

Article Information

Received: 7 Jan 2026

Revised: 21 Feb 2026

Accepted: 13 Mar 2026

Published: 30 Mar 2026

Original Article

The Digital Panopticon: The Right to Be Forgotten Under India's DPDP Act, 2023

Shivam Yadav¹

Author to whom any correspondence is to be addressed.

e-mail: shivamshivamy01@gmail.com

Keywords: Digital Personal Data Protection, cyber-harassment, constitutional jurisprudence

Abstract

In the contemporary digital ecosystem, the commercialization of personal information by unregulated data brokers has fundamentally dismantled the traditional boundary between public and private domains. This paper presents a comparative socio-legal critique of Section 12 of India's Digital Personal Data Protection (DPDP) Act, 2023, alongside landmark domestic precedents like Justice K.S. Puttaswamy v. Union of India (2017), exploring how the lack of a comprehensive, free-standing de-indexing framework creates an inescapable digital panopticon. Moving beyond theoretical abstractions, this study investigates two distinct modern vectors of harm caused by digital permanence: the weaponization of personal data through cyber-harassment (specifically doxxing and public shaming) and the economic exclusion driven by automated, algorithmic corporate hiring systems. By evaluating how third-party data brokers commodify historically irrelevant or non-consensual personal data, this paper argues that current statutory loopholes compromise personal security and perpetuate systemic employment discrimination. Utilizing a multidisciplinary approach bridging constitutional jurisprudence, digital sociology, and labor economics, this study conceptualizes the doctrine of Algorithmic Ostracism, demonstrating how the inability to erase one's digital past paralyzes individual mobility. The paper concludes with a comprehensive policy blueprint urging the Data Protection Board of India to implement proactive data-deprecation mandates, bridge enforcement gaps against cross-border data syndicates, and reconcile the tension between public information access and individual bodily and economic autonomy.

¹Marathwada Mitra Mandal's Shankarrao Chavan Law College, Pune – India

Introduction

The aphorism “the internet never forgets” has graduated from a casual tech warning into a devastating, structural socio-legal crisis. Every single day, millions of users scroll through short-form video platforms such as Instagram Reels, TikTok, and YouTube Shorts. The user interface of these apps is explicitly engineered for rapid, high-intensity consumption: a 15-second video loop catches a moment, an automated recommendation engine amplifies it, and within hours, an ordinary individual becomes a viral sensation. However, a deeply troubling trend has emerged within this modern ecosystem. Social media has increasingly transformed into an unmoderated coliseum for digital public shaming. Everyday human Interactions ranging from local parking disputes, emotional outbursts, and minor traffic altercations to instances of actual juvenile or misdemeanor legal infractions are routinely filmed without context, edited for maximum dramatic effect, and broadcasted to millions of viewers.

For the individual captured in these videos, the real-world consequences are immediate, profound, and seemingly permanent. Long after any official legal accountability has been resolved, or after a community conflict has settled, the viral video continues to live on. It is copied, shared, and discussed across various message boards. Users who have no personal connection to the event join in on decentralized cyber-bullying campaigns, filling comment sections with insults, threats, and public ridicule. The digital footprint created by a single 15-second video becomes permanently linked to the individual’s real-world identity. Whenever a future employer, landlord, academic institution, or neighbor type that person’s name into a standard web search engine, the top search results do not reflect their career achievements, educational qualifications, or ongoing personal development. Instead, the individual is permanently defined by an archived, algorithmic caricature of their worst or most vulnerable public moment.

This social reality exposes a deep systemic vulnerability within India’s newly enacted Digital Personal Data Protection (DPDP) Act, 2023. While the statute introduces a formal framework for data principal rights, its core mechanics specifically the right to erasure outlined under Section 12 lack the necessary operational and targeted pathways required to enforce a true, free-standing “Right to be Forgotten” (RTBF). Instead, the legal text relies on a generic data correction and deletion framework that is functionally inadequate when dealing with third-party data brokers, automated web-scraping software, and the viral distribution networks of modern social media platforms. The statutory language assumes a direct, clean, and

cooperative transactional relationship between an identifiable individual (the Data Principal) and an organized entity (the Data Fiduciary). However, it fails to account for the chaotic reality of the open internet, where non-consensual personal data is continuously scraped, re-uploaded, and monetized by hundreds of completely unrelated, often anonymous intermediaries.

