THE EVOLUTION OF RIGHT TO BE FORGOTTEN AND CHALLENGES IN THE ERA OF ARTIFICIAL INTELLIGENCE

Shankar Dayal[1] & Suvrat Khare[2]

ABSTRACT

Leak and breach of personal data is never ending. Every day we hear or read instances of breach of personal data. Every day leaking of data breaches Right of Privacy. The seriousness of personal data breach has captured public attention. What should be the attitude towards these breaches and leaks? What are the consequences of such breach of data? What are the measures to be taken to erase such data? What should be the extent of culpability for these breaches? What are the laws relating to data breach working in India as well as at global stage? What approach should be taken by executive to deal and erase such breach, meaning thereby how reformative they are? Whether there are laws which can deal to erase data from Artificial intelligence which works on LLM model and data retention that allows it to store data in bits and pieces in itself meaning thereby it does not need original platform once AI has read data from it. This paper focuses on Right to be forgotten aligned with AI. It examines the difficulties of execution of Right to be forgotten any why it has become an imaginary right. This paper deals with evolution of the right to be forgotten. It deals why DPDP Act does not succeed to address Right to be Forgotten in era of AI.

Keywords: Right to be Forgotten, Right to Privacy, AI, LLM model, Imaginary right, Eraser, Digital Personal Data Protection Act, 2023.

[1] Student, LL.M. Central University of South Bihar, Gaya
[2] Practicing advocate at High Court of Judicature at Allahabad

1. Introduction

In the modern era Right to privacy includes Right To Be Forgotten. It is a fundamental right which allows people to erase their presence from any platform, search engines, and databases. It is seen as a reaction to the presence of digital records of data amounting violation of Right to Privacy. It grew as a doctrine in American law which later codified as a fundamental right in European Union Legislation, and now in Indian law also through DPDP[3]. Earlier Right to be forgotten was seen as an exception to Right to Privacy and Freedom of Speech and Expression but now it is seen as an extension of these two rights. In the era of Artificial Intelligence this right seems to be an imaginary right as AI works on LLM model and data retention that allows it to retain to store data in itself. In the contemporary AI, it is the huge, continuous databases that render the actual forgetting legally and technically difficult[4].

The problem with Right to be Forgotten and its non-application to AI is due to inaccurate understanding of privacy in relation to AI. While understanding Right to be Forgotten in relation to AI we first have to dive into the concepts of human and AI memory and its forgetting. DPDP Act treats human and AI memory alike supporting a fictitious understanding of memory and forgetting but that does not relate with reality.

2. The Evolution of Right to be forgotten.

The development of right to privacy is not just a legal development but a reflection of growing respect for human dignity and autonomy with the changing of time where the world is living in two dimension physical and digital. The right comes with the control on information as a fundamental right and has given a new dimension of it as right to be forgotten**.** This facet of right to privacy has developed gradually.

2.1 Sidis v. F-R Publishing Co. (1931)

The intellectual origin of the right to be forgotten, though it was not expressly recognised as a right, is in the American common law jurisprudence on privacy in the early twentieth century. In Sidis[5] case in 1931, the United States Court of Appeals for the Second Circuit deciding a

[3] Digital Personal Data Protection Act, 2023, No. 22, Act of Parliament, 2023 (India).
[4] Olivia Rempe, *The Right to Be Forgotten- But Can AI Forget?* (April, 2025) https://cloudsecurityalliance.org/blog/2025/04/11/the-right-to-be-forgotten-but-can-ai-forget
[5] Sidis v. FR Pub. Corporation, 113 F., 2d 806 (2d Cir. 1940).

case filed by William James Sidis, a former mathematical prodigy, who had received national recognition in his youth and adolescence in 1931. Although the court had ruled against Sidis, noting that legitimate interest of the people in his location and the state of affairs overrides his and others privacy interests, the decision took into consideration the conflict between the inherent wish of an individual to have forgotten his or her past and the interests of the media and people in information.

The significance of right to be forgotten doesn't lies in what was held in the sidis case but a principal of recognition that even if someone is public figure they still have right to privacy. the court recognised that if someone is being famous that doesn't mean he loses all privacy. Continuously revisiting and endlessly sharing information about someone can cause harm to the individual's autonomy.

2.2 Directive 95/46/EC, (1995), The European Data Protection Framework.

The paradigm shift in the law of data-protection came in 1995, when the Council of the European Union Directive 95/46/EC[6] on the Protection of the Individuals with regard to the Processing of the Personal Data was adopted and which remained the most significant data-protection law in the European countries until the adoption of the General Data Protection Regulation in 2016.

The directive developed various principles that formed the conceptual base on the subsequent development of the right to be forgotten.

