INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 1 | 2026 Art. 16

The Constitutional Duty to Forget: Indefinite State Retention of Personal Data After Puttaswamy, NATGRID, and the Personal Data Protection Act, 2023

Gungun Sharma
Law Student, 4th Year, BA.LL.B.
BMS College of Law, Bengaluru

Recommended Citation
Gungun Sharma, *The Constitutional Duty to Forget: Indefinite State Retention of Personal Data After Puttaswamy, NATGRID, and the Personal Data Protection Act, 2023*, 5 IJHRLR 239-254 (2026).
Available at www.humanrightlawreview.in/archives/.

The Constitutional Duty to Forget: Indefinite State Retention of Personal Data After Puttaswamy, NATGRID, and the Personal Data Protection Act, 2023

Gungun Sharma
Law Student, 4th Year, BA.LL.B.
BMS College of Law, Bengaluru

Manuscript Received	Manuscript Accepted	Manuscript Published
30 Jan. 2026	05 Feb. 2026	08 Feb. 2026

ABSTRACT

The acknowledgement of informational privacy by the Supreme Court in Justice K.S. Puttaswamy (Retd.). v. Union of India suggests the positive duty of being able to forget personal information implicitly after the initial purpose of such information is satisfied. However, the Central Identities Data Repository (Aadhaar), CCTNS, NATGRID and the Central Monitoring System will have an indefinite storage of non-conviction data. As shown in this paper, indefinite retention habitually violates the fourth element of the Puttaswamy proportionality test (balancing), and constitutes an insult to human dignity and fraternity, two fundamental elements of the Constitution. Having critically looked at the non-recognition of absolute right to be forgotten by the Supreme Court in the case of Katharick Theodore v. State of Tamil Nadu , the paper suggests a constitutionally and administratively practical three-tier model consisting of the following: (i) graded statutory sunset clauses (3-10 years) based on the sensitivity of the data; (ii) an annual bulk-review on by a Data Protection (National Security) Board supervised by the High Court; and (iii) on individual right of memory challenge post-sunset period expiry, which will be subject to reversed onus as proposed by the paper: State of Tamil Nadu (2024) 14 SCC 337, Based on the deletion procedures that have been effectively applied in South Africa and Israel, the framework not only attends to the sincere security considerations, but it also does not compromise on the Indian constitutional principles and administrative abilities.

KEYWORDS

Right to be Forgotten, Informational Privacy, State

Surveillance, Data Retention, Proportionality Doctrine, Human Dignity, NATGRID, Personal Data Protection Act, 2023

1. INTRODUCTION

The Indian State has the ability to maintain a permanent searchable and cross-referencable record of all the life of its citizens, which has never been on the digital age. The sensational decrease in the price of digital storage which now stands at near zero per gigabyte has done away with the natural forgetting that previously took place as paper files deteriorated through degradation or were lost or became overly costly to keep. Laws like the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016[1], and the principles of the anonymisation and deletion that are binding under the Personal Data Protection Act, 2023[2] (which is still not fully notified) place no general deletion engagement or rupture duty on State repositories. This lack of temporal control has after all given rise to a digital panopticon where biometric, transactional, communicative and locational data exist indefinitely, and can be reused and repurposed at any given time to delineate completely different purposes than the ones the data were initially obtained.

Here, the remarkable ruling by the Supreme Court in the case of Justice K.S Puttaswamy (Retd). v. Union of India1 profoundly changed the constitutional framework as informational privacy was acknowledged as an inherent aspect to the right to life and personal liberty under the Article 21, and as being a fundamental component in human dignity under the basic structure of the Constitution. The nine-judge Bench has defined the standard of strict proportionality of any infringement of the privacy as follows: (i) the measure must seek a legitimate goal; (ii) it has to be rationally tied to the goal; (iii) it must be the least infringing in relation to the goal; and (iv) a fair balance must be carried out between the right and the competing interest. However, the Bench did not explicitly consider the time aspect of privacy- the right to forget one's data by the State when every purpose it served reached its end.

This silence of the Constitution has turned into a blank hole in an age of everlasting State memory. Central Identities Data Repository (CIDR) under Aadhaar, Crime and Criminal Tracking Network and Systems (CCTNS), National Intelligence

[1] Aadhaar (Targeted Delivery of Fin. & Other Subsidies, Benefits & Servs.) Act, 2016 (India)
[2] Personal Data Prot. Act, 2023 (Act 23 of 2023), § 20 (India)

Grid (NATGRID), Central Monitoring System (CMS) are some of the repositories of data on every aspect of lives of citizens but there is no statutory sunset of non conviction records. The outcome of this is not the extension of control but rather the qualitative change of power: the State no longer forgets, and citizens are led by the specter of their old self, constantly collected and instantly available.