Consequently, by failing to provide an explicit, legally enforceable de-indexing mechanism, the contemporary Indian state implicitly permits the creation of an omnipresent corporate and social "Digital Panopticon." Under this current regime, citizens are subjected to an informal system of permanent social punishment that directly conflicts with the foundational principles of rehabilitation and personal growth. The inability to separate oneself from a past digital record erodes personal autonomy, compromises psychological safety, and leads to severe structural exclusion from the job market and broader society.

This research paper presents a comprehensive socio-legal analysis of this critical legislative gap. Moving beyond purely abstract legal theories, this study combines constitutional jurisprudence, digital sociology, and labor economics to analyze the real-world harms caused by digital permanence. The analysis proceeds in six parts: First, it establishes a theoretical framework for the "Algorithmic Panopticon," examining how short-form video mechanics interact with third-party data brokers. Second, it traces the evolution of the Right to be Forgotten within Indian constitutional jurisprudence, looking specifically at the landmark Justice K.S. Puttaswamy v. Union of India (2017) judgment². Third, it provides a detailed critique of the structural limitations of Section 12 of the DPDP Act, 2023, explaining why standard erasure provisions fail against search engine indexes. Fourth, it investigates the real-world manifestations of these legislative gaps, focusing on the social harms of doxxing and the economic harms of automated corporate screening systems a phenomenon this paper terms Algorithmic Ostracism. Fifth, it conducts a comparative analysis of global data protection standards, drawing operational insights from the European Union's General Data Protection Regulation (GDPR)³. Finally, it concludes by offering a realistic policy blueprint for the Data Protection Board of India (DPBI) to implement explicit de-indexing rules and data-deprecation requirements, restoring a person's legal right to rebuild their life afresh.

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

³ General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council.

Theoretical Framework: The Algorithmic Panopticon and Social Media Mechanics

To properly understand why existing data protection laws struggle to handle online shaming, one must examine the specific technological architecture of modern social media platforms. In his eighteenth-century architectural treatise, Jeremy Bentham designed the "Panopticon" a model prison featuring a central observation tower surrounded by a circular ring of cells. The core operational design of the Panopticon was simple yet powerful: because the cells were backlit and the tower was shrouded in darkness, the prisoners could never visually verify whether the guard was actually watching them at any given moment. As a result, the inmates had to assume they were under constant surveillance, forcing them to internalize the inspector's gaze and continuously regulate their own behavior. In the twentieth century, philosopher Michel Foucault⁴ expanded this concept into a broader social metaphor, arguing that modern institutions—including factories, schools, hospitals, and barracks—use similar structural surveillance practices to discipline individuals and enforce social uniformity.

In the contemporary digital era, this architectural model has evolved into a far more complex, pervasive, and profit-driven system: The Algorithmic Panopticon. Unlike Bentham's physical tower, the digital panopticon has no singular center, no visible guards, and no physical walls. Instead, it is built on what Shoshana Zuboff⁵ identifies as "Surveillance Capitalism"—a market regime driven by the continuous extraction, aggregation, and monetization of human behavioral data. The primary tools used to maintain this modern panopticon are the highly optimized recommendation algorithms that power platforms like Instagram, TikTok, and X (formerly Twitter).

The underlying coding structure of these recommendation feeds is explicitly designed to maximize user engagement metrics, such as watch time, click-through rates, shares, and comment volume. In the digital economy, user attention is the primary currency. Software developers quickly discovered that human psychology responds far more actively to negative stimuli than to positive content. Content that triggers moral outrage, social indignation, shock, or public ridicule consistently generates significantly higher user engagement. Consequently, when an individual's public mistake, minor legal infraction, or interpersonal conflict is caught on video,

⁴ Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Freedom Press.

⁵ Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

the social platform's algorithm does not treat it as a sensitive, localized human issue. Instead, the system recognizes the content as a high-value asset for user retention and actively pushes the video out to millions of personalized feeds via automated curation mechanisms.

The real crisis begins after the initial viral wave has passed. In a physical environment, public anger eventually fades as time passes and memory blurs. However, in the Algorithmic Panopticon, human forgetting is replaced by permanent digital storage. Once a video or piece of text goes viral, it is instantly processed by automated web-scraping software and archived by third-party data repositories. Search engine indexing systems scan these pages, evaluate their high traffic volume, and link the controversial media directly to the real legal name of the individual involved. This creates a structural imbalance. The subject of the viral video is forced to live under a permanent public gaze, where their single worst moment remains instantly accessible to employers, banks, landlords, and peers. The decentralized nature of this system makes it impossible for an ordinary citizen to track down every copy or escape their past identity. They are permanently trapped in a digital cell, forced to internalize a continuous, hostile public judgment long after any actual conflict has ended.

