

THE PARADOX OF ERASURE: RECONCILING THE RIGHT TO BE FORGOTTEN WITH TECHNOLOGICAL REALITIES IN NIGERIA

Olaluwoye Oyinkansola Oluwatosin*

Abstract

The rapid expansion of digital technologies has intensified concerns surrounding personal data protection, particularly in relation to the right to erasure or the right to be forgotten. While the right to erasure seeks to empower individuals to control their digital footprint, the persistence of data within distributed systems, cloud storage, and artificial intelligence, raises critical questions about the feasibility of achieving complete erasure. This study examines the paradox between the legal promise of erasure and the enduring nature of digital data within Nigeria's evolving data protection framework. This study adopts a doctrinal research design, relying on statutory analysis of relevant statutes. The study found that while Nigeria's legal framework formally recognises the right to erasure, significant gaps persist in its practical enforcement due to technological constraints, weak regulatory capacity, among others. A shift is recommended from an absolutist conception of erasure and explore a more pragmatic approach such as anonymisation where complete erasure is not feasible, stronger regulatory oversight, and clearer compliance obligations for data controllers.

PhD Candidate, Lecturer, Department of Private and Business Law, Ajayi Crowther University, Oyo, Oyo State, Nigeria. Email: olaluwoyeoyinkan@gmail.com, (Address: 1, Azeez Aina Layout, Olusanya, Ring Road, Ibadan, Oyo State.

Keywords: Artificial Intelligence, Data Subject Right, Digital Privacy, Right to Erasure

1. INTRODUCTION

In today's digital age, constant data sharing is the price of participation, but privacy remains the expectation. Individuals continuously disclose personal data in exchange for access and convenience, yet simultaneously assert an enduring expectation of privacy.¹ The right to be forgotten, also known as the "right to erasure" thus captures a core tension in modern data protection law in Nigeria. This right confers individuals with the right to request internet platforms to delete or remove their information from the public domain. However, it creates a significant legal challenge where the statutory right to be forgotten conflicts with the immutable and pervasive nature of modern technologies like blockchain and artificial intelligence. There is thus a contradiction between the legal expectation of deletion and the practical difficulty of fully removing data in digital systems that have been designed to store, replicate and analyse information persistently. Even when data is deleted it may persist in backups, caches, or be reflected in machine learning models and indexes.

It is widely acknowledged that, although human beings naturally tend to forgive and forget with the passage of time, the internet possesses an enduring capacity to store, retrieve, and preserve information indefinitely. This persistence is reflected in the continuous availability of online content such as videos, photographs, documents, and audio recordings, which collectively create a lasting digital footprint of individuals' lives. The rapid advancement of technology in recent decades has revolutionized the way we live, communicate and interact with the world.

¹ A relevant quote states: '*Nothing fixes a thing so intensely in the memory as the wish to forget it*' - Michel de Montaigne

From the internet and social media to artificial intelligence and big data, technology has become an integral part of our daily lives and shaping various aspects of society and raising important questions about human rights in the digital age.² As human lives become increasingly interconnected through digital platforms and our personal information is stored and shared in unprecedented ways, the protection of data and digital rights has emerged as a critical concern. The rise of digital economy, artificial intelligence, cloud computing, and data-driven innovation has made it increasingly necessary to safeguard the rights of individuals whose data is being collected and used.³

The right to be forgotten enables individuals to request the deletion or removal of personal data that is no longer necessary, unlawfully processed, or otherwise prejudicial to their interests. In Nigeria, this right has been formally codified under section 34 of the Nigerian Data Protection Act 2023 (NDPA)⁴ marking a significant milestone in the country's data protection trajectory. The provision reflects a growing recognition of the need to empower data subjects with greater control over their personal information, particularly in an era where digital records can shape reputational, economic, and social outcomes indefinitely. It also signals Nigeria's attempt to align with global data protection standards, most notably the European Union's General Data Protection Regulation (GDPR), which enshrines a similar right under Article 17.