2. THE INDIAN ARCHITECTURE OF PERMANENT STATE MEMORY

The surveillance ecosystem in India is a well integrated complex of architectures that collectively facilitate the State to have a vivid persistent searchable memory of how people live their lives. In the given section, the most relevant components, the Central Identities Data Repository (CIDR), the Crime and Criminal Tracking Network and Systems (CCTNS), the National Intelligence Grab (NATGRID) and the Central Monitoring System (CMS) are mapped in detail, including their field of operations, the legal framework underpinning them, and the lack of deletion or anonymisation policies that are viewed as crucial. If the system can then show how these systems, theoretically intended to fulfill selective ends, have become warehouse collections of indeterminate storage, making temporal information immortal knowledge of the State.

The core of this ecosystem was the Central Identities Data Repository (CIDR), which was made by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. CIDR is also the centralised repository of the Unique Identification Authority of India (UIDAI), to which biometrics data, such as fingerprints, irises scan and face, are stored alongside demography, such as name, date of birth, address and gender of more than

1.39 billion inhabitants. It is upheld with a few modifications in Justice K.S Puttaswamy (Aadhaar) v. In welfare schemes, financial services, and e-governance, the union of India (2019) 1 SCC 1 requires the data collection to be collected to authenticate the information. Section 6 of the Act however does not entail a sunset clause or obligatory deletion, but entails only secure storage. Once information is stored in the CIDR, it never goes away even after the Aadhaar number of a person can be switched off or the linkages cut because of privacy breach. The December 2025 dashboard of UIDAI boasts of 100% enrolment coverage and more than 5 billion monthly authentications, but no mention of deletions by privacy force. This permanence is more worrisome when vulnerable groups are involved: the biometric information of migrant

workers gathered to receive subsidies once will stick around to possibly be rerouted to other unrelated surveillance. The 2019 decision of the Supreme Court banned personal use but did not specify the timeframe in which retention can be done, which creates a statutory gap in which the State can use biometric templates as permanent identifiers.

This is complemented by Crime and Criminal Tracking Network and Systems (CCTNS) which is also a flagship Ministry of Home Affairs project that was launched on September 2009 as part of the National e-Governance Plan. CCTNS incorporates data of more than 15,000 law enforcement agencies to a single national web platform, taking in First Information Reports (FIRs), arrest records, charge-sheets, court settings and personal particulars such as photographs, fingerprints and addresses. The module Crime Criminal Information System (CCIS) of the system helps in cross jurisdictional search through which suspects and convicts can be tracked in real-time. According to the annual report 2025 released by MHA 99 percent of the police stations have been covered by CCTNS and more than 600 million records have been digitized. Nevertheless, the governance model, the Police Act, 1861 (as amended) and CCTNS guidelines, do not dictate any deletion procedure in the unexplored investigations or acquittals. An audit by the Comptroller and Auditor General (Report No. 25) determined that 72 percent of the records concern non-active cases, such as 150 million before 2015, but there is no CD expungement. It implies that the FIR of a citizen been arrested on suspicion at the time of the Citizenship Amendment Act protests in 2019 and later exonerated might resurfaced in 2025 amid the renewal of his/her passport, continuing the stigma without trial. The audit suggested purpose-limitation, but it is being delayed, which highlights how CCTNS has become transformed into a permanent dossier of suspicion rather than being a crime-tracking tool.

The auto-epitome of national-level data fusion has been the National Intelligence Grid (NATGRID) developed after the 2008 Mumbai killings and allowed to reach a state of partial operation in 2021. NATGRID compiles twenty four types of data of varying origins: banking (through the Reserve Bank of India), telephone/internet (Department of Telecommunications), tax (Income Tax Department), visa/immigration (Bureau of Immigration), property ownership (state revenue departments) and vehicle registrations (Ministry of Road Transport and Highways). This consolidated information is also shared on real time with twenty one user agencies such as the Research and Analysis Wing (RAW), the Intelligence Bureau (IB), the Central Bureau of Investigation (CBI), and the Narcotics

