THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-29 ISSUE NO:- 29 , NOVEMBER 28, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Digital Number : 2025-23534643
CC BY-NC-SA
Authored By :- Darshan.S
College: Sri Jagadguru Renukacharya College of Law Bangalore

# THE CONSTITUTIONAL CONTOURS OF NON-CONNECTIVITY: REIMAGINING THE "RIGHT TO BE OFFLINE" AND "DIGITAL ANONYMITY" UNDER ARTICLE 21

**Abstract**:

As India transitions into a "Digital First" state, the mandatory nature of digital IDs and pervasive data collection creates a new constitutional tension. This paper explores whether the Right to Privacy, as established in K.S. Puttaswamy (2017), encompasses a reciprocal "Right to be Offline." It further analyzes the "Right to Digital Anonymity" against the backdrop of the Digital Personal Data Protection (DPDP) Act, 2023 and the 2025 Rules, arguing for a constitutional "Opt-Out" mechanism to preserve human dignity in the algorithmic age.

**Keywords**: Article 21, Right to Privacy, Digital Governance, Right to be Offline, Digital Anonymity, DPDP Act, Human Dignity

## Introduction

The Indian Constitution was conceived as a transformative charter, capable of adapting to social, economic, and technological changes while preserving the core values of liberty, dignity, and equality. Article 21, which guarantees the right to life and personal liberty, has been the principal vehicle through which this transformation has occurred. Judicial interpretation has expanded its

scope far beyond mere animal existence to include the right to live with dignity, autonomy, and meaningful choice. In the contemporary era, however, this constitutional guarantee faces a novel challenge arising from the rapid digitisation of governance.

India's transition towards a "Digital First" or "Digital-by-Default" governance model marks a structural shift in how citizens interact with the State. Welfare delivery, identity verification, financial transactions, and access to public services are increasingly mediated through digital platforms. While these initiatives promise efficiency, transparency, and inclusion, they also risk creating new forms of exclusion that are less visible but constitutionally significant. The dependence on digital infrastructure presumes access to technology, digital literacy, stable connectivity, and willingness to participate in data-driven systems—assumptions that do not reflect India's socio-economic realities.

The constitutional concern is not digitisation per se, but compulsion. When digital participation becomes the sole gateway to basic rights such as food, healthcare, pensions, and legal identity, the right to life risks being transformed into a conditional entitlement. This raises a fundamental question: can the State, consistent with Article 21, require citizens to be continuously connected, identifiable, and traceable in order to survive with dignity?

This paper situates this question within the framework of the Right to Privacy as recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). It argues that privacy is not merely a right to control information, but a broader guarantee of decisional autonomy and freedom from forced exposure. From this foundation, the paper develops the concepts of a "Right to be Offline" and a "Right to Digital Anonymity" as necessary constitutional safeguards in an algorithmic state. These rights are presented not as barriers to technological progress, but as essential conditions for preserving human dignity in a digital democracy.

*1.The Digital-by-Default Governance Model in India*

The Indian State's embrace of digital governance has been both ambitious and expansive. Flagship initiatives such as Aadhaar, Unified Payments Interface (UPI), and DigiLocker represent a paradigm shift in administrative functioning, moving governance from physical interfaces to digital platforms. This "Digital-by-Default" model assumes that technology is the

most efficient and desirable medium for State-citizen interaction. However, when examined through a constitutional lens, this assumption reveals significant structural tensions.

Aadhaar has emerged as the foundational digital identity infrastructure in India. Although originally conceived as a voluntary means to improve welfare targeting, Aadhaar has gradually become embedded across multiple sectors, including banking, telecommunications, taxation, and social welfare. Despite judicial pronouncements limiting its mandatory use, the lived reality for many citizens is one of indirect coercion. Authentication failures, biometric mismatches, and lack of connectivity have resulted in exclusion from essential services, particularly for vulnerable populations such as the elderly, disabled, and rural poor.

Similarly, the widespread adoption of UPI has transformed India's financial ecosystem. While digital payments promote convenience and traceability, they also marginalise those who rely on cash due to lack of smartphones, digital literacy, or trust in technology. The gradual discouragement of cash transactions creates an environment where economic participation increasingly depends on digital compliance rather than individual choice.

DigiLocker further exemplifies the shift towards digital identity management. By digitising official documents such as educational certificates and driving licences, the State aims to streamline access and reduce fraud. However, when physical documents are treated as inferior or insufficient, citizens are effectively compelled to enter digital ecosystems irrespective of consent or capability.