² Vlon Pollozhani Shehu & Visar Shehu 'Human rights in the technology era-Protection of data rights' (2023) <https://www.researchgate.net/publication/371848592_Human_rights_in_the_technology_era_Protection_of_data_rights> accessed 3rd March 2026

³ Goodman Bryce, Flaxman Seth 'European Union regulations on algorithmic decision-making and a "right to explanation" 2017 <<https://onlinelibrary.wiley.com/doi/epdf/10.1609/aimag.v38i3.2741>> accessed 3rd March 2026

⁴ Section 34 (1) d Nigerian Data Protection Act, 2023

However, despite its normative appeal, the right to be forgotten presents profound conceptual and practical challenges, especially when juxtaposed with the realities of modern data ecosystems. The notion of “erasure” presupposes that personal data can be completely and permanently removed from digital systems upon request. Yet, in practice, data is rarely confined to a single, controllable location. Instead, it is often replicated across multiple servers, stored in cloud infrastructures, embedded in algorithmic models, and transferred across jurisdictions with varying regulatory standards. Against this backdrop, this paper seeks to examine the viability of the right to be forgotten within Nigeria’s data protection regime. It interrogates the extent to which the legal promise of erasure can be reconciled with the technological realities that define contemporary data processing practices.

2. CONCEPTUAL FRAMEWORK

2.1 Data Subject

The right to the privacy of personal information is firmly enshrined in the Constitution of the Federal Republic of Nigeria 1999 (as amended), which constitutes the ground norm. Within this constitutional framework, the beneficiaries of these rights are broadly characterised as “citizens.” However, with the evolution of Nigeria’s data protection regime, a more precise and technologically attuned terminology emerged. Specifically, the Nigeria Data Protection Regulation 2019 and the Nigerian Data Protection Act 2023 adopt the term “data subjects” to denote individuals whose personal data is subject to processing and, consequently, entitled to protection. This shift in nomenclature reflects a transition from a purely constitutional conception of privacy to one that is more aligned with contemporary digital realities.

A data subject means an identified or identifiable living individual to whom personal data relates and applies.⁵ This is a natural person who can be identified, directly or indirectly by reference to a name, an identification number, location data, one or more factors to the physical, physiological, genetic, mental, economic, cultural or social identity. Examples are; A bank customer whose BVN, phone number, and transaction history are stored by a bank, a student whose academic records and biometric data are held by a university. An employee whose payroll, medical or performance records are processed by an employer, a social media user whose photos, messages, or location are processed by an online platform or a patient whose medical records are processed by a hospital. A person still remains a data subject even if their name is not mentioned, provided they can still be identified by their IP address, biometric data, facial recognition data and unique customer numbers.

2.2 Personal Data

This constitutes another key concept in the analysis of the right to be forgotten under applicable privacy laws. The Nigerian Data Protection Act, 2023, being the primary legislation on the protection of data defines personal data as:

“Any information relating to an identified or identifiable natural person (data subject) an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual”⁶

⁵ Article 4(1) GDPR 2016, Section 65 NDPA, 2023, 1.3 NDPR 2019

⁶ Article 4(1) General Data Protection Regulation (GDPR) 2016, Section 65 NDPA, 2023.

The Nigeria Data Protection Regulation 2019 also defines personal data as follows:

“Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.⁷

2.3 Sensitive Personal Data

Sensitive personal data often called special category data, refers to a specific class of personal information that is considered highly private and requiring stronger legal protection because its misuse could significantly harm an individual’s rights, dignity, or freedoms. The Nigerian Data Protection Act, 2023 defines “Sensitive Personal Data” as personal data relating to an individual’s;

- a. genetic and biometric data for the purpose of uniquely identifying a natural person;
- b. race or ethnic origin;
- c. religious or similar beliefs, such as those reflecting conscience or philosophy;
- d. health status;
- e. sex life;
- f. political opinions and affiliations;
- g. trade union membership; or

