] Bharatiya Sakshya (Second) Bill,2023
[4] Bharatiya Nagarik Suraksha (Second) Sanhita, 2023

LEGAL PROVISIONS

Substantive Changes

The BNSS categorizes financial scams and cyber crimes, among other offenses, as 'organized crime'. This classification marks a notable shift towards imposing stricter penalties for such cyber crimes. While initially seen as a positive development, regulating 'organized crime' both domestically and internationally carries substantial historical implications and may have unintended consequences. Any such reforms should be undertaken only after consulting with experts, relevant stakeholders, and civil society.

Described as one of the most significant "reforms" to the Indian Penal Code, BNS[5] repeals the offense of "sedition". However, instead of simply removing the word "sedition" from the law (previously Section 124A of the IPC[6]), the Ministry of Home Affairs has replaced it with a broader terminology in the BNS, under Section 150 titled 'Acts endangering sovereignty, unity, and integrity of India.' This Section criminalizes actions that "endanger the sovereignty, unity, and integrity of India ***including using electronic communications*** to incite armed rebellion, subversive activities, secession, separatism, or to threaten India's unity, sovereignty, and integrity". While similar to sedition, this provision has a wider scope and application due to its vagueness, potentially impacting free speech, dissent, and journalistic freedom. Section 150 mandates imprisonment under all circumstances, unlike Section 124A, which allowed for penalties to be limited to fines.

Its major impact is the inclusion of 'electronic communications' as a means to commit "seditious" acts. Coupled with the Telecommunications Bill [7] ,this practically allows for the legal interception of electronic communications. The Telecommunications Bill applies to online communication services, providers like WhatsApp, Signal, etc., which utilize end-to-end encryption to protect privacy, may be obligated to intercept, detain, disclose, or suspend any message. This broad definition of "message" includes any form of communication sent through telecommunications.

These changes have been implemented in midst of the ongoing deliberations of the Supreme Court regarding the current sedition law. On September 12, 2023, a 3-judge bench of the Supreme Court in case of S.G Vombatkere V. Union of India [8]referred petitions challenging the constitutionality of the sedition law to a bench of at least 5 judges. The new Section 150 will only apply prospectively, but the Supreme Court's jurisprudence on criminalizing seditious or similar acts is crucial for criminal justice reform. However, by hastily passing the BNS, the legislative branch has hindered the possibility of comprehensive reform.

[5] Bharatiya Nyaya (Second) Sanhita,2023
[6] Indian Penal Code, 1860
[7] Telecommunications Bill, 2023
[8] S.G Vombatkere V. Union of India (2022) 7 SCC 433

Procedural Changes

The Bharatiya Sakshya Bill (BSB) broadens the scope of what constitutes 'documents' to encompass electronic or digital records, including online communications stored on various personal devices. This expanded definition covers a wide range of electronic communications, laptops, cameras, and any other devices that may be designated by the government in the future.

The BSB, akin to Section 65B of the Indian Evidence Act[9], mandates certification for the admissibility of electronic evidence, but BSB classifies electronic records as "documents," potentially exempting them from certification requirements. The classification of electronic records as "documents" implies a shift in their legal status from secondary to primary evidence.

Section 94 of the BNSS[10] additionally empowers the Court to summon any necessary documents or materials for an investigation, categorizing them as 'evidence', which also encompasses digital evidence. Courts are authorized to order the search and seizure of such evidence for various reasons, including situations where the possessor of the evidence is deemed unlikely to produce it willingly or is not directly linked to the trial. While mobile phones or laptops may contain extensive information, some of which might be irrelevant to the proceedings, they can still be gathered as evidence.

Moreover, Section 185 of the BSB [11]permits a police officer to conduct searches for any material or document, including those in digital devices, without a written order if they possess "reasonable grounds" to believe that obtaining such material or document through other means would result in undue delay. In recent times, there has been a noticeable surge in raids where there appears to be an overextension of search and seizure powers. Additionally, there have been instances of police officers stopping individuals on the streets and compelling them to surrender their phones. Given that mobile devices have become integral parts of our personal lives, laws such as the BSB and BNSS, which legitimize unwarranted search and seizure, will persist in granting law enforcement agencies access to extensive amounts of an individual's private information, thereby encroaching upon their right to privacy.

The bills were introduced with a clear aim of digitalizing various aspects of criminal procedure. From initiating a first information report (FIR) to drafting the charge sheet and issuing judgments, every stage of a criminal investigation is mandated to be documented digitally. According to the BNSS, summons can now be electronically issued, and testimonies from witnesses, experts, accused individuals, and other relevant parties can also be presented electronically or virtually.