I. First, the directive acknowledged that individuals had inherent rights to information relating to them such as the right to access, rectification, and objection. Such rights were referred by European scholars as ARCO rights; Access, Rectification, Correction and Opposition.

II. Secondly, the directive made it clear that processing of individual's data should be according to the law, and should be consent based.

III. Third, the directive identified the concept of data minimization, which is that an organisation only obtains that personal data that is required to achieve the given purpose

[6] Directive 95/46/EC, 1995 O.J. (L 281) 31.

of the processing.

Although right to be forgotten was not explicitly mentioned in the directive but the core idea behind it started resonating in it and have started to give control to individuals over the personal data and control over information that how it should be used. so even the phrase "right to be forgotten" didn't appear in the text but it laid down the doctrinal foundation for it. It planted the seed and which later turned into enforceable right as the right to be forgotten in GDPR.

2.3 Google Spain SL and Google Inc v Agencia Espanuela de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez (2014).

The case of Google Spain SL and Google Inc v Agencia Espanuela de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez[7], decided by the Court of Justice of the European Union in May 2014, brought the right to be forgotten to a point where it is a separate, enforceable legal right under EU. The case was initiated by an application of a Spanish citizen by name Mario Costeja Gonzalez Spanish citizen Mario Costeja González requested the removal of old news links about his settled debts, as Google search results still displayed them, which was unfairly affecting his reputation and career.

The case of Google Spain judgment had enormous weight on several grounds.

I. Firstly, it provided that right to privacy and data protection was not just enforceable against state actors but against private corporations as well.

II. Secondly, it acknowledged that the perpetuity of digital information posed unique harms and that could not be countered with the same legal measures as it would have been done prior the digital era.

III. Thirdly, it indicated that the right to be forgotten was not a shield against state, but requires an affirmative step by the data controllers to erase and delink the data.

IV. Fourthly, the ruling upheld the value of the personal dignity and individual autonomy that could override the economic interests of the technology firms and under certain

[7] Google Spain SL v. Agencia Española de Protección de Datos, European Ct. Reports 3193 (CJEU 2014).

circumstances, it overrode the general interest of the people in the overall access to the archived information.

2.4 General Data Protection Regulation 2016.

The conceptual and practical justification of the right to be forgotten is legislatively embodied in the General Data Protection Regulation (GDPR)[8] adopted in 2016 by the European Union which coming into effect on May 25, 2018. The right to erasure was codified in article 17[9], therefore, turning into an express statutory right in European.

The Article 17 of the GDPR gives the individuals the right to request the data controller to erase their personal data without any undue delay in certain conditions. These situations are -:

I. Where the personal data of individual is no longer required, in relation to the purpose for which it was initially gathered or processed.

II. Where the individual to whom the data concerns withdraw his/her consent

III. Where the personal data has been processed unlawfully

IV. Where the personal data must be removed to meet legal obligations imposed by the law

V. Where the personal data has been processed against the consent of the individual to whom it relates

VI. Where the processing has no other justifiable reason.

2.5 The Puttaswamy Judgment and the Acceptance of the Essentiality of Privacy in India (2017).

Puttaswamy[10] is a landmark ruling by a nine-judges constitutional bench, voted in support of the view that privacy is a fundamental right of the right to life and personal liberty in Article 21. More importantly, the court did not view privacy as a rigid viewpoint rather it viewed it as a multidimensional right which included personal autonomy, bodily integrity and informational

[8] GDPR, 2016 O.J. (L 119) 1.
[9] GDPR, Regulation (EU) 2016/679, art. 17, 2016 O.J. (L 119) 1.
[10] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

privacy. Informational privacy was originated as an individual right to regulate the gathering, sharing and utilization of personal data concerning the individual including medical records, financial data, academic data and on-line information.

The judgement of Puttaswamy in course of the right to be forgotten in India cannot be overestimated. The judgement established a constitutional basis on data protection legislation that was not in existence before. It determined that the state collection, storage and use of personal data regardless of whether this is biometric like Aadhaar, surveillance or any technological process must be according to the constitutional standards of legality, legitimacy and proportionality. Thus, the ruling addressed the formulation of detailed data protection law, something that had been long overdue but never implemented before.

2.6 Digital Personal Data Protection Act, 2023.

The passage of the Digital Personal Data Protection Act, 2023[11] (DPDPA) is the peak of the journey of the Indian nation to the wholesome data protection law in the present day. In spirit with the constitutional requirement set by Puttaswamy, the government finalised of the DPDPA in August 2023. The enforcement of this act will be done in 3 phases phase 1 will come into effect on 14 November 2025 with Phase 2 rolled out on 14 November 2026. The full substantive provisions such as the critical parts such as the consent mechanisms and erasure rights will take effect by 14 May 2027 that is 18 months after the notification.[12]

The DPDPA tackles the challenge of right to erasure by the use of Section 8[13] that gives the individuals, a right to request the deletion of their personal data in certain conditions. However, the provision of the DPDPA dealing with data erasure is significantly less detailed and explicit in comparison with the one of Article 17 of the GDPR[14]. The Act provides individuals with the right to give consent to data processing, and requires data fiduciaries to both stop processing personal data and to destroy personal data after that consent has been revoked, unless it is required by the law to retain the data or there is need to perform legitimate functions.

