International Journal of Juridical Studies & Research (IJJSR), Vol. 1, Issue 1, May 2024 Page 260 - 273

From Civil Liberties to Digital Rights: The Legal Architecture of Digital Citizenship in India

DR. LAHAMA MAZUMDAR

Abstract

Rapid digitisation of the economies and the societies has changed the concept of human rights, civil liberties and citizenship, giving rise to the notion of digital citizens who interact, communicate and transact in the digital world. The paper therefore looks forward to examine the evolving legal architecture of digital citizenship in India, with particular focus on constitutional guarantees, statutory frameworks and judicial interpretations. The study identifies a gap in existing knowledge: while much has been written about individual laws, there is limited integrated analysis of how constitutional rights, data protection law and judicial doctrines collectively shape digital citizenship in India. The paper employs doctrinal research methodology, drawing on constitutional provisions, status such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 and leading case laws.

KEYWORDS: *Digital Citizens, Data protection, Cyber-security, Digital Rights, Digital governance, legal frameworks.*

.

Dr. Lahama Mazumdar PHD, LLM, BSC LLB (IP Hons)

Introduction

The digital transformation of India has fundamentally redefined the relationship between citizens, the state and private entities. In an increasingly interconnected and digitized world, the concept of human rights and citizenship extends beyond national borders to encompass the digital realm. As societies become increasingly reliant on digital technologies for communication, commerce, and governance, the concept of digital citizenship and rights in the digital world emerges as a crucial facet of contemporary disclosure. Digital Citizenship encapsulates the rights, responsibilities and participation of individuals in the digital society where online interactions and transactions are integral aspects of daily life. As technology continues to evolve and shape our socio-economic landscape, the need for robust framework to govern digital citizenship becomes imperative.

This research undertakes a study of the regulatory frameworks for digital citizenship in India, as to whether new human rights emanate from the realm of internet or how are the existing human rights featuring in digital world. India with its burgeoning population and rapidly expanding digital infrastructure stands as one of the world's largest and most dynamic digital economies. The country boasts a robust legal framework encompassing various statutes and legislations aimed at regulating and protecting the rights of digital citizens. From constitutional provisions guaranteeing informational privacy and right to access internet, specialised legislation addressing cybercrimes and data protection, India's regulatory landscape reflects a multifaceted approach to digital governance. Further its ongoing initiatives like the Digital Personal Data Protection Act, 2023 and the Digital India Act[1] underscores India's commitment to addressing emerging challenges in the digital domain.

In India the law relating to electronic governance and digitisation was first hand regulated through the Information Technology Act, 2000. In India citizens didn't enjoy right to privacy, let alone information privacy, till 2017. On 24th August 2017, a nine-judge bench of the Supreme Court in K.*S Puttaswamy v/s Union of India*[2] ruled that right to informational privacy is a fundamental right for Indian Citizens under Article 21 of the Indian Constitution. It also laid down the concept of data protection and right to be forgotten over the internet. With rapid digi-industrialisation, India saw a new market for data of its own citizens, where data breach was a rampant occurrence.

[1] Ministry of Electronics and Information Technology, "Proposed Digital India Act , 2023" *Goi* (2023).
[2] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (SC) (per Chandrachud J) at 1–21.

Companies (*data fiduciaries*) with Indian consumers (*data principal*) would collect their data and as a result of less stringent mechanisms of data security, expose the data to data breach. India therefore built its own Digital Personal Data Protection Act, 2023 to protect its digital citizens from data breach and manipulation online. The digital citizens were not only introduced to the right to informational privacy but also got acquainted the concept of consent for data collection, right to access information about personal data, right to correction and erasure of personal data, right of grievance redressal and right to post-mortem privacy. [3]

The study therefore seeks to elucidate the key dimensions of digital citizenship regulation and human rights in India. By analysing the constitutional provisions, statutes and judicial interpretations, we aim to discern the underlying principles and policy imperatives shaping the country's regulatory framework. Furthermore, by exploring case studies we endeavour to assess the effectiveness and implementation of digital citizenship regulations in practice. Central to this inquiry is an exploration of the rights and duties conferred upon digital citizens within Indian jurisdiction. Fundamental rights such as the right to privacy, freedom of expression, and access to information, form the bedrock of digital citizenship, serving as cornerstones for democratic participation and individual autonomy. However, alongside these rights come a host of responsibilities, including compliance with cyber-security protocols, respect for intellectual property rights, and ethical conduct in online interactions. Moreover, this study endeavours to unpack the institutional mechanisms and regulatory agencies tasked with overseeing digital citizenship issues in India.