⁷ Part One, 1.3, XIX Nigerian Data Protection Regulation, 2019

- h. other information prescribed by the Commission (NDPC) as Sensitive Personal Data under section 30(2)⁸

The Nigeria Data Protection Regulation 2019 defines Sensitive Personal data to wit: “Sensitive Personal Data” means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.⁹

2.4 Right to Erasure or the Right to be Forgotten

The term “right to erasure” or the Right to Deletion also known as the right to be forgotten, is one of the fundamental rights available to a data subject under the Nigerian Data Protection Act. The right to erasure is the legal entitlement of a data subject to have personal data concerning them erased without undue delay where the continued processing of such data is no longer justified, lawful, or necessary. Individuals have the right to ask organizations to delete their data from their systems under certain circumstances. This can be when the data is no longer needed when it was processed unlawfully, or when it no longer serves the original purpose for which it was collected.

This right is neither expressly defined under the Nigeria Data Protection Regulation 2019 nor explicitly articulated in the principal legislation governing data protection in Nigeria, the Nigerian Data Protection Act, 2023. Notwithstanding this absence of a formal definition, the statutory framework implicitly recognises the substance of the right by empowering data subjects to request the prompt erasure of their personal data by data controllers under specified circumstances. The Nigeria Data Protection Regulation 2019 adopts the term “deletion” whereas the Nigerian Data Protection Act 2023 employs the term “erasure” to describe the same

⁸ Section 65 Nigerian Data Protection Act, 2023

⁹ Part One, 1.3, XXV Nigerian Data Protection Regulation, 2019

concept. Where can this right be exercised? This right is exercisable where: the data is no longer necessary in relation to the purpose for which it was collected, the data subject withdraws the consent upon which the processing is based; the personal data have been unlawfully processed and the data subject objects to continued processing of such data the data controller processes data without lawful basis. This applies to both physical and digital storage of data, and organizations are required by law to comply with such requests within a specific timeframe.

3.0 HISTORICAL EVOLUTION OF THE RIGHT TO BE FORGOTTEN

The right to be forgotten was globally highlighted by the decision of the European Union Court of Justice (the “EUCJ”) in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.¹⁰ According to Bielu and Ibezim, this case served as a catalyst for the European Union (EU) to codify the right to erasure in the General Data Protection Regulation (GDPR).¹¹ However, preceding this landmark case, the Argentine Court addressed the right to erasure in the 2009 legal matter of *Virginia Da Cunha v Yahoo S.R.L and Google*,¹² involving the Argentine popstar, Virginia Da Cunha. In this instance, Da Cunha sought the removal and erasure of internet search results linking her to explicit content. Despite the trial court ruling in her favour, the appellate Court later overturned the decision.¹⁶

¹⁰ C-131/12 2014 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131#t-ECR_62012CJ0131_EN_01-E0001> accessed 23 March 2026

¹¹ KJ Bielu and O Ibezim, *Enforcement of the Right of Erasure in Africa: A Comparative Socio-Legal Study*, (2023) (4)(2) *Law and Social Justice Review* (LASJURE)

¹² 99.613/06 (2014) Edward L. Carter, *Argentina's Right to be Forgotten*, 27 *Emory Int'l L. Rev.* 23 (2013).

In this case, a Spanish citizen, Mr. Mario Gonzalez filed a claim before the Spanish Authority for Personal Data Protection (“SPDP”) against two national newspapers, as well as Google Spain and Google Inc (“Google”). The applicant had a problem with the fact that any internet user who typed his name in the Google search engine would receive, as a result, two publications by a Spanish newspaper regarding a confiscation order for his house, relating to an attachment proceeding for the recovery of his social security debts. He sought for an order that the newspaper and Google erased his name from the publications and that his personal data be erased from results produced from Google searches. His argument was hinged on the fact that the attachment and confiscation had been long resolved; therefore, reference to it was completely uncalled for. The SPDP on one hand dismissed the claim regarding the Newspaper on grounds that the newspaper was not obliged to repeal the publications, since they were lawfully published on the date on which they were issued; but on the other hand, upheld that of Google, holding that search engines (Google) are personal data processors and were mandated to erase the personal data further to the request by Mr. Gonzalez.