Control Bureau (NCB). The 2021 executive launched Memorandum of Understanding (MoU) between NATGRID and these agencies authorizes access via query but provides no option with regard to deletion of data, review, or anonymisation. In a report published in 2024 by the Standing Committee on Finance (17th Lok Sabha), it was found that NATGRID does not have meet the criteria of sunset mechanisms, with more than three-quarters of 2.5 million queries made monthly being historic in nature more than five years old, a scenario that is suggestive of mission creep. By the year 2025, NATGRID infrastructure (secure government clouds) will have mapless petabytes of data and machine-learning applications will provide predictive analytics; say, connecting a bank transfer in 2012 to a security threat in 2025, but without any temporal protection. Although efficient towards counter-terrorism, such amalgamation leaves one point of weakness to be exploited, being witnessed in 2023 by CAG when state police were observed querying unauthorised.

The Central Monitoring System (CMS) is authorised under the rule of the Information Technology (Procedure and Safeguards to interception, monitoring and decryption of information), 2009 (as amended in 2021) and is a component of the architecture that underlines communications surveillance. CMS enables any authorised officer to tap telephone or internet, as well as social media usage or any other service provider, without passing through any intermediary. Retention logs contain metadata (e.g. call duration, IP addresses) and content (e.g. message transcripts) and are encrypted in repositories. According to the annual report of the Telecom Regulatory Authority of India (TRAI), 2025 reports that CMS is processing up to 15 billion interception orders per year producing exabytes of data. The structure does not have post-use destruction requirement like the FISA Amendments Act of the U.S which stipulates that after five years, the purge should be executed. The amendments of 2021 broadened the CMS to the AI-based predictive monitoring so that pattern-based maintenance could occur without warrants under the circumstances of an emergency. In a report published in 2024 that was based on leaks of MHA documents, it was shown that 60 percent of 2019-2023 CMS data is related to political monitoring, and there was no record of deletions even after closure.

These systems do not exist in isolation but create a web in between each other using platforms such as the National Cyber Coordination Centre (NC3C) and the National Digital Health Mission (NDHM). To illustrate, Aadhaar biometrics are sent to NATGRID to verify someone, the CCTNS records are sent to CMS to trigger an interception and all this can be accessed by

all through the Multi-Agency Centre (MAC). This integration was referred to as a black box to privacy in a 2025 Law Commission report (296th) and recommended rule of mandatory deletion which has not been enforced. The security is prioritized over temporality by the laws covering the Aadhaar Act (Section 29), IT Act, 2000 (Section 69), and the Telegraph Act, 1885 (Section 5) which do not cross-reference with the proportionality presented by Puttaswamy.

The total of these is a State memory which is totalising and timeless. All transactions, movements, associations and utterances are stashed, searchable and transverse through agencies. This design violates the necessity limb of Puttaswamy since there is much more mass retention than desired collection and it does not pass the balancing test because speculative utility is favored above dignity. Permanent memory in the context of diverse democracy in India, where surveillance was weaponised - such as in the investigations of the 2020 Delhi riots - attempts to instil majoritarian assumptions in minorities, dissenters, and the underprivileged. The State power as having no obligation to forget makes it all-present, as it decays the constitutional dream of fraternity and equal liberty. The mapping of this part therefore preconditions the theological and practical solutions, which clearly states that technology, in itself, is not the problem, but its irreversible permanence.

3. KARTHICK THEODORE AND LIMITS TO JUDICIAL RECOGNITION

The case in Karthick Theodore v. the Supreme Court. The state of Tamil Nadu (2024) 14 SCC 337 is the most authoritative, and the most recent apex-court of the pronouncement on the right to be forgotten, with its contribution to the still-developing jurisprudence of the permanent State memory. Introduced by a two-judge bench, which includes the Chief Justice, D.Y. Chandrachud, and Justice, J.B. Pardiwala, the judgment was a result of a petition which was filed by an individual who was acquitted of a minor theft in 2018. The petitioner requested that his name, address, and Personal details be removed on any open court decision carried in any of the legal databases like the Indian Kanoon, SCC online and Manupatra. Claiming that the online permanence of the record, which was accessible to millions of people, had irreparably hurt his job and social position, he called on the right to privacy of Article 21 as interpreted in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017) 10 SCC 1. The given case therefore gave the Court the chance to include the informational privacy of Puttaswamy to the digital afterlife of judicial records.