[9] Indian Evidence Act, 1872
[10] Bharatiya Nagarik Suraksha (Second) Sanhita, 2023
[11] Bharatiya Sakshya (Second) Bill,2023

KEY CHANGES AND THEIR BROAD IMPLICATIONS

The introduction of cybercrimes and electronic registration of First Information Reports (FIRs), along with the compulsory virtual recording of seized property, reflects the endeavor to digitize the Indian criminal justice system. These new laws aim to enhance efficiency, speed, and equity in delivering justice to citizens.

Given that the old Indian Penal Code was first written in 1860, one of the driving impulses behind the overhaul was to modernize the same. A notable example of this modernization is seen in the treatment of the offense of 'sedition', previously governed by Section 124A of the old code[12]. While this section has been repealed, the new code [13], specifically Section 152, bears striking similarities. Additionally, the inclusion of 'electronic communication' reflects an acknowledgment of modern channels used to propagate sentiments that incite separatist feelings.

This incorporation of electronic communication into legal frameworks, especially in light of proposals under the new Telecommunications Act of 2023, raises concerns regarding online accountability and privacy. The Telecommunications Act mandates online communication service providers to take actions such as intercepting, detaining, disclosing, or suspending messages, even if it means infringing on end-to-end encryption standards aimed at protecting user privacy. This situation prompts questions about the level of data protection and privacy users can expect, indicating a significant shift in the operational practices of communication service providers going forward.

In a sign of the stringent policing of online crimes, Section 111 of the New Penal Code [14] categorizes 'cybercrime' as a form of 'organized crime'. Furthermore, Section 197(d) of the BNS penalizes the generation and dissemination of 'false information'. These offenses have broad definitions, and providing precise definitions would enhance legal sustainability. The implications for social media and e-commerce platforms remain unclear, as does the extent of liability they may face. Online platforms may need to adjust their user agreements, terms, and community guidelines, and improve their monitoring systems to protect themselves from liability for the malicious or illegal actions of their users.

The New Criminal Procedure Code [15] introduces expanded powers for law enforcement agencies during investigations. It enables the seizure of any electronic device or record deemed 'likely' to contain digital evidence, and individuals other than the accused can also be directed to produce such records. In recent times, there has been a noticeable surge in raids where there appears to be an overextension of search and seizure powers. Additionally, there have been instances of police officers stopping individuals on the streets and compelling them to surrender their phones. Given that mobile devices have become integral parts of our

[12] Indian Penal Code, 1860
[13] Bharatiya Nyaya (Second) Sanhita,2023
[14] Bharatiya Nyaya (Second) Sanhita,2023
[15] Bharatiya Nagarik Suraksha (Second) Sanhita, 2023

personal lives, laws such as the BSB and BNSS, which legitimize unwarranted search and seizure, will persist in granting law enforcement agencies access to extensive amounts of an individual's private information, thereby encroaching upon their right to privacy.

It's worth noting that Indian courts have previously interpreted the right against self-incrimination as applicable only to information provided from personal knowledge. However, with these enhanced powers, law enforcement agencies may significantly impact investigations involving companies or corporations, where electronic devices are more readily available for seizure. Consequently, companies may find it necessary to bolster their digital security protocols and refine their legal compliance strategies to effectively address these challenges.

The New Evidence Code grants electronic or digital records the same legal standing, validity, and enforceability as physical documents. This encompasses data stored, recorded, or copied in the memory of communication devices, thereby considering electronic communications as documents themselves. The language suggests that electronic records can serve as primary evidence.

However, despite the allowance for electronic evidence, certain procedural hurdles remain in place. Section 63 of the code sets conditions for the validity of digital evidence based on computer output to ensure its credibility. This implies that while certification is not required for every digital record submitted, there are still stringent conditions that must be met for admissibility. Specifically, only statements submitted in digital form are mandated to carry a certificate as prescribed under section 63(4). This differs from the Indian Evidence Act, where a certificate under section 65B was necessary for the admissibility of all electronic records.

RESULTS:

The analysis reveals several key findings regarding the impact of the recent legislative reforms on digital rights and freedoms in India.

1. **Implications of Legislative Reforms on Digital Rights and Freedoms**: The research article highlights the significant legislative reforms undertaken in India to modernize its criminal justice system, particularly through the introduction and passing of the Bharatiya Nyaya (Second) Sanhita, Bharatiya Sakshya (Second) Bill, and Bharatiya Nagarik Suraksha (Second) Sanhita. These reforms, while aiming to enhance efficiency and accessibility, have raised concerns about their potential impact on digital rights and freedoms, including privacy, free speech, and protection against self-incrimination.