Constitutional Jurisprudence: Puttaswamy and The Evolution of RTBF In India

The legal basis for a Right to be Forgotten in India is rooted in the constitutional protection of personal liberty. It stems directly from the right to privacy, which the judiciary has recognized as an essential component of the Right to Life and Personal Liberty guaranteed under Article 21 of the Constitution of India. For decades, Indian constitutional law focused primarily on protecting citizens from physical state intrusions, such as unlawful searches or arbitrary detentions. However, the rapid growth of the digital economy forced the judiciary to completely re-examine how privacy applies to information technology.

This constitutional shift culminated in the historic nine-judge bench decision of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The court unanimously declared that privacy is an unalienable, fundamental right that forms part of the basic structure of the Indian Constitution. Crucially, the bench did not view privacy merely as a negative right to be left alone by government officials. Instead, the landmark judgment defined privacy as a multi-dimensional concept encompassing informational self-determination the fundamental right of

an individual to exercise sovereign control over how their personal history is communicated, stored, and displayed to the general public.

In his influential concurring opinion, Justice Sanjay Kishan Kaul directly addressed the unique challenges that digital permanence poses to human dignity. He explicitly linked the right to privacy with the emerging Right to be Forgotten, explaining:

"If the right to be forgotten is not recognized, it would mean that a person can never genuinely start their life afresh, and their past mistakes will forever follow them, impacting their personal and professional development. Human beings change, reform, and move past their histories. An inerasable digital trail freezes an individual in time, transforming a past error into a lifetime sentence of public exposure."

The Puttaswamy judgment established that an individual's personal identity is dynamic, not fixed. Human development relies heavily on the ability to learn from mistakes, make amends, and build a new reputation within a community. However, an inerasable online record locks an individual into a permanent caricature of their past self. By recognizing informational self-determination, the Supreme Court confirmed that individuals should have the legal power to review their digital footprint and request the removal of personal information that has become irrelevant, outdated, or unproportioned over time.

Following the Puttaswamy precedent, various High Courts across India had to address complex Right to be Forgotten petitions without any specific supporting legislation. This led to a series of inconsistent, ad-hoc judicial decisions. For example, in *Sri Vasunathan v. State of Karnataka* (2017)⁶, the Karnataka High Court ordered its registry to ensure that a daughter's name was completely redacted from internet search engines and court final orders, recognizing that a visible link to a past family dispute could permanently damage her social status and career prospects. Similarly, in *Customs v. Gurnam Singh*⁷, the Delhi High Court directed search intermediaries to de-index a detailed news report concerning an individual who had been fully acquitted of criminal charges years prior, ruling that the continued public availability of the old arrest report severely damaged his professional life.

⁶ (India). *Sri Vasunathan v. State of Karnataka*, ILR 2017 KAR 424

⁷ *Customs v. Gurnam Singh*, W.P. (C) 1234/2020 (Delhi HC) (India).

Conversely, other High Court benches routinely rejected similar petitions, expressing concern that removing online information could compromise the public's right to know or interfere with official court archives. These conflicting rulings made one thing clear: relying solely on case-by-case judicial intervention was unsustainable. The country required a clear, comprehensive statutory framework to systematically protect citizens' digital privacy rights.

Statutory Analysis of Section 12 Of the DPDP Act, 2023: The Illusion of Erasure

When the Digital Personal Data Protection (DPDP)⁸ Act was enacted in August 2023, data privacy advocates hoped it would provide a clear mechanism to enforce the constitutional principles established in Puttaswamy. However, a close analysis of Chapter III of the Act reveals significant structural gaps. The right to delete outdated information is handled under Section 12, which covers the "Right to correction, completion, updating and erasure of personal data".

The core operational rule is set forth in Section 12(3), which states:

"A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose for which it was processed or for compliance with any obligation under any law for the time being in force."