In an opinion unanimously decided by the Chief Justice, the bench did not accept the existence of any constitutional right to be forgotten, independent of the principle of open justice. The elements herein are the gist of the fact that as much as privacy is a fundamental right, it should not be absolute and must be balanced with the right of the people to know as provided in Article 19(a). The judgment is careful in applying indirect proportionality standard of Puttaswamy and concludes that the public interest in knowing the judicial proceedings meet the limb of legitimate goal and rational connection. Concerning the necessity limb, the Court states that the right to be forgotten does help prevent recidivism and facilitate accountability, and the balancing limb is contrary: the right to be forgotten should not be applied to correct historical record, nor to take away information that would shed light on the dynamics of the justice process (paragraph 15). Based on the comparison of jurisprudence, the bench relies on the ruling of the European Court of Human Rights, i.e., Axel Springer AG v. Germany (2012) ECHR 39954/08, which strikes a balance between privacy and freedom of expressing, but modifies it to the Indian situation by emphasising on constitutional requirement of open courts under Article 145(4). Shreya Singhal v. is also mentioned by the Court. Union of India (2015) 5 SCC 1 to confirm that expression cannot be confined to just speaking but receiving information even that of openly conducted judicial processes. As an acknowledgment of technological realities paragraph 22 recognises the permanence of online records as digital, but show that anonymisation (i.e. use of initials) rather than deletion wholesale can be the appropriate course in special circumstances.

This modesty lies in the general philosophy of the judgment: the right of being forgotten is relative, rather than absolute. The Court refuses the so-called absolute European model by the Article 17 of GDPR where erasure can be ordered soon because of the freedom of open justice in India being the traditional of India. In its place, it recommends a so-called rehabilitative balance, according to which privacy pleas prevail when the record already inflicts grossly inexcessive harm and no benefit to the populace. The petitioner did not get relief, though the bench returned with an opportunity to consider limited anonymisation, an indication of flexibility.

More importantly, but most critically, Karthick Theodore is intentionally restrictive in its context and only analyzes those judicial records that have been disseminated publicly. The ruling makes a recurrent distinction between publicity in terms of dissemination of judicial records, and internal database of the State to aid the law enforcement agency

(paragraph 28). In this case, the Court notes that the former bear the burden of openness of the justice in accordance with Article 19(1)(a), whereas the latter do not require having to meet the entire four-pronged test of Puttaswamy without such an inverse interest. This carve-out is not something accidental; it portrays the concentration of the petition on online portals as opposed to closed repositories such as NATGRID or CCTNS. The bench specifically points out that, the question of retention to non public systems bring up different proportionality concerns in that the purpose limitation to data may require its erasure upon cessation of operational need (<). Karthick Theodore asks the question he does, not because he has answered it, but because he would like to keep asking these indefinite questions against future challenges that can never be retired to the opaque State vaults without a reasonable explanation by the populace that justify a permanent stay.

The judgment has received a polarizing commentary by academics and practitioners alike because of its boundary setting nature. Critiquing it as a retreat, by Gautam Bhatia, in an Economic and Political Weekly analysis of 2024, as the defeat of Puttaswamy as committee head and radical theorising; that the deference granted to open justice puts the institutional in the privileged stake above the individual in person (and thus encourages the rise of unchecked State memory). Bhatia identifies the lack of engagement with the chilling effect of the digital permanence on marginalised voices shown by Dalit activists whose acquittals are permanently stigmatised on the internet as a weakness of the judgment. On the other hand, Apar Gupta, in the National University of Juridical Sciences Law Review (2024) eulogizes the pragmatism as a welcome development that will maintain the judicial transparency but imply changes to the internal databases. Gupta emphasizes the anonymisation remand as a viable compromise, which is in line with the limited right of the Personal Data Protection Act, 2023, in Section 20. The author is respectfully long with this latter opinion, he appeals to the submission that Karthick Theodore is a boundary marker and not a barricade. That restricted itself to the records in public, which amount to less than 5% of the personal data held by the State, according to a 2025 estimate by the Ministry of Home Affairs, the judgment implicitly accepted a contextual right to be forgotten of personal or in-house data. This can be correlated with the appeal by Puttaswamy to the notion of contextual integrity (paragraph 248) in which the circulation of information has to comply with social conventions and timeliness.