Research Problem:

The emergence of the digital age in India has fundamentally reshaped the way civil liberties are exercised, restricted and protected, thereby raising urgent concerns about the adequacy of existing

[3]Burman, Anirudh, *Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee Could Learn from Europe's Experience*, (2018) 30(2) NLSIR 45 at 50.

legal and constitutional frameworks. Rights such as freedom of speech and expression, equality, privacy and access to information, though firmly rooted in the Indian Constitution, face new challenges in their transformation in to the digital sphere. The IT Act, 2000 and the DPDP Act, 2023 constitute the primary legislative tools governing cyberspace. However, both laws reveal considerable limitations, including broad power of surveillance, weak enforcement of data protection and insufficient checks against censorships and misuse of personal information. Judicial Pronouncement such as the Justice K.S Puttaswamy's Privacy judgement or the Shreya Singhals Section 66A judgment highlight the role of Indian Judiciary's role in protecting digital freedoms, but also expose gaps in legislative clarity and institutional enforcement.

Objectives:

1. To critically examine the legal foundation underpinning digital citizenship in India.

2. To evaluate the effectiveness of existing statutory provisions and judicial safeguards in protecting digital rights.

3. To identify existing legal and policy gaps and propose actionable recommendations for reform.

Methodology

This is primarily doctrinal research based on constitutional provisions, statutory law and judicial precedents. It focuses on critical analysis of primary and secondary legal sources to examine the intersection of civil liberties and digital rights in India.

The Architecture of Digital Citizenship in India

A concept of digital identity for transactions has been evident in commercial practice for many years. However, the full implications of this development are now emerging as governments digitalize government services. Today the world has completely based itself on digital transactions.

Payments have become digitised where RBI and other regulatory bodies are currently overseeing the digital payment systems and transactions. The Reserve Bank of India even introduced the digital rupee or the digital currency system in the Union budget for 2022-23. The CBDC (Central bank's digital currency) can benefit customers with better liquidity, scalability, acceptance and convenience.[4] RBI is working towards ensuring security, reliability and consumer protection in digital payment systems. The government is even promoting digital inclusion and access though initiatives like digital India. These efforts aim to enhance government services online, ensuring accessibility and efficiency for citizens. Social media and intermediaries have also become new mediums of communications and with the netizens increasing online presence a method of regulating activities online is on the grow. The government has introduced guidelines for intermediaries and social media platforms under the Information Technology Act, 2000. The guidelines mandate platforms to take measures for content moderation, user privacy protection and compliances with Indian Laws. [5]

Constitutional Provisions and Fundamental Rights

Digital citizenship encapsulates the rights, responsibilities and participation of individuals in the digital society where online interactions and transactions are integral aspects of daily life. In India, the constitutional framework forms the bedrock for digital citizenship, influencing how digital rights and responsibilities are interpreted and then protected. In the constitutional hemisphere right to informational privacy along with freedom of speech and expression online, right to information and right to equality form the main branch of concerns.