Dissatisfied, Google appealed the decision before the EUCJ. Google requested that the EUCJ should determine its liability as a Data Processor and assess whether a Data Subject has the right to request that Google erase his personal data-on the right to have his personal data forgotten. In delivering its ruling, the EUCJ found that Google is indeed a processor of personal data. Also, the court took into consideration the privacy rights of Mr. Gonzalez and found it weightier than the economic interest of Google. The EUCJ found that even though search engines have the right to process Personal Data, this right is limited, especially when it is in contention with the right to privacy, which goes to the heart of the rights of Data Subjects. The EUCJ underlined that the economic interests of the search engine (Google) are not enough to override the right to privacy and further stated that the right to privacy prevails over the right of the public to gain access to the Personal Data of a Data Subject. On the basis of the aforementioned reasoning, the court ruled in favour of Mr. Gonzalez and

held that the information relating to the attachment proceedings relating to him be deleted, given that the information was outdated, and Google had the obligation to erase it. This decision gave credence to the right to be forgotten.

In *Hillary Ogom v. Google LLC & Anor*,¹³ which was brought before the High Court of Lagos State, a cleric, who had been convicted and imprisoned in the United Kingdom, filed a suit against Google in Lagos, Nigeria. He sought a court order to compel Google to delete or erase information pertaining to his previous conviction and imprisonment in the United Kingdom from Google search engine. His claim was premised on the alleged stigmatisation he faced due to the continued presence of the information on Google. The Court dismissed this action and held that the claimant failed to establish a violation of his rights to privacy, freedom of association and the dignity of his human person. Additionally, the Court stated that he had failed to meet the legal requirements for invoking the right to be forgotten. Several lapses were identified in this case, first, the claimant, Hillary premised his claim on his right to privacy under the constitution of the Federal Republic of Nigeria, 1999 alone, and failed to reference or rely on the right to be forgotten as contained in the *Nigeria Data Protection Regulation 2019* (which was the extant regulation at the time). If this right had been properly explored, the High Court may have likely followed the path of the EUCJ in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*¹⁴ while giving its decision.

4 THE LEGAL FRAMEWORK FOR THE RIGHT TO ERASURE IN NIGERIA

The Nigeria Data Protection Regulation 2019 gives the Data Subject the right to request the data controller to delete personal data without delay

¹³ Suit No. IKD/319/GCM/2019 (Unreported)

¹⁴ *ibid*

and the controller shall delete the Personal Data where one of the following grounds applies:

- a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
- b) the Data Subject withdraws consent on which the processing is based
- c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing
- d) the Personal Data have been unlawfully processed; and
- e) the personal Data must be erased for compliance with a legal obligation in Nigeria.¹⁵

The NDPA 2023 which is the principal legislation which guarantees the rights of data subjects, also guarantees the right to erasure and the enforcement of same. This right may be exercised in two distinct ways:

- a) Proactive Deletion by the Organisation (Data Controller):** Pursuant to section 24(d) of the Nigerian Data Protection Act 2023, a data controller is authorised to independently erase personal data *suo motu* where it has become unnecessary for the purpose for which it was originally collected.
- b) Deletion at the Instance of the Data Subject:** Under section 34(1)(d) of the Nigerian Data Protection Act 2023, a data subject is entitled to request the deletion of their personal data. Upon such a request, the data controller is expected to promptly effect the erasure, provided that no lawful basis exists for retaining the data and that it is no longer required for its original purpose.

The data controller is also under obligation to delete the personal data without undue delay, where-

- a) the personal data is no longer necessary in relation to the purpose for which it was collected or processed; or

¹⁵ Part 3, 3.1, 9 Nigerian Data Protection Regulation 2019

b) the data controller has no other lawful basis to retain the personal data”¹⁶

Section 24 (1) (b) of the NDPA 2023¹⁷ states that a data controller or data processor shall ensure that personal data is collected for specified, explicit and legitimate purposes, and not to be further processed in a way incompatible with these purposes. This is referred to as the principle of data minimisation. This principle connotes that the data controller should limit the processing and/or collection of personal information to directly achieving the specific purpose for which the information is collected or processed. By this, it is not acceptable to collect extra data because it might be useful later on, or simply because no thought has been given to whether it is necessary in a specific scenario.