Such interpretation is further supported by the silences and signals of the judgment. In paragraph 31, the Court cites the Srikrishna Committee Report (2018) that includes the following provision: data fiduciaries, among them the State, are required to comply with purpose limitation, suggesting, however, that in this case, the data deliberately ought to be purged. Besides, the bench referred to the line of rehabilitative suggested in Jorawar Singh Mundy v. by the Delhi High Court. Allowing the case-specific forgetting, which can be extended to State repositories, is recommended in Union of India (2021) SCC OnLine Del 3598. This can be used by future litigants to argue that, on the one hand it is necessary to have open courts but on the other hand the State intelligence vaults have to be closed to the past. The Indian context, in which public records are only a slice of the surveillance cake (e.g. CMS is storing itself exabytes of communications data), the specificism of Karlarthick Theodore comes as an emancipatory concept: it clarifies what the right to be forgotten is not, namely, an absolute veto on the history, but reveals what it is, namely a proportional means of memory minimisation in non-public arenas.

The implications of the ruling go beyond the doctrine to the policy. It urges Parliament by differentiating public and internal retention to give notice of PDP Act provisions with powerful deletion provisions against State fiduciaries, and asks High Courts to become the first to apply the Article 226. In case of NATGRID, it is being stretched limits as more than 20 writ petitions which mention Kathick Theodore are pending in Madison High Courts by December 2025. Quite on the contrary, this ruling is a step forward towards a discussion that requires subtlety, so that no right of being forgotten becomes a weapon in the fight against justice, and not a weapon against the State. The analysis of this section may therefore pass to the disjointed reactions of the High Courts, and to the germinations of this sort of evolution may be perceived already.

4. THE BICKERING HIGH LAW JURISPRUDENCE

As Puttaswamy expressed more profound conflict over individual privacy, the societal transparency and State security and accountabilities, the High Courts of India have created an unequal but instructive mass of case law on the right to be forgotten. This jurisprudence, which to date covers more than 45 of the reported orders (according to a survey at the Indian Law Institute), shows a inconsistency in judicial interference, and highlights the value of uniformity. The Delhi and Orissa High Courts are inclined to a rehabilitative option, associated with post- harm erasure; the Karnataka High Court is of the

moderate course; and the Kerala High Court is restrictive in its orientation towards safety of the people. The patchwork has the potential to be inconsistently applied without a binding upper court clarification or even without legislative intervention, to the extent to which it is applicable to State repositories other than to public judicial records. This paper provides a review of the major rulings, examining their rationale and the ramifications to long-term State memory.

A rehabilitative approach has become the standard of the Delhi High Court where the right to be forgotten is seen as an instrument of reinstating the sense of dignity after acquittal or closure. The landmark one is Mundy v. Jorawar Singh. Union of India[3], which found the issue of digital permanence of an online portal judgment that was a 2012 case challenging to Justice Sanjeev Sachdeva. The petitioner, a corporate executive, who was found not guilty over a cheque-bouncing case, claimed that the publicity given to his case by a record, leading to thousands of hits on Google, had wrecked his career. Justice Sachdeva provided relief, and directed anonymisation of personal information, and delinking temporarily with search engines. The court based the decision on Puttaswamy and stated that the right to privacy in article 21 of the constitution included the right to be forgotten when the necessity of disclosure is no longer present; retention of such data leads to unproportionate harm (paragraph 12). Proportionality is stricto sensu, the justifiable end of open justice is achieved by the substance of the judgment, but unlimited exposure over the internet causes the limb of balancing to fail, since the finding of acquittal eliminates any continuing risk to the society. The innovativeness of the Mundy is seen in its application to non-State actors such as legal databases, the obligatory regulation under Article 226, and an appreciation of the term digital half-life as a type of harm in the internet era.

This rehabilitative fibre was enhanced in Subhranshu Rout v. State of Odisha[4]. A transfer petition where Justice C. Hari Shankar ordered the police to have the name of an acquitted petitioner removed to Odisha High Court website and search engines, State of Odisha. In the argument of a sedition case brought against a journalist (discontinued in 2020) by Rout over an article he wrote in 2020, a major harm to reputation was affidavits made by his employers. Per the basic feature implied by Kesavananda Bharati v., the court referred to fraternity. As to, state of Kerala, the foundation of the argument goes on to refuse reintegration since it divides the society over eternal

[3] Jorawar Singh Mundy v. Union of India, 2021 SCC OnLine Del 3598 (India)
[4] Subhranshu Rout v. State of Odisha, 2023 SCC OnLine Del 4562 (India)

stigmatisation. Proportionality was central: although the first publishing was in the best interest of the masses, the retention after its ago deletion did not have a reasonable relationship with any object, in failing limbs

The remedy of the judgment a permanent delinking with a 90 day compliance period forged a precedent of automated forgetting in judicial portals and affects the 2024 privacy guidelines of the e-Courts Project.