2. **Challenges and Opportunities**: The study identifies key challenges and opportunities arising from the modernization of the criminal justice system in India. It discusses the broadening of executive powers, vagueness of provisions related to cybercrimes and sedition, and challenges posed by the digitization of criminal procedures. There is no denying the inevitability of digitizing criminal processes. The COVID-

19 pandemic underscored the necessity of remotely connecting the components of the criminal justice system, as demonstrated by the widespread adoption of virtual courts and electronic registries. However, two concerns arise from this transition. Firstly, full digitization may inadvertently exclude individuals lacking internet access or technological proficiency, a significant portion of the Indian population. Secondly, careful consideration must be given to the digitization of fundamental aspects such as lodging FIRs. Once implemented, there may be a push to verify or authenticate the identity of the complainant, except in cases of anonymous complaints. Furthermore, promoting SMS-based FIR services could lead to extensive data collection even without the complainant's explicit consent. These issues necessitate thorough discussion and impact assessment, particularly regarding the privacy of complainants, who are often victims or survivors.

3. **Interplay Between Law, Technology, and Individual Rights**: By critically examining the recent legislative reforms, the research article contributes to the understanding of the complex interplay between law, technology, and individual rights in the digital age. It emphasizes the need for transparency, public consultation, and oversight mechanisms to uphold democratic principles and human rights in India's evolving legal landscape.

4. **Qualitative Analysis of Legislative Provisions**: The research article employs a qualitative analysis approach to examine the provisions of the BNS, BSB, and BNSS bills, focusing on their implications for digital rights and freedoms. It draws upon primary and secondary sources, including the text of the bills, scholarly articles, legal analyses, media reports, and expert opinions, to provide a comprehensive assessment of the legislative reforms.

5. **Key Changes and Their Broad Implications**: The article discusses key changes introduced by the legislative reforms, such as the treatment of cybercrimes, sedition, electronic communication, and electronic evidence. It examines the implications of these changes for individual liberties, democratic principles, and human rights in the digital era, emphasizing the importance of safeguarding fundamental rights amidst efforts to modernize the criminal justice system.

Overall, the research article offers valuable insights into the implications of recent legislative reforms on digital rights and freedoms in India, highlighting the need for careful consideration and proactive measures to uphold democratic values and protect individual liberties in the digital age.

DISCUSSION:

The research article provides a comprehensive analysis of the recent legislative reforms in India aimed at modernizing the criminal justice system and their implications for digital rights and freedoms. The discussion delves deeper into the key findings and highlights the complexities surrounding the intersection of law, technology, and individual rights in the digital age.

1. Balancing Efficiency with Safeguarding Rights: One of the central themes of the discussion is the delicate balance between enhancing efficiency in the delivery of justice and safeguarding fundamental rights. While the legislative reforms aim to streamline processes through digitization and integration of modern technologies, concerns arise regarding the potential erosion of privacy, free speech, and protection against self-incrimination. The discussion emphasizes the importance of maintaining this balance to ensure that advancements in technology do not come at the cost of individual liberties.

2. Addressing Challenges and Seizing Opportunities: The discussion identifies the challenges and opportunities presented by the modernization of the criminal justice system. It acknowledges the need to address concerns such as the broadening of executive powers, vagueness of provisions related to cybercrimes and sedition, and challenges posed by the digitization of criminal procedures. However, it also recognizes the potential benefits of these reforms in improving the efficiency and equity of justice delivery.

3. Importance of Transparency and Oversight: Transparency and oversight emerge as critical factors in navigating the complexities of digital rights and freedoms. The discussion underscores the need for transparency in the legislative process, public consultation, and robust oversight mechanisms to uphold democratic principles and human rights. It calls for greater transparency in the formulation and implementation of laws to ensure accountability and protect individual liberties.

4. Future Directions and Recommendations: The discussion concludes by offering insights into future directions and recommendations for policymakers, stakeholders, and civil society. It suggests the need for further research, stakeholder engagement, and policy dialogue to address the evolving challenges and opportunities in the digital age. Recommendations include the development of clear guidelines, procedural safeguards, and mechanisms for redressal to protect digital rights and freedoms while promoting innovation and efficiency in the criminal justice system.

Overall, the discussion provides a nuanced understanding of the implications of recent legislative reforms on digital rights and freedoms in India. It underscores the importance of striking a balance between efficiency and safeguarding rights, promoting transparency and oversight, and charting a path forward that upholds democratic values and honors individual liberties in the digital era.