DPDP Act does not cover the major components of the Right to Be Forgotten: de-referencing

[11] Digital Personal Data Protection Act, 2023, No. 22, Act of Parliament, 2023 (India).
[12] Digital Personal Data Protection Act Notification, G.S.R. 843(E), No. 757, Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025),
[13] Digital Personal Data Protection Act, 2023, § 8, No. 22, Act of Parliament, 2023 (India).
[14] GDPR, *supra* note at 9.

requirements of search engines, criteria of relevance and necessity of data, mass processing of algorithms, and the issue of AI's perpetrated data permanence.

3. The Right to Be Forgotten in the Era of Artificial Intelligence

The right to be forgotten, now faces an emerging challenge in the era of artificial intelligence. The critical analysis of the technical and architectural irreconcilabilities between the neural network-based AI systems and the right to be forgotten has shown that current world paradigms of machine learning seem to be in conflict with the idea of permanent data deletion and that legal and technological solutions will be needed to effect a reconciliation or whether societies will be required to think fundamentally differently about privacy rights in the era of artificial intelligence.

3.1 The Instant Technical Incompatibility of Neural Networks and Deletion.

The fundamental technical issue behind the incompatibility between AI systems and the right to be forgotten lies in the architectural built of contemporary machine learning. In contrast to classical databases, where data is stored in discrete and identifiable records, which can be found, retrieved, and deleted, neural networks spread the information among billions of parameters (weights and biases) that are not easy to be analysed.[15]. Once a personal information of a particular person is integrated into this model during the training process, such information spreads in the parameter space pattern that is essentially opaque and cannot be reverse-engineered in the present world of technology.

Even if it is theoretically possible to determine the parameter and remove the data from the neural network, the expense of doing it is so high that it is practically unaffordable. The simplest idea of complete deletion is explicit unlearning (also called retraining-and-forget), which consists of just deleting the data point that the user is trying to delete in the training data and re-training the entire model as though this data did not exist originally. It is a method that will ensure no residual effect of the deleted data[16]. But the cost of computation is appalling.

The estimation of this can be taken reference from this that, GPT-4 took one month (34 days)

[15] Rickard Brannvall, Laurynas Adomaitis, Olof Gornerupand Anass Sedrati et al., *Technical Report for the Forgotten-by-Design Project: Targeted Obfuscation for Machine Learning* (Dec. 2024), https://arxiv.org/abs/2501.11525.

[16] Alex Oesterling, Jiaqi Ma, Flavio P. Calmon, Himabindu Lakkaraju *Fair Machine Unlearning: Data Removal while Mitigating Disparities*, at AISTATS 2024 (PMLR Vol. 238), https://arxiv.org/abs/2307.14754**.**

of active calculations on 1024 supercomputers (CPUs and GPUs combined) to be taught (1024 servers). This used up approximately 50 gigawatt-hours (GWh) of electricity,[17] which is equivalent to electricity supply of 2 million houses for a day in India. In case all users of ChatGPT ask to delete their personal information were accepted that request during retraining, the cost in terms of energy used would be neither economically viable nor environmental.

3.2 The Impossibility of Organizing Significant Audits.

Conventional privacy auditing system of data is based on the examination of data systems by determining the location of personal data storage, the nature of data exchange within systems, as well as the confirmation that the deletion processes have been carried out. The method is successful with classic databases but there is severe challenge with it in neural networks.

An auditor who wants to check whether a company is within the requirements of RTBF with respect to GPT-4 or any other similar AI has an insurmountable task: the parameters of the model are in 1.7 trillion (that is impossible to check without cracking the black box problem), and even the interpretation of these values is impractical. With distributed representations, the regulator has no way of following particular training data through the model as (distributed representations are impossible to do so). The regulator also does not have the autonomy of checking whether deletion was effective (membership inference attack techniques are inaccurate and contentious). The regulator has not in place the mandate that compels the company to undertake overall retraining due to the prohibitively high cost.[18]

4. Three Awkward Futures in the new era.

With this profound incompatibility and challenges in the architectural built of system in new era of artificial intelligence which is quite different from the classical data system, societies are presented with three major ways:

4.1 Regulation Wins- Legal Innovation and Enforcement.

Regulators in this case react to the technical impossibility of RTBF by empowering legal systems and enforcement strategies. Instead of living with existing technical shortcomings

[17] Manab, Meem Arafat, *Eternal Sunshine of the Mechanical Mind: The Irreconcilability of Machine Learning and the Right to be Forgotten*, arXiv:2403.05592 (Mar. 2024), https://arxiv.org/abs/2403.05592**.**
[18] Marino, Bill et al., *Bridge the Gaps between Machine Unlearning and AI Regulation*, arXiv:2502.12430 (Feb. 2025), https://arxiv.org/abs/2502.12430.

regulators may adopt these strategies:

I. **Strict input requirements:** Do not train large-scale AI models on personal data without explicit and granular supplement to that data point.

