

Algorithmic Ostracism: India's Digital Personal Data Protection (DPDP) Act, 2023 and the Constitution

Shivam Yadav¹

ABSTRACT

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India transformed Indian constitutional jurisprudence by affirming informational privacy as an essential component of individual autonomy and dignity. However, the permanence of digital records has created a new constitutional challenge that this paper conceptualizes as “Algorithmic Ostracism”, the systematic social, economic, and psychological exclusion of individuals through the perpetual circulation and algorithmic processing of personal data. The article examines two principal manifestations of this phenomenon: first, doxxing and online public shaming, which compromise bodily security, mental well-being, and personal dignity; and second, automated background verification systems that enable economic exclusion using historical and contextually irrelevant personal information.

Through a critical analysis of the Digital Personal Data Protection Act, 2023, the paper argues that the Act fails to adequately address harms arising from third-party data aggregation, search engine indexing, and automated decision-making. In particular, Section 12(3)'s limited right to erasure and the broad employment-related exemptions under Section 7 leave citizens vulnerable to enduring digital stigma. Drawing upon constitutional principles established in Puttaswamy and emerging judicial recognition of the Right to be Forgotten, the paper advocates for statutory de-indexing mechanisms and stronger data erasure rights to secure a meaningful constitutional “right to a clean slate” in the digital age.

KEYWORDS

Algorithmic Ostracism, Informational Privacy, Digital Erasure, Data Protection, Constitutional Dignity

¹ Student at Marathwada Mitra Mandal Shankarrao Chavan law College, Pune, Maharashtra.

INTRODUCTION: THE CONSTITUTIONAL PROMISE VS. DIGITAL IMMUTABILITY

The landmark declaration of privacy as an inalienable fundamental right under Article 21 of the Constitution of India² in *Justice K.S. Puttaswamy v. Union of India* (2017)³ marked a watershed moment in global jurisprudence. The Supreme Court observed that privacy is the ultimate guarantee of individual autonomy, shielding a citizen's core choices from both state and non-state interference. Central to this structural autonomy is the concept of 'informational privacy', the absolute right of an individual to control their digital identity and determine what aspects of their life are disseminated across public spaces.

Historically, human societies relied on the natural fragility of human and institutional memory to function equitably. The inability to recall every past misstep allowed individuals to outlive ancient mistakes, re-invent their socioeconomic standing, and seek personal and professional rehabilitation. However, the rise of modern digital architectures has flipped this historical paradigm. Today, the digital commons operate under a rule of absolute, permanent, and unyielding memory. When highly contextual personal data points, ranging from old student political affiliations to wrongful accusations or non-consensual private images are scraped, indexed, and cached by search engines or commercial data brokers, they become permanent digital tattoos.

This paper argues that this immutable permanence creates a severe and novel constitutional injury, termed as Algorithmic Ostracism. By critically analysing the structural boundaries of the Digital Personal Data Protection (DPDP) Act 2023, this article evaluates how state inaction against third-party data scraping systematically dismantles the horizontal protections implicit in the Puttaswamy ruling. Without an enforceable mechanism to demand a clean digital slate, the fundamental right to life with dignity is rendered entirely illusory for citizens trapped in a perpetual, commercialised digital panopticon.

VECTOR ONE: DOXXING, PUBLIC SHAMING, AND THE THREAT TO BODILY PRIVACY

The first vector of Algorithmic Ostracism manifests as malicious, targeted cyber-harassment, most prominently through the phenomenon of 'doxxing,' defined as the non-consensual

² INDIA CONST. art. 21.

³ Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

aggregation, cross-referencing, and online publication of private, identifying data. While contemporary public discourse frequently treats doxxing as an unfortunate but minor internet nuisance, it functions as a profound constitutional infraction. When bad actors exploit automated scripts to scrape public registries, corporate filings, old residential addresses, and private contact information to orchestrate viral public shaming campaigns, the injury is deeply structural.⁴

Under the Puttaswamy doctrine, privacy is not an abstract, ivory-tower concept; it is intrinsically linked to bodily security, psychological integrity, and mental peace. Doxxing destroys this protective barrier, inviting digital harassment directly into an individual's physical home and workplace. This phenomenon is deeply gendered and asymmetrical, routinely weaponised to silence women, activists, journalists, and marginalised communities.

The core legal failure lies within the current statutory landscape. When victims seek remedies under the Information Technology Act, 2000 (such as Section 66E for privacy violations), technology intermediaries and bad actors routinely hide behind the "Public Domain Exception." They argue that if a piece of data was scraped from an open public land record, a government voter list, or a historical, public social media profile, it can no longer be protected by privacy laws.

This defence directly violates the Supreme Court's reasoning in Puttaswamy, which explicitly established that an individual does not completely surrender their privacy simply by stepping into a public space or sharing information for a specific, limited purpose. The complete absence of an independent, accessible "Right to be Forgotten" means that even if a victim manages to survive an immediate wave of public shaming, the digital footprint remains permanently indexed on dominant search engines, leaving their personal security perpetually exposed to any future bad actor or blackmailer with an internet connection.