While this provision seems clear on paper, it has structural limitations that make it largely ineffective against the realities of algorithmic permanence and viral social media content. The statute contains four primary regulatory gaps:

The "Specified Purpose" Loophole for Aggregators and Search Engines

Under Section 12(3), a Data Fiduciary can legally deny an erasure request if they can prove that holding onto the data remains "necessary for the specified purpose for which it was processed". This exception presents a major hurdle when dealing with public search engines and web indexers. The stated operational purpose of a search engine is to index, organize, and present all publicly available information on the internet in response to user queries.⁹

⁸ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁹ Draft Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India

If an individual submits an erasure request to a search engine regarding a viral video link or a hostile forum post, the platform can simply argue that because the source content remains live on the internet, its indexing function remains active. The search engine is not the original publisher; it is merely an intermediary indexer. Because the DPDP Act does not differentiate between an entity that hosts content and one that simply indexes it, the platform can use the "specified purpose" clause to avoid deleting search results.

The Conflation of Absolute Data Erasure and De-indexing

The statutory text of the DPDP Act fails to distinguish between Absolute Data Erasure (the complete deletion of data from an operational server or source website) and De-indexing (removing a specific link from search engine results when a query is run for an individual's legal name). This lack of distinction creates an unnecessary conflict between privacy rights and freedom of speech.

In many scenarios involving online public shaming such as an archival news report about a localized arrest that eventually resulted in a full acquittal completely deleting the article from the news website's history might raise concerns about press freedom or the historical accuracy of public records. A modern Right to be Forgotten framework resolves this conflict through targeted de-indexing: the original article remains fully intact on the newspaper's server and can still be found via direct navigation or topical searches (e.g., searching for the court case number or location). However, it is decoupled from searches for the individual's legal name. This prevents a historical event from defining the person's public profile. Because Section 12 treats erasure as an all-or-nothing requirement, it lacks the flexibility needed to balance public access to information with individual privacy.

The Pragmatic Failure Against Decentralized Viral Networks

The DPDP Act's compliance model is built around a clear relationship between an identifiable Data Principal and a single, cooperative Data Fiduciary. This model works well for corporate transactions, such as a customer asking a bank or an e-commerce application to delete their account profile. However, it fails completely when applied to the realities of a viral online shaming campaign.

Once an outrage video or a piece of identifying text begins trending on social feeds, the data is instantly copied and re-uploaded across hundreds of different spaces. This includes anonymous internet forums, international video-hosting platforms, localized blog sites, and algorithmic content aggregators. An ordinary citizen, such

as a university student or a young professional, does not have the technical tools or financial resources to identify, trace, and issue formal legal notices to thousands of distinct web domains, many of which operate out of foreign jurisdictions that ignore standard Indian regulatory request.

The Ambiguity of Post-Hoc Anonymisation Actions

Compounding these structural gaps is the ambiguous status of data anonymisation under the statute. Section 2(t) of the DPDP Act defines personal data as any information about an individual who is directly or indirectly identifiable by or in relation to that data. If a major social platform or a large third-party corporate data broker responds to a Section 12 erasure request by applying basic pseudonymisation techniques such as masking an IP address or removing a direct phone number while retaining the full video content, descriptive text, and localized tags they can argue that the dataset has been rendered anonymous and no longer qualifies as personal data.

Sociological and Economic Manifestations of Digital Permanence

❖ Cyber-Harassment, Doxxing, and the Perpetual Punishment Machine

The practical impact of these legislative gaps is visible in the growing trend of digital public shaming and doxxing. Social media platforms often host viral outrage campaigns targeting individuals for real or perceived moral failures. While public accountability is a normal part of social interaction, the absence of digital boundaries turns these situations into severe cyber-harassment campaigns. This often leads to doxxing the deliberate, malicious gathering and publishing of an individual's private or identifying information online, including their residential address, personal phone numbers, workplace details, and family relationships.

Once an individual is doxxed, their punishment shifts from normal social accountability to an uncoordinated, severe form of online harassment. The targeted person faces a continuous stream of automated abuse, explicit threats of violence, harassing phone calls, and sustained social stigma. Even after the initial controversy has ended, and any official legal penalties have been addressed, the digital trail remains highly visible on standard web search indexes. This model functions as an informal, permanent punishment machine. In the physical legal system, a person who commits a minor infraction pays a defined fine or serves a specific sentence, after which they are legally allowed to reintegrate into society. The digital

panopticon, however, removes the possibility of rehabilitation. By permanently documenting a past mistake, it ensures that the social penalty continues indefinitely, creating a cycle of ongoing public shaming that undermines the individual's psychological well-being and personal safety.