Right to Informational Privacy: Right to privacy was unrecognized but widely discussed in India since a very long time. Article 21 of the Indian constitution lays down regarding right to life and personal liberty thereby also forming the umbrella under which Right to privacy found its home. In the constitutional assembly debates, Mr. Kazi Syed Karimuddin, a member of the constitutional assembly was the first to pursue the idea of including right to privacy in the realms of the constitution.[6] Even though unsuccessful, the concept got heavily discussed in multiple landmark

[4] PwC, "Central Bank Digital Currency in the Indian context" (2021).
[5] Adyasha Kar, "Freedom of speech and expression in the realm of digital media," 4 *Supremo Amicus* 72–8 (2018).
[6] Smt. Kalpana Kumar, Shri B. Phani Routh, Smt. Bela Sharma, *Right to Privacy*, 2020.

judgments. M.P Sharma v/s Satish Chandra followed by the decision of Kharak Singh v/s State of UP ruled stating that right to privacy is not a part of the Indian Constitution. However, with the judgment of K.S Puttaswamy v/s Union of India, right to privacy alongside right to informational privacy found its place in the Indian context Informational privacy is currently one of most debated issues with concerns of data theft and breach. The Aadhaar Judgment or the landmark judgment of K.S Puttaswamy v/s Union of India laid down the bricks of right to privacy online. The aadhaar is a basically a database containing intricate details of the citizens including their biometric information. It was argued that the compulsory requirement of aadhaar for access to social welfare schemes violates the right to privacy of an individual. Aadhaar includes biometric information that is connected to bank accounts, permanent account number (PAN) creating every possible chance that the information collected with Aadhaar may get misused and eventually hamper the privacy of individuals. The court while discussing about the concepts of informational privacy highlighted some major concerns that were later on resolved to certain extent by the Digital personal data protection Act 2023.[7] The concerns of the court laid down the rights of the data principal in the new legislation. The rights include: Firstly, Right to be deleted/Right to be forgotten. Right to be forgotten essentially refers to the ability of an individual to limit, de-link, delete or correct the disclosure of his personal information that is misleading, embarrassing or even irrelevant. To have an absolute control over one's own information online is a right that was recognized by this judgment. Secondly, Right to post mortem privacy or Right to nominate. The DPDPA, 2023 introduced this concept under section 14 of the Act, where a data principal can nominate an individual who shall in the event of death or incapacity of the data principal would exercise the rights of the data principle. Lastly, the data principal also has the right to access information about personal data. The data fiduciary involves any individual or any entity that collects and processes the personal data. Now when a data fiduciary collects and processes the personal data of any netizen, the Act has put an obligation on them to inform the data principal or the netizen what will be done with that data and what processing activities will be undertaken by them.

The DPDP Act 2023 also marks a significant step on regulating the collection, processing of personal data with implications of state surveillance. In the popularly known as the Pegasus Case (Manohar Lal Sharma v/s Union of India 2021) the vulnerability of digital citizens privacy was

[7] Payal Thaorey, "Informational Privacy: Legal Introspection In India," 2 *ILI Law Review* 160–79 (2019).

highlighted. Allegations surfaced that the spyware was used to secretly access the phones of journalists, activists and political figures. It raised concerns about unauthorised surveillance and intrusion into personal communication. The court in this case acknowledged that indiscriminate surveillance could violate right to privacy under Article 21, even though the state argues the necessity of such measures for national security. The court emphasised that any intrusion into private data must adhere to the principles of legality, proportionality and accountability. Although the DPDP Act does explicitly target state surveillance, its provisions create a legal baseline for accountability which could be extended onto the state. As stated above data fiduciaries, the ones collecting, processing, sharing the data are now accountable to ensure purpose limitation, maintain security safeguards and ensure right of access, correction and erasure.

Freedom of speech and expression: Article 19(1) (a) of the Indian constitution deals with freedom of speech and expression. In the digital context this right extends to online communication and expression, influencing regulations regarding internet content and user-generated content on platforms. Freedom of speech and expression on the internet has been one of the most relevant issues since more than a decade. The question has been around whether the right has to be interpreted differently as per the digital and the physical space and whether the intermediary is responsible to regulate the e-content being hosted by them. In Shreya Singhal v/s Union of India, the Supreme Court of India faced the earlier two questions. Article 19(1)(a) lays down the right to free speech and expression, however, the right is not absolute and is subject to certain limitations in the form of reasonable restrictions on grounds of sovereignty, security of state, public order, decency, morality, contempt of court, defamation or incitement to an offence. In the above case a public interest litigation was filed to challenge the constitutional validity of Section 66A of the IT Act, 2000 wherein the State of Maharashtra was called upon to explain the manner of the arrest of two girls for writing posts on Facebook(a social media platform) relating to closure of Mumbai over Bal Thackeray's death. Later, Ministry of Information Technology also issued an advisory on implementation of Section 66A dated 9th Jan 2013 that required police not to arrest any person under Section 66A till approval is taken from Inspector-general of Police or Superintendent of Police at District level. Section 66A was cognizable offences that allowed police officers to appregend and investigate a case without a warrant. Hence, the result of this was that many uncanny arrests of the people were made by the police throughout the country for publishing any