II. **Ban some uses**: While we work on the privacy of personal data, make it illegal to train some of the most dangerous uses of AI on its data (facial recognition, behavioural prediction, etc.).

III. **Mandate architectural designs:** Design AI systems with deletion consideration, by employing privacy-friendly architectures, with some loss of performance to ensure deletion can always be guaranteed.

IV. **Establish deletion insurance:** Hold companies to insure on their capability to comply with deletion requests establishing market incentives on deletion capacity.

3.2 Technology Wins- Breakthrough Solutions.

In this case, researchers make breakthroughs in the fields of machine unlearning, certified deletion, and privacy-preserving AI architecture. This could involve:

I. **Certified deletion at scale:** algorithms that offer mathematical assurances that all data has been removed, even in large models.

II. **Privacy-preserving training:** AI architectures that can match the current system in performance and have deletion features built-in.

III. **Decentralized AI models**: Abandoning the mega-models in favour of distributed, specialized models with technical easy deletion.

IV. **Quantum computing methods**: Providing quantum computing as an alternative way of performing deletion operations possible only on classical computers.

4.3 Pragmatic Compromise: Remaking Rights and Coming to Terms with Constraints.

In the said case, societies also practice pragmatically that they cannot have perfect deletion and

redefine privacy rights:

I. **Lapse of time:** The data should be removed after customized durations (e.g., 5 years) and not on-demand.

II. **Anonymization instead of deletion:** Attention moves away to deletion to anonymization and residual statistical dangers are tolerated.

III. **Tiered privacy**: There are various rules of various data and AI applications, and some applications require weaker promises of deletion.

IV. **Transparency-based accountability**: You can have transparency-based accountability instead of deletion by introducing information to users on what data was used and how, and leaving informed decisions on whether to participate.

V. **Litigation-based compensation**: Compensation should not be based on deletion and instead allow users to prosecute companies due to secondary personnel data retention.

5. Conclusion

The Right to Be Forgotten is actually a good intention regulatory protection and some people will claim that the Right to be forgotten is a valuable right that should be protected. But here there is a very obvious derailment between law and technical reality. As the case with Privacy by Design implementation as observed by privacy researchers, it is hard to enforce and push legal mandates in data-processing systems in two different languages, resulting in the problematic miscommunication with disastrous effects. There is a need to bridge such a gap in languages and conceptualizations of terms such as memory and forgetting.

As Vint Cerf, an internet pioneer, put it: "You can't go out and remove content from everybody's computer just because you want the world to forget about something. [That's not] a practical proposition at all."[19] The ability of AI not to "forget" is true in the sense of large databases where it uses its retention memory even though the original database is deleted. As

[19] Warman, M. (2012) *Vint Cerf attacks European internet policy.* (Apr. 1, 2012) www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-atacks-European-internet-policy.html

stated, it may be impossible for AI to forget. The clash of RTBF with modern AI has shown a complete technical incompatibility: the neural network systems, which use neural networks to support the most powerful AI systems today, are simply incapable of supporting meaningful and verifiable full-scale data deletion. The fact that data is distributed among billions of parameters makes it opaque so that it is impossible to delete it, verify, or audit.

The Right to be Forgotten, today seen as right to be forgotten by humans by courts. This does not apply on technologies like AI. If we have to see true spirit of Right to be Forgotten than we have to see it from the eye of different fields like neuroscience, cognitive science, anthropology, psychology, and sociology.

India, when formulating its Digital Personal Data Protection Act, should also have to deal with this same incompatibility. Section 12 of the DPDP Act regarding the right to correction and erasure (along with the associated provisions) is inherently subject to the technical infeasibility of GDPR as a technicality of similar kind. When Data Protection Board in India starts its work, it will encounter a lack of control as the two available options are to accept that deletion cannot be complete or ban AI-based applications that fail to accomplish it. Any actions taken by India will have far-reaching consequences across the world, as other developing democracies will look upon it as an example of whether the right to be forgotten will continue to exist in the era of artificial intelligence or will it become irrelevant and a distant dream as a far-fetched right to be forgotten in the world where machines hold the record of what humanity should forget.