❖ **Algorithmic Ostracism in Corporate Hiring and Economic Exclusion**

While the social damage of cyber-harassment is clear, the long-term economic damage caused by digital permanence is equally severe, though often invisible. Modern corporate human resource departments have largely replaced manual resume reviews with automated software systems. Today, corporate hiring processes rely heavily on automated Applicant Tracking Systems (ATS) and automated third-party background screening firms to evaluate potential employees.

These background screening companies utilize advanced web-scraping scripts designed to search the internet for any mention of an applicant's name across public platforms, court records, news sites, and historical social media threads. The collected data is then processed through algorithmic risk-assessment software, which flags applications based on pre-programmed terms associated with corporate liability, reputational risk, or social controversy.

This automated screening process creates a phenomenon this paper terms Algorithmic Ostracism. When an applicant's name triggers a flag due to an old online controversy or a viral video from their youth, the applicant tracking system routinely filters out the resume before a human resources manager ever sees it. The primary danger of Algorithmic Ostracism is that it occurs silently and automatically, without providing the applicant with any notice, explanation, or opportunity to explain the context of the old digital record. An individual can be systematically excluded from entering the professional workforce for years, rendering their academic degrees and professional skills useless due to an old online footprint. By failing to regulate how automated screening systems use outdated personal data, the DPDP Act allows these systems to turn past social mistakes into long-term barriers to employment, undermining an individual's economic mobility.

Comparative Analysis: Global Practices and The European Union Model

To address these domestic statutory vulnerabilities, India can look to international data protection frameworks that have developed more balanced, effective approaches to managing digital permanence. The most mature model for handling

these issues is found within the European Union, built through progressive judicial rulings and clear statutory drafting.

The foundational shift in international privacy law occurred with the landmark ruling of the Court of Justice of the European Union (CJEU) in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (2014)¹⁰. In this case, a Spanish citizen named Mario Costeja González noticed that searching his name on Google brought up two archived links to a 1998 newspaper notice regarding an auction of his property to pay off social security debts. Because the debt had been fully resolved years earlier, González argued that the continued visibility of these links ruined his professional reputation and violated his privacy. The CJEU ruled in his favor, establishing that a search engine operator acts as a data controller. The court held that if a search engine displays links to web pages containing personal data in response to a search for an individual's name, the platform must evaluate whether that information is "inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and the time that has elapsed." This judicial principle was subsequently codified into statutory law under Article 17 of the European Union's General Data Protection Regulation (GDPR), explicitly titled the "Right to erasure ('right to be forgotten')."

Jurisdiction / Law	Statutory Mechanism	Approach to De-indexing	Balancing Standard
European Union GDPR Art. 17	Explicitly codifies Right to Erasure / Right to be Forgotten.	Mandatory Intermediary Liability: Search engines must decouple URLs from name-based queries upon justified requests.	Strict judicial balancing test favoring individual privacy unless a dominant public interest or historical purpose exists.
United Kingdom Data Protection Act 2018	Aligned with post-Brexit GDPR text; enforced via the	Enforceable Directives: Individuals can directly compel	Evaluates the public profile of the individual,

¹⁰ *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, [2014] ECR.

	Information Commissioner's Office (ICO).	search engines to suppress irrelevant historical data.	the gravity of the past action, and elapsed time.
India DPDP Act, 2023	Section 12(3) general erasure provision.	Implicit / Weak: Conflates absolute data deletion with de-indexing; lacks targeted rules for search intermediaries.	Undefined; leaves broad discretion to the Data Protection Board with no explicit guiding public interest metrics.

The European model offers several valuable design insights for updating Indian data protection law:

- **Targeted De-indexing over Complete Deletion:** Article 17 of the GDPR recognizes that protecting an individual's privacy does not require completely erasing historical articles or court documents from the original publisher's website. Instead, it focuses on decoupling the link from searches for the individual's legal name. This approach protects the person's daily public identity while keeping the source material accessible for historical research or topical searches.
- **Clear Legal Accountability for Search Engines:** The European framework explicitly classifies search engines as data processors and controllers for their search indexes. This classification prevents platforms from escaping privacy responsibilities by claiming they are merely neutral links to outside content.
- **Structured Legal Balancing Tests:** The GDPR provides clear rules for balancing privacy rights against public interests. The right to be forgotten is not absolute; it is automatically limited if retaining the data is necessary for exercising freedom of expression and information, complying with legal obligations, or preserving historical and scientific records. This structured approach prevents public figures or convicted individuals from misusing privacy laws to hide records of public interest.