opinion or view. The petitioner filed a writ petition under Article 32 of the Indian Constitution, seeking the Supreme Court of India to declare Section 66A, 69A and 79 of the IT Act ultra-vires to the Constitution of India. It was asserted in the petition that the wordings of the provision are wide and ambiguous. The petitioner further affirmed that the objective of these provisions was inclined towards its reckless exploitation and thus falls out of the purview of Article 14, 19(1)(a) and 21 of the Indian Constitution. There are terminologies like "*menacing, offensive, annoyance, inconvenience, obstruction, danger, and insult*" which are not explained or defined in any act. Thus, it makes it more prone to unwanted abuse. It was asserted that the distinction gives an authority to the police officers to apprehend netizens or the digital citizens for their remarks which can also be made by the general citizens of the country. Thus, such classification violates the fundamental right to equality penned down under Article 14 of the Indian Constitution.

The court exclaimed that the main issue was whether section 66A violated the right to freedom of expression guaranteed under Article 19(1)(a) of the Constitution of India. As an exception to the right, Article 19(2) permits the government to impose "*reasonable restrictions . . . in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offense*." The Petitioners argued that Section 66A was unconstitutional because its intended protection against "*annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, or ill-will*" falls outside the purview of Article 19(2). The argument was majorly on account of the plea that Section 66A was unconstitutionally vague as it failed to specifically define its prohibitions and neither of them was included in the scope of reasonable restrictions. In addition, the contention was also that the law had a "chilling" effect on the right to freedom of expression. The government, on the other hand had argued that the legislature is in the best position to fulfill the needs of people and courts may interfere with legislative process only when "a statute is clearly violative of the rights conferred on the citizen under Part-III of the Constitution." The government contended that mere presence of abuse of a provision may not be a ground to declare the provision as unconstitutional. According to the government, vagueness cannot be a ground to declare a statute unconstitutional "if the statute is otherwise legislatively competent and non-arbitrary". The court discussed three essential aspects of speech i.e., discussion, advocacy and incitement where the court stated that mere discussion or even advocacy

of a particular cause howsoever unpopular is within the rights of people and if the law curtails it has the freedom to only curtail that discussion or advocacy that amounts to an incitement. Now, Section 66A was capable of limiting all sorts of internet communications as it doesn't realise the difference in the scope of the provision. The court also addressed that Section 66A is capable of imposing chilling effect on the freedom of expression as because it fails to define terms like 'inconvenience or annoyance" which could go around and curtail a very large amount of protected and innocent speech.[8]

Commenting on the matter of differential treatment of netizens and citizens, the court opined that there is an intelligible difference between information transmitted through internet and other forms of speech, which permits the government to create separate offences related to online communications. Even though Section 66A was declared unconstitutional on grounds of violating Article 19(1) (a), the court did clarify that the provision was not violative of Article 14 and it was normal to treat both the communications (internet and non-internet) differently.