Collectively, these initiatives reflect a governance philosophy that prioritises efficiency over choice. The constitutional issue arises when digital systems are not offered as options but imposed as defaults. In such a framework, the absence of offline alternatives transforms administrative modernisation into a form of structural exclusion, raising serious concerns under Article 21's guarantee of life with dignity.

*2. Article 21 and the Centrality of Choice*

At the heart of Article 21 lies the principle that life and liberty must be meaningful, not merely symbolic. The Supreme Court has consistently held that the right to life encompasses more than physical survival; it includes the conditions necessary for human dignity, autonomy, and

self-determination. Choice is a central component of this constitutional vision. Without choice, liberty becomes illusory and dignity hollow.

In K.S. Puttaswamy, the Court explicitly recognised that privacy is grounded in individual autonomy and the freedom to make personal decisions without undue State interference. This recognition has profound implications for digital governance. If privacy protects the individual's control over personal information and life choices, then a governance model that eliminates non-digital alternatives directly undermines this protection.

When access to essential services such as food distribution, healthcare, pensions, or identity verification is contingent upon digital authentication, the individual is deprived of meaningful choice. Consent in such circumstances is not voluntary but compelled by necessity. The constitutional harm arises not merely from data collection, but from the denial of alternatives that respect individual autonomy.

Forced digital participation also raises substantive due process concerns. Any procedure that affects life or liberty must be just, fair, and reasonable. A system that excludes individuals due to technological barriers, biometric failure, or lack of connectivity fails this test. The State's obligation under Article 21 is not only to provide services, but to ensure that access mechanisms do not themselves become instruments of deprivation.

Thus, the erosion of choice through digital compulsion represents a direct challenge to the constitutional promise of liberty. A rights-based constitutional order cannot permit the transformation of citizens into passive subjects of technological systems. Choice is not a luxury; it is the foundation of freedom. When choice is removed, the right to life under Article 21 is fundamentally compromised.

*3.The Right to be Offline as an Extension of Privacy*

The concept of a "Right to be Offline" emerges naturally from the constitutional understanding of privacy as autonomy and control. It does not imply rejection of technology or opposition to digital governance. Rather, it asserts the individual's right to limit digital engagement and resist compulsory connectivity. In an era of pervasive surveillance and data-driven decision-making, the ability to remain offline is integral to preserving personal dignity.

Privacy, as articulated in Puttaswamy, includes the right to determine when, how, and to what extent personal information is shared. Continuous digital participation erodes this control by subjecting individuals to constant monitoring, profiling, and data aggregation. The absence of offline alternatives effectively forces citizens into a permanent state of digital exposure, undermining the very essence of informational self-determination.

The Right to be Offline also protects psychological autonomy. Constant digital engagement can create a sense of coercion and vulnerability, particularly when identity verification and data sharing are unavoidable. For many individuals, especially those from marginalised communities, digital systems represent not empowerment but surveillance and exclusion.

Comparative constitutional perspectives reinforce this argument. While jurisdictions such as the European Union have focused on data protection and consent, the underlying principle remains the preservation of human dignity against technological overreach. India's constitutional framework, with its emphasis on substantive due process and dignity, is well-suited to recognise a similar right grounded in Article 21.

Recognising the Right to be Offline ensures that technology remains a tool of governance rather than its master. It preserves the balance between innovation and individual freedom, ensuring that digital progress does not come at the cost of constitutional values.

*4.Digital Anonymity and the DPDP Act, 2023*

Digital anonymity is an essential but often overlooked component of constitutional freedom. It allows individuals to engage, express, and transact without constant identity verification. Anonymity protects dissent, experimentation, and psychological security, particularly in digital spaces where surveillance is pervasive. Under Articles 19 and 21, anonymity is closely linked to free expression and personal liberty.

The Digital Personal Data Protection Act, 2023 represents India's first comprehensive attempt to regulate personal data processing. While the Act introduces important safeguards such as purpose limitation and consent-based processing, it operates within a framework that assumes digital participation as inevitable. Consent, in this context, is often formal rather than substantive, especially when access to essential services is conditioned upon acceptance of data processing terms.

The Act does not adequately recognise the value of anonymity-preserving systems or the right to transact without identification where identity is unnecessary. Mandatory identification for routine digital interactions increases the risk of profiling and creates chilling effects on speech and association.