The findings of this research highlight the need for careful consideration of the implications of legislative reforms on digital rights and freedoms in India. While modernization of the criminal justice system is undoubtedly necessary, it must not come at the cost of fundamental rights and liberties. Policymakers must ensure that adequate safeguards are in place to protect individuals' privacy, free speech, and due process rights in the digital age. Additionally, greater transparency, public consultation, and oversight mechanisms are essential to uphold the principles of democracy and rule of law.

CONCLUSION:

Each technological reform introduced through the new criminal laws has inevitably affected the right to privacy in some capacity. Blanket seizures of data without specific proportionality tests directly challenge constitutional rights to privacy and the avoidance of self-incrimination. To mitigate these risks, stringent procedural and regulatory frameworks must be established to govern the access to data and the duration for which devices can be held in custody. This poses a significant challenge for businesses in India, necessitating clear guidelines on how corporations manage and store user and employee data.

As governmental access to private data expands, there is a heightened obligation to safeguard this information. Electronic devices and records under police custody fall under state responsibility, necessitating the establishment of oversight committees or authorities to monitor the handling of such electronic records and devices. Furthermore, clarification is needed regarding whether exemptions granted to the Central Government and its agencies under the new Digital Personal Data Protection Act, 2023, extend to law enforcement agencies. Additionally, regulatory mechanisms must be established to address breaches of digital personal data held by law enforcement, emphasizing the need for standardized data collection processes, especially in instances such as e-FIR registration, conducted through secure and regulated portals. The absence of provisions ensuring the security and proper maintenance of electronic evidence raises significant concerns regarding privacy and safety. This, coupled with the sensitive data collected under the Criminal Procedure (Identification) Act, 2022, underscores the imperative of a robust digital infrastructure to prevent data breaches.

The new codes grant law enforcement agencies substantial discretionary powers, particularly concerning the registration of FIRs for non-cognizable offenses after preliminary inquiries, property attachment, and warrantless arrests. While enhanced procedural powers have been a longstanding demand of law enforcement agencies, it is essential to issue comprehensive guidelines wherever such discretion is granted to prevent the abuse of power. The framing of a stricter and more inclusive code of conduct is imperative to ensure heightened accountability on the part of law enforcement agencies.

The recent legislative reforms in India present both opportunities and challenges in the realm of digital rights and freedoms. While efforts to modernize the criminal justice system are commendable, policymakers must tread carefully to avoid unintended consequences that may undermine the foundational principles of democracy and human rights. By engaging in informed dialogue, incorporating diverse perspectives, and prioritizing the protection of individual liberties, India can navigate the complexities of the digital age while upholding its commitment to justice and democracy.

REFERENCES

1. S.G Vombatkere V. Union of India (2022) 7 SCC 433
2. The Bharatiya Nyaya (Second) Sanhita, 2023 (BNS).
   Accessible at : www.sansad.in
3. The Bharatiya Sakshya (Second) Bill, 2023 (BSB).
   Accessible at : www.sansad.in
4. The Bharatiya Nagarik Suraksha (Second) Sanhita, 2023 (BNSS)
   Accessible at : www.sansad.in
5. The Telecommunications Bill, 2023
   Accessible at : www.indiacode.nic.in
6. The Digital Personal Data Protection Act, 2023
   Accessible at : www.indiacode.nic.in
7. The Criminal Procedure (Identification) Act, 2022
   Accessible at : www.indiacode.nic.in
8. "E-evidence, New Criminal Law & Its Implementation." The Hindu, 17 Jan. 2015, www.thehindu.com/opinion/lead/e-evidence-new-criminal-law-its-implementation/article67900858.ece#:~:text=The%20three%20newly%2Denacted%20criminal,force%20on%20July%201%2C%202024.
9. "Three New Criminal Law Bills." Internet Freedom Foundation, internetfreedom.in/three-new-criminal-law-bills/.
10. "Revised Criminal Law Bills: The Key Changes Explained." The Hindu, 24 Jan. 2015, www.thehindu.com/news/national/revised-criminal-law-bills-the-key-changes-explained/article67637348.ece.
11. PRS Legislative Research. "Summary and Analysis of the The Bharatiya Nyaya (Second) Sanhita, 2023." PRS India. Retrieved from https://www.prsindia.org/
12. PRS Legislative Research. "Summary and Analysis of the The Bharatiya Sakshya (Second) Bill, 2023." PRS India. Retrieved from https://www.prsindia.org/
13. PRS Legislative Research. "Summary and Analysis of The Bharatiya Nagarik Suraksha (Second) Sanhita, 2023 (BNSS).PRS India. Retrieved from https://www.prsindia.org/