The Nigeria Data Protection Act (NDPA) 2023 General Application and Implementation Directive (GAID) 2025 emphasises the data subject’s right to be forgotten. It specifically provides in Article 38 (1) that; A data subject has the right to have his or her personal data erased if: The personal data is no longer necessary for the purpose a data controller or data processor originally collected or processed it. By the provisions of Article 38 (1) (a) of the NDPA-GAID 2025,¹⁸ once data collected has been used for the purpose for which it was collected or processed, or is deemed to no longer be necessary for the purpose for which it was collected or processed, the subject has the right to request that the data controller/data processor erases the data from its system. ‘A data controller or data processor is relying on an individual’s consent as the lawful basis for processing the data and that individual withdraws his or her consent.’

The Act states that data processing shall be lawful when inter alia, the data subject has given and not withdrawn consent for the specific purpose

¹⁶ Nigerian Data Protection Act 2023, s 34 (2)

¹⁷ Ibid. NDPA 2023, s 24 (1) (b)

¹⁸ Art 38 (1) (a) of the NDPA-GAID 2025

or purposes for which personal data is to be processed.¹⁹ The entirety of Section 26 of the Act unequivocally announces the right of a data subject to withdraw consent which had already been given. Consent is a crucial principle of data protection that allows the data subject to be in control of when their personal data is processed. Consent given should be explicit, and the data controller/processor must show that consent is retained at the time of collection and/or processing.

The NDPA 2023-GAID 2025 has made it clear that a data subject has the right to withdraw consent already given, and upon such withdrawal, also reserves the right to demand that personal data be deleted. A data controller or data processor is relying on legitimate interest as its justification for processing an individual's data, of which, the individual objects to this processing, and there is no overriding legal ground for the organisation to continue with the processing. A court may, at the instance of a data subject or in the course of legal proceedings, give a ruling or judgment mandating that a data controller/processor erase personal data of a data subject. This leaves the data controller/processor with no choice but to comply, unless a stay of execution of the judgment is secured and the ruling or judgment is appealed. The Act states that without prejudice to its provisions, where a data controller or data processor has made personal data public or has shared data with third parties, the data controller is under obligation to ensure the erasure of such personal data by the third parties at the request of the data subject or in compliance with the directives of the Commission in that regard.²⁰

Complying with the Right to Be Forgotten is not straightforward; it requires businesses to balance privacy rights, legal obligations, and public interest considerations when handling personal data removal requests. This brings us to the question of whether a data subject's right to be forgotten is absolute if properly invoked. The provisions of the NDPA

¹⁹ NDPA 2023, s 25 (1) (a)

²⁰ Art. 38(3), The NDPA 2023 -GAID 2025,

2023 give the impression of the absoluteness of these provisions. But, is this right of erasure or right to be forgotten or erasure absolute? There are certain exceptions provided by the law which restricts this particular right.

4.1 Exceptions to the Data Subject's right to erasure or the right to be forgotten

Article 38 (2) of the NDPA 2023-GAID 2025,²¹ provides exceptions to the rights of data subjects to erasure also known as the right to be forgotten. The subsection provides that an organisation's interest in processing the personal data may override a data subject's right to be forgotten if:

- a) The data is being used to exercise the right of freedom of expression and information subject to the limit of derogation permitted under *Section 45* of the *1999 Constitution* and other safeguards of the *NDPA 2023*.

The Constitution of the Federal Republic of Nigeria 1999²² (as amended) (the Constitution) states that every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference. It also states that “every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions”.