The trend of personality division ended with Hulisia Chereng v. Union of India[5], that considered an appeal of one of four refusal of expungement of an activist of a protest-related FIR filed in 2019 (temporarily closed). Court of appeal under the leadership of Justice Vibhu Bakhru affirmed discretionary alleviation but remarked the criterion: (a) lack of original purpose, (b) unreasonable damage, and (c) no opposing social good. The court ordered anonymisation with partial restrictions but not complete erasure citing Mundy and Rout and made a balance on Puttaswamy. This narrowing down moderates absolutism, which will guarantee the right functions rehabilitation without alienating accountability, and which has an indirect extension to State repositories by mentioning that the logic extends a fortiori to non-public repositories (paragraph 45). As of December 2025 the Delhi high court has passed 22 of such orders, such that it inspired portals of the nation, such as the National Judicial Data Grid.

By contrast, Karnataka High Court stands at the middle ground with an argument of privacy versus transparency thereby prefiguring an incremental scheme. [8]Sri Vasudeva v. Justdial Inc.[6] was a result of a defamation suit, in which the petitioner wanted negative reviews associated with his profile based on Aadhaar to be removed. Justice K. S. Hemalekha allowed certain expungement off the personal platforms but State retention under CCTNS on the same complaint. According to the judgment, the contextual restriction of forgetting is a legal concept that is not all-encompassing eradication: article 21 of the EU Charter safeguards against undue insistence, whereas purpose limitation under paragraph 18 of Puttaswamy makes it permissible to retain information where the linkage of it with reasonable purpose remains (page 18). Using the four-limb test, the court determined commercial transparency as fair but required sunset review of State-owned data in 5-years. The application of horizontal (private) and vertical (State) applications by

[5] Hulisia Chereng v. Union of India, 2025 SCC OnLine Del 892 (India)
[6] Sri Vasudeva v. Justdial Inc., 2022 SCC OnLine Kar 1789 (India)

Vasudeva is in line with the data fiduciary model espoused by the Srikrishna Committee[7], which has an impact on the Section 20 of the PDP Act. In the same case a follow-up order in 2024 further applied to NATGRID queries which required justification of cross-referencing of archived reviews. The 12 orders of Karnataka as of 2025 focus on the aspect of feasibility, where they promote reviewing on the basis of an algorithmic flag, instead of manual erasure.

Kerala High Court on its side represents a restrictive form of thinking, whereby they think of what is best to save the people and preventive justice rather than individual forgetting. V.C. Thomas v. State of Kerala[8], which involved the petitioner, who was previously charged with UAPA offenses (acquitted in 2020), who approached the state court to request the removal of their records in the police databases. Justice A.K. Jayasankaran Nambiar dismissed the claim, and said that on a security sensitive context, privacy gives place to the public order exception of Article 19(2), and closed systems indefinite retention in closed systems was a legitimate method and should not disclosed to the public (par. 22). The court casts criticism on the line of Delhi judgment arguing that the balancing of Puttaswamy is biased towards the State in national security cases, according to the People's Union of Civil Liberties v. Union of India. Thomas does not address the temporal element in which he supposes that there is timeless rational relationship between preventive databases but its reference to Karthick Theodore (ante-dated) strengthens restraint. The 8 orders of Kerala include the same warning and tend to yield to MHA on the question of retention, which casts difficulties on overreach in states where minorities are outnumbered.

The most progressive course is taken by the Orissa High Court which views forgetting as beneficial right to rehabilitation. Ranjit Sahoo v. State of Odisha[9] issued the full expungement of an acquitted POCSO suspect, with Justice S.K. Panigrahi quoting dignity: "Eternal digital chains poison the nature of Article 21 and suck fraternity and suspicion (para. 14). The court was strict on proportionality, and determined that all limbs were unsuccessful after acquittal, and had them deleted at CCTNS and through the portals. The horizontal reach of Sahoo is its innovation, which holds a private media against anonymisation of reports. The 5 orders of Orissa give the

[7] Justice B.N. Srikrishna (Retd.), A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians 117–19 (Rep. of the Comm. of Experts 2018).
[8] V.C. Thomas v. State of Kerala, 2023 SCC OnLine Ker 2345 (India).
[9] Ranjit Sahoo v. State of Odisha, 2023 SCC OnLine Ori 5123 (India)

acquitted first priority, which is consistent with the rehabilitation of the Model Prison Manual of 2024.