From a constitutional perspective, the absence of anonymity safeguards undermines dignity and autonomy. A democratic society must allow spaces where individuals can exist without constant traceability. Digital anonymity, therefore, should be viewed as a constitutional interest flowing from the right to privacy and life under Article 21.

*5. Constitutional Opt-Out Framework*

To reconcile digital governance with constitutional values, this paper proposes a constitutionally grounded opt-out framework. Such a framework ensures that digital systems remain inclusive without becoming coercive. The proportionality test laid down in Puttaswamy requires the State to adopt the least intrusive means to achieve legitimate objectives. Mandatory digitisation without alternatives fails this test.

An opt-out framework would require the State to provide parallel offline access to all essential services. It would also mandate anonymity-preserving mechanisms where identity is not essential. Importantly, the burden would lie on the State to justify why digital-only access is necessary in specific contexts.

*6. Digital Divide as a Constitutional Inequality*

The Digital-by-Default governance model deepens existing socio-economic inequalities rather than eliminating them. India's digital divide is not merely about access to devices or internet connectivity; it is a layered phenomenon involving literacy, language barriers, disability, age, geography, and gender. When digital access becomes a prerequisite for exercising fundamental rights, structural inequality is constitutionalised. Article 21, read with Article 14, prohibits indirect discrimination arising from ostensibly neutral policies that disproportionately harm vulnerable groups. The failure to account for unequal digital capacity converts administrative efficiency into constitutional exclusion. A right that is theoretically universal but practically inaccessible ceases to be a right in substance.

*7.Algorithmic Governance and the Erosion of Human Agency*

Digital governance increasingly relies on algorithmic decision-making for welfare eligibility, risk assessment, and identity verification. Algorithms operate on predefined datasets and logic structures that often lack transparency and contextual sensitivity. When human decision-making is replaced or overridden by automated systems, individuals lose the ability to explain, contest, or correct errors. This erosion of agency directly impacts dignity under Article 21. The Constitution envisages governance that is accountable and humane, not opaque and automated. A Right to be Offline functions as a safeguard against the dehumanisation of governance by restoring human discretion and accountability.

*8. Surveillance State Concerns and Chilling Effect*

Mandatory digital participation enables continuous data generation and aggregation, facilitating surveillance without proportional safeguards. Even in the absence of overt misuse, the knowledge of being constantly monitored produces a chilling effect on speech, association, and personal behaviour. Constitutional freedoms lose their vitality when citizens self-censor due to fear of traceability. The Right to Digital Anonymity mitigates this chilling effect by preserving zones of unobserved existence. Article 21 protects not only physical liberty but also mental freedom, which cannot survive under omnipresent surveillance.

*9.Consent Fatigue and the Myth of Informed Consent*

The DPDP Act, 2023 relies heavily on consent as the legitimising basis for data processing. However, in a digital ecosystem where consent is required repeatedly and compulsorily, consent loses its normative value. Individuals mechanically accept terms without understanding implications, a phenomenon known as “consent fatigue.” When refusal results in denial of essential services, consent becomes a legal fiction. Constitutional consent must be meaningful, voluntary, and revocable. A Right to be Offline restores consent by allowing refusal without punitive consequences, thereby aligning statutory frameworks with constitutional morality.

*10. Impact on Vulnerable and Marginalised Communities*

Digitisation disproportionately affects senior citizens, persons with disabilities, transgender persons, nomadic communities, and those without stable documentation. Biometric failures,

linguistic limitations, and lack of assistive technologies often result in denial of services. Article 21 imposes a positive obligation on the State to protect the most vulnerable. A governance model that prioritises technological efficiency over human accommodation violates this obligation. The Right to be Offline ensures that constitutional protections remain inclusive rather than technologically select.

## 11.**Conclusion**

India's digital transformation is irreversible and, in many ways, desirable. However, constitutionalism demands that progress remain anchored in human dignity and freedom. Article 21 cannot be reinterpreted to mean that life and liberty are available only to those who are digitally compliant.

The Right to be Offline and the Right to Digital Anonymity are not radical innovations but logical extensions of established constitutional principles. They reaffirm that choice is the essence of liberty and dignity its ultimate goal. In an algorithmic age, these rights ensure that the Constitution continues to protect the individual against both traditional and technological forms of State power.