The right to speech and expression was once again brought to light through the case of Anuradha Bhasin v/s Union of India. Infamously known as the case of internet shutdowns, the supreme court emphasized that any restriction on freedom of speech and expression must adhere to the principles of proportionality and necessity. The judgment highlighted that indefinite internet shutdowns are unconstitutional particularly when affecting fundamental rights. Right to access internet in today's times is of great essence, internet is a medium for education, occupation and all other means and forms of expression. [9]

Right to Information: Access to information enables citizens to hold the government accountable, which is crucial for the protection of life and liberty. Lack of information can lead to corruption and inefficiency which may endanger the lives and liberties of individuals. The judiciary has often linked the right to information with Article 21 of the Indian Constitution where in the case of State of Uttar Pradesh v/s Raj Narain, the Supreme Court observed that the right to know is derived from the concept of freedom of speech and expression under Article 19(1) (a) which is essential for the

[8] Chinmayi Arun, "Gatekeeper Liability and Article 19(1)(A) of the Constitution of India," 19 *NUJS Law Review* (2015).

[9]Sarvjeet Singh and Veda Handa Shrutanjaya Bhardwaj, Nakul Nayak, Raja Venkata Krishna Dandamudi, "Shrutanjaya Bhardwaj , Nakul Nayak , Raja Venkata" *Indian journal of law and technology* (2020).

exercise of Article 21. The Right to Information Act, 2005 enables citizens to access information from public authorities thereby becoming critical aspects of both democratic governance and citizenship empowerment. Information regarding public policies, health services, environmental protection and other welfare measures are critical for protecting the right to life. The RTI Act ensures that citizens have access to such information, thereby supporting the broader interpretation of Article 21. In the digital age, this right includes access to government information and transparency in e-governance initiatives. The RTI Act, 2005 covers central, state and local governments as well as bodies owned, controlled or substantially financed by the government. Any citizen of India can request information by paying a nominal fee. RTI Act has facilitated greater transparency in government operations, exposed corruption and has positively empowered citizens to hold authorities accountable. RTI Laws empower citizens to access government held information. In the digital age, this means that citizens can request and receive information online, promoting transparency and accountability. This also promotes digital literacy as understanding how to access and interpret information online is crucial for digital citizens. RTI encourages development of digital literacy by requiring governments to provide information in accessible digital formats. Digital citizenship emphasizes active engagement in civic activities using digital tools. RTI enables citizens to participate more effectively by providing them with the information needed to make informed decisions and engage in public discourse.

Right to Equality: Article 14 of the Constitution ensures equality before law and equal protection of laws. In the digital realm, this principle is crucial for ensuring non-discriminatory access to digital services and opportunities regardless of their socio-economic status, gender, race or other attributes. The concept of socio-economic justice breathes through this right. This helps influence policies towards digital literary, bridging of the digital divide, and promoting equitable access to digital infrastructure. It ensures that everyone has access to digital tools, addressing concerns of digital divide where certain groups or regions may lack access to technology and connectivity. The Department of Electronics and Information Technology, Government of India has even taken the bold initiative to prepare North East for Digital India. The Digital India has set the pace for a makeover that shall change the face of entire nation, impacting cities, towns and villages. [10]

[10]Department of Electronics and Information Technology, *For Digital* (2014) 19.

Statutory Safeguards

Information Technology Act, 2000

The Information Technology Act, 2000 of India plays a significant role in shaping digital citizenship by providing a legal framework for electronic governance and ensuring secure digital interactions. The key contributions include***: Firstly, Legal Recognition of Electronic Transactions***; the IT Act provides legal recognition to electronic records and digital signatures, facilitating e-commerce and electronic governance. This enables citizens to conduct transactions and interact with the government and businesses online, promoting digital inclusion. This in a way enhances security and trust in Digital Interactions. Securing documents with Digital signatures enhances security of documents in the sense that if any breach of security happens in the midst of transmission of documents the hash values engaged in the asymmetric cryptography system of digital signature would not match. ***Secondly, the IT Act, 2000 facilitates E-Governance***; where the Act provides a framework for electronic governance enabling the government to deliver services online. This enhances accessibility and convenience for citizens, allowing them to access public services and information more efficiently. ***Thirdly, the Act addresses concerns of Cyber Crimes and contraventions throughout India***. Cyber contraventions are basically civil contraventions covered in the IT Act, 2000. Section 43 covers provisions relating to unauthorized access, denial of access, introducing computer contaminants or virus, disrupting computer network, hacking, identity theft, phishing or computer source code theft. The Act defines cyber crimes and prescribes penalties for offenses like identity theft, cyber-terrorism, disclosure of information in breach of lawful contract, cheating by personation, transmission of sexually explicit act, transmission of sexually explicit act depicting minor, etc. Amongst these provision was also the infamous Section 66A i.e., punishment for sending grossly offensive messages online which was later on declared unconstitutional in Shreya Singhal v/s Union of India. National Crime Reports Bureau as per the year 2022 reported a total of 65,893 cases registered under cyber crimes, showing a total increase of 24.4 percent in registration over 2021. As per the Analysis 64.8 percent of the cyber crime cases registered were for the motive of fraud (42, 710 out of 65, 893 cases) followed by Extortion with 5.5 percent (3.648 cases) and sexual exploitation with 5.2 percent (3,