This right is, however, subject to the limit of derogation permitted under Section 45 of the Constitution. This provision shall not invalidate any law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health, or for the purpose of protecting the rights and freedom of other persons.²³

- b) The data processing is necessary:

²¹ Article 38 (2) of the NDPA 2023-GAID 2025

²² Section 39 of the Constitution of the Federal Republic of Nigeria 1999 (as amended)

²³ Ibid. s 45

- i. to comply with a legal ruling or obligation.
 - ii. to perform a task that is being carried out in the public's interest or when exercising an organisation's official authority.
 - iii. for public health purposes and to serve the public interest.
 - iv. to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
- c) The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely impair or halt progress towards achieving the goal of the processing.
 - d) The data is being used for the establishment of a legal defence or in the exercise of other legal claims.

The right to be forgotten may not also apply where there is a public interest pursued by disclosure of the data to the general public, provided that the burden of proving the existence of a public interest shall be on the data controller who intends to keep the personal data public.²⁴ From the foregoing, it is evident that data subjects are entitled to request the erasure of their personal data from data controllers and data processors, however, what happens in situations where this data has already been incorporated into artificial intelligence training models posed by the permanence of training data within such models?

5.0 PRACTICAL, LEGAL AND TECHNOLOGICAL CHALLENGES IN THE ENFORCEMENT OF THE RIGHT TO BE FORGOTTEN

The French Philosopher, Michel de Montaigne explains the paradox of forgetting when he said 'nothing fixes a thing so intensely in the memory as the wish to forget it'.²⁵ This in a way captures the enigma associated

²⁴ The NDPA 2023-GAID 2025.

²⁵ Michel de Montaigne Quotes <<https://allauthor.com/quote/195/>> Accessed March 23, 2026.

with the erasure of data in this digital age: The balance of interests between personal autonomy/privacy viz-a-viz technological immutability. Villaronga, Kieseberg and Li²⁶ also posits that artificial intelligence fundamentally changes our current understanding of privacy because much of what scholars conceive to be privacy today rests on an understanding of how humans process information especially, how humans remember and forget and that unfortunately our current laws are not fit to handle the complexities and challenges of artificial intelligence. They stated that when individuals request that their personal information be deleted, this is equivalent to metaphorically requesting that others forget that information.

However, this metaphor is unique to human minds only and does not translate to the Artificial Intelligence and machine learning era. Specifically, the right to be forgotten requirements of data deletion do not easily translate because AI does not “forget” data in the way that humans do and this makes data deletion in artificial intelligence contexts much more complex. Hence, the problem concerning the right to be forgotten lies in the clash between the good intentions of the regulators and the actual complexities of real-life technical environments.

It is further submitted that the implications of erasure in the context of artificial intelligence extend far beyond the data subject making the request. Unlike in traditional databases, where a discrete entry can be deleted with minimal collateral consequences, AI models do not simply store raw data in identifiable units. Instead, personal data contributes to the statistical patterns, weights, and correlations that collectively determine how the model functions. This means that once an individual’s

²⁶ Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li- Humans forget, Machines Remember, artificial intelligence and the right to be forgotten
https://scholarship.law.bu.edu/faculty_scholarship/817/ Accessed March 23, 2026.

data has been used in training, it becomes deeply entangled with other datasets, shaping the predictive outputs of the system as a whole. Attempting to erase one person's information therefore risks disrupting or altering the performance of the entire model.

This perspective underscores the profound tension between the legal right to erasure and the technical immutability of AI training models. The data protection laws as stated above allows the erasure of data when it no longer serves purpose, consent is withdrawn or processing becomes unlawful. However, in Artificial Intelligence, deleting data carries significant consequences as the act of erasure produces ripple effects beyond the individual. Removing one data subject's information potentially disrupts the learned patterns that also rely on related data from others, thereby producing unintended consequences. Hence, while the law conceptualises erasure as an individual right, in practice it requires a collective dimension when applied to AI, forcing regulators, developers, and policymakers to rethink how the 'right to be forgotten' can be realised in environments where forgetting one may inadvertently mean reshaping the knowledge of many.