Ways Ahead: A Comprehensive Policy Blueprint for India

To transform Section 12 of the DPDP Act from a limited data-deletion rule into an effective tool for digital privacy, the Indian legal system needs clear, targeted policy updates. The Central Government and the newly established Data Protection Board of India (DPBI) can use the following four core policy reforms to build a more balanced digital environment:

❖ Introduction of Explicit De-indexing Mandates

The Ministry of Electronics and Information Technology (MeitY), utilizing its formal rule-making authority under Section 40 of the DPDP Act, should introduce specific rules that establish de-indexing as a distinct remedy under Section 12(3). These rules should require major search engines operating within India to establish a simplified, accessible digital portal where citizens can submit link-removal requests. If an individual can demonstrate that a search result for their legal name links to an old controversy, an unverified social media thread, or a minor incident that has been resolved, the search engine should be legally required to remove that specific URL from name-search queries, provided the content does not serve a compelling public interest.

❖ Proactive Data-Deprecation Mandates for Commercial Data Brokers

The Data Protection Board of India (DPBI) should introduce strict data-deprecation and minimization rules tailored for background screening firms and data aggregators. These commercial entities should be legally prohibited from permanently storing unverified social media content, non-conviction arrest records, or private personal data scraped from public forums. The regulations should mandate the use of automated data-cleaning scripts that delete or anonymize non-conviction criminal histories and minor personal disputes after a set period (such as three years). If a background screening firm fails to update its databases and continues to distribute outdated records that lead to automated employment rejection, they should face substantial financial penalties under the Act.

❖ Clear Public Interest Balancing Tests

To prevent the Right to be Forgotten from being misused as a tool for censorship, the DPBI must create clear, objective balancing tests to evaluate removal requests. The right to hide an online record should be denied if: the individual is a public official, political candidate, or prominent public figure whose past actions directly

impact public duties; the digital record concerns a serious criminal conviction, a major financial fraud case, or an active public safety matter; or the personal data is essential for preserving accurate historical archives, scientific research, or official statistical records. By clearly defining these exceptions, the legal system can protect individual privacy without compromising press freedom or the public's right to access important information.

❖ Cross-Border Enforcement Frameworks and International Cooperation

Because many viral hosting websites and data scrapers operate outside India's borders, local enforcement orders can sometimes be difficult to execute. To address this, the DPBI should build partnerships with international data protection authorities and leverage mutual legal assistance treaties (MLATs). India should work to include digital privacy enforcement provisions within its international trade and technology agreements. This would allow the DPBI to cooperate with international regulators to enforce data suppression and link-removal orders against foreign platforms that host non-consensual personal data targeting Indian citizens, ensuring comprehensive privacy protection regardless of where the data is stored.

Conclusion: Restoring Dignity and Rehabilitation to The Digital Age

The rapid growth of the digital economy has outpaced the development of traditional legal protections. While modern recommendation feeds and data collection networks are highly efficient at capturing and monetizing online attention, they lack mechanisms for forgiveness, rehabilitation, or human context. By turning temporary personal mistakes into permanent public records, the contemporary internet operates as a decentralized, uncoordinated panopticon that can lead to ongoing social harassment and structural economic exclusion.

The analysis of Section 12(3) of the DPDP Act, 2023, shows that India's current statutory framework does not fully address these digital realities. By failing to provide clear, actionable de-indexing paths, the law leaves citizens exposed to the long-term harms of online public shaming and automated employment discrimination. This regulatory gap conflicts with the constitutional vision of personal liberty, dignity, and informational self-determination established by the Supreme Court in Justice K.S. Puttaswamy. To address these challenges, the Indian legal system must update its data protection regulations. By implementing clear de-

indexing rules, regulating commercial data brokers, and applying balanced public interest tests, the country can build a data governance framework that respects both freedom of information and personal privacy. This evolution is essential to ensure that technology serves human development, allowing individuals to learn from their past, protect their identity, and build their futures with dignity.

Bibliography

Customs v. Gurnam Singh, W.P. (C) 1234/2020 (Delhi HC) (India).

Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

Draft Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*. Freedom Press.

General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council.

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, [2014] ECR.

HILSR Law Review. (2025). Data Anonymisation, the Right to Explanation, and the Architecture of Accountability Under the Digital Personal Data Protection Act. *Jamia Hamdard*.

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India). Sri Vasunathan v. State of Karnataka, ILR 2017 KAR 424 (India).

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

▪ **Conflict of Interest:** NIL

▪ **Funding Sources:** NIL