VECTOR TWO: ECONOMIC OSTRACISM VIA AUTOMATED BACKGROUND VERIFICATION SYSTEMS

While doxxing targets physical and psychological safety, the second vector of Algorithmic Ostracism quietly attacks economic survival through automated corporate background verification and algorithmic curriculum vitae sifting. Modern human resource departments,

⁴ A. T. Chen et al., Audience Responses to Online Public Shaming in Social Media Contexts, 28 *Cyberpsychology, Behavior, and Social Networking* (2025), <https://pmc.ncbi.nlm.nih.gov/articles/PMC12329387/>.

driven by cost-efficiency, increasingly rely on automated AI crawlers to scan an applicant's digital history before hiring. These systems scrape information indiscriminately from deep web archives, court registries, and social platforms without contextual parameters.

This practice poses a major threat to the fundamental right to practice a profession under Article 19(1)(g)⁵ and equal employment opportunities under Article 16.⁶ If a background crawler pulls up an old, long-settled financial dispute, an expunged juvenile record, or a photograph from a decade-old college protest, the algorithm automatically drops the candidate from the hiring pipeline. The candidate is quietly blacklisted without ever being contextualised, or even understand why they were rejected.

This economic exclusion highlights a massive loophole within the DPDP Act, 2023. Under Section 7 of the Act,⁷ data processing for 'employment purposes' is exempted from several stringent consent requirements. This statutory loophole allows corporate entities to passively exploit a citizen's past data under the guise of corporate compliance and risk management.

This framework creates a permanent underclass of citizens who are completely locked out of the formal economy because of a digital record they can neither change nor escape. It effectively deprives them of their right to financial rehabilitation, violating the core constitutional principle that any restriction on economic liberty and livelihood must meet a strict threshold of reasonableness, fairness, and non-arbitrariness.

THE INADEQUACY OF THE DPDP ACT, 2023 AND THE NEED FOR THE RIGHT TO BE FORGOTTEN

DPDP Act, 2023 was intended to provide a robust framework for data protection, but its treatment of the Right to the Erasure under Section 12(3)⁸ is deeply flawed and unequipped for the modern internet. Section 12(3) only allows an individual to request data erasure from a 'Data Fiduciary' if they actively withdraw their original consent, or if the data is no longer necessary for the specific purpose for which it was originally collected.

This mechanism is entirely unequipped to handle third-party data brokers, aggregators, and search engines. A regular citizen has no realistic way to track down, identify, and withdraw consent from thousands of shadow data brokers who scraped their information without their

⁵ INDIA CONST. art. 19, § 1(g).

⁶ INDIA CONST. art. 16.

⁷ Digital Personal Data Protection Act, No. 22 of 2023, § 7 (India).

⁸ Digital Personal Data Protection Act, No. 22 of 2023, § 12(3) (India).

knowledge. The DPDP Act entirely misses the point by putting the burden of erasure on the victim rather than forcing data aggregators to automatically wipe out old records after a set period.

Furthermore, India lacks a free-standing, universally applied 'Right to be Forgotten' like the European Union's GDPR Article 17⁹. While the Delhi High Court acknowledged the right in *Jorawar Singh Mundy v. Union of India* (2021)¹⁰ ordering the removal of an old court judgment that ruined an acquitted man's career the remedy remains scattershot, expensive, and dependent on filing individual, exhausting lawsuits.

Without a clear, systemic statutory right to demand that search engines de-index irrelevant historical data, Section 12(3) of the DPDP Act remains an incomplete shield, completely failing the proportionality standard laid down by the Supreme Court.

CONCLUSION: TOWARDS A CONSTITUTIONAL CLEAN SLATE

A legal system that does not allow its citizens to digitally log off and start anew turns the internet into a lifelong digital prison. Algorithmic Ostracism directly undermines the constitutional promise of human dignity, personal liberty, and equal opportunity.

To bring Indian data law into strict compliance with the Puttaswamy judgment, the Data Protection Board of India (DPBI) and the judiciary must expand the Right to Erasure into a true Right to be Forgotten. We must implement clear legislative policies:

Mandatory Look-Back Limits: Forcing background verification companies and corporate hiring tools to ignore non-felony personal data older than five years.

Statutory De-indexing Frameworks: Empowering citizens to directly request search engines to remove outdated, harmful, or non-consensual personal links from public search results without requiring expensive litigation.

Only by recognising the right to a clean slate can the law restore horizontal equity, protect vulnerable citizens from online harassment, and ensure that technology serves as a tool for human progress rather than an absolute, unyielding mechanism of social exclusion.

⁹ Regulation (EU) 2016/679, art. 17.

¹⁰ *Jorawar Singh Munday v. Union of India*, 2021 TMI 792 (DEL HC).