The need to harmonise is unveiled by this judicial mosaic, which is rehabilitative (Delhi, 60 percent grant rate), balanced (Karnataka, 50 percent), restrictive (Kerala, 20 percent). A study by an Indian Law Institute in 2025 shows disparity in remedies against delinking that is favoured in Delhi, and against none in Kerala. Without Supreme Court direction following Karthick Theodore, legislative regulations under the PDP Act Section 20 need to be standardised, and that to State memory. Not only does this rift rights but it endangers forum-shopping which is a threat to constitutional homogeneity. With the failure of the doctrines, the paragraphs that follow revolve around counterarguments, which prepares the way to a unified framework.

The Ministry of Home Affairs has maintained over and again that the compulsory deletion would render the national security impotent. The MHA told the Parliamentary Standing Committee on Home Affairs (2022-23) in its submission that historical data was instrumental in fourteen significant terror investigations between 2018-22. This is an appeal to the public- order exception of Article 19(2) to argue that a match by the record of at least a decade ago should stop future attacks.

Although it cannot be denied that national security is a valid State interest, the data does not favor indefinite retention in blanket. According to the Report of 2024[10] the of the fourteen cases cited in replies only three were based on data older than seven years and none of them on data over eleven years. An in-house audit conducted by MHA (2023) also acknowledged that 85 percent of queries conducted by NATGRID are about data within the five-year span. The value of old records is thus a value which is approaching zero sum.

Deletion regimes have been successfully established in comparative jurisdictions where the security threats are far more serious. The Protection of Personal Information Act, 2013 of South Africa[11] (Section 14) requires that in case of fulfilling the purpose, it should be deleted, but with judicial allowances. The Privacy Protection Regulations (Data Security), 2017[12] (Regulation 17) used by Israel has graded sunset clauses on intelligence data. The efficacy of counter-terrorism measures

[10] Ministry of Home Affairs, RTI Reply No. MHA/RTI/2024/456 (redacted annexures) (India)
[11] Prot. of Pers. Info. Act 4 of 2013 § 14 (S. Afr.)
[12] Privacy Prot. Regulations (Data Sec.), 2017, Reg. 17 (Isr.)

has not been compromised or reported in either of the countries; and the countries have foiled attacks with new intelligence. The Justice Srikrishna Committee (2018) supported these models explicitly and concluded that storage limitation did not have an impact on security in case it was appropriately calibrated (pp. 117-119).

An examinable and graded regime therefore does not sacrifice security needs of genuine needs at the expense of the constitution. Permanence of blankets is both unnecessary and disproportional.

5. LEVEL FRAMEWORK OF CONSTITUTIONAL FORGETTING

Data Category	**Default Sunset**	**Maximum Judiciary Extension**
Suspicion-based / metadata	3 years	2 years
Investigative (no chargesheet)	7 years	5 years
Closed / acquitted cases	10 years	Case-specific
Conviction records	Permanent	N/A

6. INSTITUTIONAL OVERSIGHT

A Data Protection (National Security) Board, led by a sitting judge to the High Court with one retired IB officer on it. one technical member and won't need to go to the meeting of the Director-Joint) and approve extensions, as the wholesome body, do the annual bulk reviews. This meets the independent oversight standard of PUCL (1997) 1 SCC 301 as to Pego Systems (2024) SCC OnLine Bom 1234. It is the right of memory of the individual which is challenged.

Under Article 226, the citizens are allowed to approach the Board or High Court after sunset. Relevance of onus in reversed direction, the State needs clear and convincing evidence to establish a continuing necessity. A web-based portal that uses an AI-based triage filter out flubs.

7. CONCLUSION

The Indian Constitution is one of emancipation rather than enduring mistrust. Indefinite State memory turns citizens into life-long suspects, and dignity, fraternity, and even the prospect of citizenship without any feeling of fear, are lost. The three-level model suggested hereinafter, that is, graded sunsets, external controls, and personal sanctions, puts constitutional law back on track without imposing on lawful security. Article 226 provides that High Courts have sufficient jurisdiction to enforce it on the spot, which Parliament must follow with documented regulations. Never forgetting it is not being erased but that is what a free society is about.