Easterbrook in his famous article²⁷ cautioned against the temptation to craft special legal regimes for emerging technologies arguing that '*we should not struggle to match an imperfect legal system to an evolving world that we understand poorly. Instead, he stated that the law should do what is essential to permit the participants in this evolving world make their own decisions, thus the world of cyberspace will evolve as it will and enjoy the benefits.*' This perspective is illuminating when examined through the lens of the right to be forgotten and the challenges it poses for Artificial Intelligence (AI) training models. While the right to be forgotten

²⁷ Easterbrook, Frank H. 'Cyberspace and the Law of the Horse' (PDF) (1996) University of Chicago Legal Forum<https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles> Accessed March 23, 2026.

is enshrined in instruments such as the NDPR 2019, NDPA 2023, GAID 2025, GDPR, empowering individuals to demand erasure of personal data, the technical reality of AI complicates these provisions, since training data once absorbed and ingested into models, cannot easily be extracted from the model's parameters or sometimes impossible to 'untrain'. Easterbrook's argument for the modern age would suggest that law should resist technical mandates such as the compulsory model 'untraining' which currently is not feasible but instead focus on embedding the principles of privacy, fairness and accountability on the part of the controllers as this will leave room for innovation without prematurely constraining the evolution of artificial intelligence systems.

The arguments therefore are that; the right to erasure borders around privacy and digital rights which are fundamental human rights and same should remain paramount even in the face of technological advancements or limitations. Conversely, demanding full erasure from AI technologies is almost technically impracticable and may also hinder innovation in the society. Where do we now draw the line between the legal right to erasure and the practical immutability of artificial intelligence training data? How then do we reconcile these two realities of individuals' control over their digital identities and footprints and the structural permanence of AI training models that resist forgetting?

In the case of *NT1, NT2 v Google LLC*²⁸, the UK High Court reached a decision regarding the right to be forgotten where two data subjects who were businessmen requested Google to delist and erase search results linking information about their past crimes and convictions. NT1 had been convicted of conspiracy to account falsely with the purpose of evading tax. He was sentenced to four years' imprisonment and received a disqualification from acting as a company director. The Court of Appeals noted that he had been the principal actor in the false accounting conspiracy. Justice Warby rejected the requested delisting. He underlined

²⁸ 2018 EWHC 799 (QB) UK

that the claimant played a limited role in public life, and the information was not inaccurate, related to his business life, not his personal life, and originally appeared in national media, being a foreseeable consequence of his criminal conduct. Justice Warby concluded that the information retains sufficient relevance today, even though, thanks to a change in the law, the conviction was spent. He highlighted that NT1 remains in business and ‘the information serves the purpose of minimising the risk that he will continue to mislead, as he has in the past’.

A different outcome was reached regarding the second claimant. NT2 had been convicted of phone tapping and computer hacking, of which he pleaded guilty. He was sentenced to six months’ imprisonment. In this case, Justice Warby found that the information had become out of date and irrelevant and there was no sufficient legitimate interest of internet users in its continued availability. The judge noted that the claimant’s past offending was of little, if any, relevance to assess his suitability to engage in business, there was no risk of repetition, and no need for anybody to be warned about it. See also the case of *Tokunbo Olatokun v Polaris Bank Limited*.²⁹

It would seem from the above cases cited that the key element when it comes to exercising the right is the contextual and appropriate balancing of rights and interests of data subjects involved and the extent to which the non-erasure would affect the subjects.

²⁹ Suit No: LD/17392MFHR/2024 Per Hon. Justice Y.A Adesanya of the Lagos High Court where the court found that the bank breached sections of the NDPA by failing to restrict further processing of personal data and denying the applicant’s right to object and erase his personal information to stop sending him marketing emails.