434 cases). The above statistics is with regard to States and Union Territories.[11] Cases included offences in relating to Identity Theft (5740 cases), computer related offences (23894 cases), cheating by personation (13506 cases), Punishment for transmitting and publishing sexually explicit Act (1931 cases) and child pornography (1166 cases). [12]. Inferring from the above report maintaining digital hygiene and sanctity of digital citizenship will go a long way in reducing the crime rates.

Overall, the Information Technology Act, 2000, by providing a robust legal framework, significantly contributes to the development and protection of digital citizenship in India. In enhances security, trust, and accessibility in the digital space, empowering citizens to engage more fully in the digital economy and society.

The Digital Personal Data Protection Act, 2023

The Ministry of Electronics and Information Technology after careful consideration on various aspects of data protection has now formulated and made public the 'Digital Personal Data Protection Act, 2023'. The Act has been carefully categorized into 9 chapters after carefully reviewing the 2019 bill and the 2022 bill aiming to balance the rights of individuals with national and commercial interests. Unlike stricter global regimes, it adopts a relatively soft approach to data localisation, allowing cross border data transfer with governmental supervision fostering trade and e-commerce.

The Act defines roles of data principal and fiduciaries. The Data Principal entails the individual to whom the personal data is related to and the Data Fiduciary who collects, processes and shares the data including in its ambit private companies, social media platforns, universities, employers and governmental agencies. The rights of data principals, such as consent, access, correction, erasure and post mortem privacy are aimed to protect citizens in digital sphere, while also tasking

[11]National Crime Reports Bureau, *Crime in India 2022*, 2022 National Crime Records Bureau, *Crime in India 2022, Volume II* (2022), available at: https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf..
[12]National Crime Records Bureau, *Crime in India 2022, Volume I* (2022), available at: https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf.

fiduciaries with compliance and accountability. What seems noteworthy is how the Act seeks to balance both in favour of national interest as has been discussed in earlier parts of the paper.

Critically, while the Act empowers citizens, it also preserves state primacy through exceptions for national security, law enforcement and public order reflecting the tension between individual privacy and state surveillance highlights in cases like K.S Puttaswamy v Union of India and the Pegasus controversy. The provisions underscore that India's digital citizenship framework remains evolving seeking to safeguard personal freedoms without compromising state authority in digital domain.

Conclusion

The EU's GDPR provides a stronger framework for individual rights, including data minimization, portability and independent oversight. The US model relies more on sectoral regulations, offering weaker privacy safeguards. The Indian DPDP Act somehow falls in between, however it does prioritise state interests over citizen autonomy to larger extent. Constitutional guarantees of equality, free speech and right to information reinforced by the Supreme Court's recognition of informational privacy as a fundamental rights- form the bedrock of digital freedoms for citizens. Complementing these, statutory measures such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide regulatory contours for security, accountability and data protection in digital sphere. However provisions addressing unauthorised access, cyber terrorism and surveillance to preserve national security, public order state about the primary goal of India. Together these provisions illustrate India's attempt to safeguard human rights in cyberspace while addressing the challenges of surveillance, cybercrime and misuse of digital technologies. Yet, the framework in flux, requiring constant recalibration to ensure that digital citizenship strengthens democracy, fosters trust and upholds the dignity of individuals in the 21st century.