Zhao³⁰ submitted that it will be nearly impossible to forget all digital memories in the context of Artificial Intelligence training models. It may be nearly impossible to completely delete or block all access to the data or digital memories regarding AI agents. To achieve full “forgetting” data controllers and processors must (1) continuously trace all the digital locations where the relevant data, including the derivative data is archived, and (2) individually evaluate whether the data should be deleted or de-indexed within a reasonable period of time, but doing so is costly. After the tracing and evaluation, the data at issue should be removed from the requester’s view to prove it has been forgotten. The data deletion may interrupt the consistent functioning of a particular Machine Learning process. The author also opined that, considering long-term backups, which store the long history of the previous algorithmic processing as references for future operation and possess extraordinary merits for the consistency of the machine learning process, the downside to it is a certain level of deterioration of such backups could negatively affect the entire operation of the machine. Further, the efficiency of the algorithm could decrease due to a lack of data of enough volume, possibly resulting in the ineffectiveness of the whole training data model.

We would also agree with Zhao on this because deleting or erasing a data subject’s data and having a long term backup for it, is as good as not deleting the data and also attempting to remove the data from the requester’s algorithm or view to prove that it has been forgotten is clearly against the principle of transparency which is clearly provided for in the data protection laws. Zhao suggested that new technical measures, such as encryption, anonymization and pseudonymization but opined that they

³⁰ Zeyu Zhao-The Application of the Right to be forgotten in the machine learning context: From the perspective of the European Laws, *Catholic University Journal of Law and Technology*. Vol 31, Issue 1, Pg 83, 2022.

still not as effective as they are presumed to be.

Another Challenge is the conflict with Other Rights such as Freedom of Expression. The right to be forgotten is not absolute and must be carefully balanced against competing fundamental rights, particularly the right to freedom of expression. No right enjoys inherent superiority; rather, any conflict between them is resolved on a case-by-case basis, taking into account the specific facts and circumstances involved.

Public's Right to Information is another challenge. The accessibility of information plays a crucial role in facilitating research, due diligence, and the protection of public safety. For example, the continued availability of records concerning a person's prior criminal conviction may be necessary to prevent them from occupying sensitive positions or to safeguard vulnerable groups, such as children, from potential harm. Although such consequences may appear punitive after the completion of a sentence, they often serve important societal objectives.

6.0 CONCLUSION

Although the internet may retain an enduring memory, a strong legal framework, coupled with a balanced judicial approach, can prevent individuals from being permanently defined by their past. Clear regulatory standards and consistent enforcement can foster an environment in which privacy rights are protected without unduly restricting freedom of expression or access to information. Privacy is a fundamental human right and by extension the right to be forgotten as a data subject right and same must be maintained with respect and dignity as was reechoed by the the Supreme Court in the case of *Chief Dr. (Mrs) Olufunmilayo Ransome-Kuti & Ors v. The Attorney General of the Federation*³¹ that "human Right is a right which stands above the ordinary

³¹ (1985) NWLR (Pt. 6) 211 Human Right is a right which stands above the ordinary laws of the land and which in

laws of the land and which in fact is antecedent to the political society itself. It is a primary condition to a civilised existence and what has been done by our constitution...is to have these rights enshrined in the constitution so that the rights could ‘immutable’ to the extent of the ‘non-immutability’ of the constitution itself.”

7.0 RECOMMENDATIONS

A shift is recommended from an absolutist conception of erasure to a more pragmatic approach. This should include functional delisting, stronger regulatory oversight, and clearer compliance obligations for data controllers. Beyond legal and technological frameworks, individuals also play a critical role in managing their digital identities. Digital literacy and awareness of privacy rights are essential for understanding how personal data is collected, stored, and shared. Data subjects should adopt proactive measures, such as adjusting privacy settings, using encrypted communication tools, and exercising caution when disclosing personal information online. Although the right to be forgotten offers a legal mechanism for seeking data removal, preventive practices remain the most effective means of safeguarding digital privacy.

fact is antecedent to the political society itself. It is a primary condition to a civilised existence and what has been
done by our constitution...is to have these rights enshrined in the constitution so that the rights could ‘immutable’
to the extent of the ‘non-immutability’ of the constitution itself.