ENFORCEMENT OF THE RIGHT OF ERASURE IN AFRICA: A COMPARATIVE SOCIO-LEGAL STUDY*

Abstract

The paper explores the enforcement of the right of erasure in Africa, focusing on a comparative legal and sociological analysis. With the surge in internet users in Africa, the need to protect data subjects' personal information has become paramount. The 'Right to be Forgotten,' rooted in the European Union's jurisprudence, allows individuals to limit, delete, or correct misleading or irrelevant personal information on the internet. This research delves into the backdrop of the right of erasure in Nigeria, evaluating its legislative and sociological frameworks, and comparing them with European norms. The historical evolution of this right, particularly through the landmark Google Spain case, is examined, emphasizing its incorporation into the General Data Protection Regulation (GDPR). In the context of Nigeria, the study analyzes the provisions of the Nigeria Data Protection Act, 2023 (NDPA) and the Nigeria Data Protection Regulation (NDPR), highlighting potential conflicts and similarities. A comparative analysis with other common law jurisdictions, including the United Kingdom, South Africa, and Ghana, reveals variations in the grounds for erasure. The work also addresses the delicate balance between the right to erasure and the right to information, emphasizing the need for a nuanced understanding of both in the digital age. The study used the Doctrinal legal research methodology, and it is analytical and descriptive in nature. This study employed aids and texts from various online materials, journal articles, and newspapers articles. The research found that Nigerian courts can contribute to the development of a robust legal framework that protects individuals' right to erasure in the evolving digital landscape. In form recommendations to Nigerian Courts, the research outlined key steps for a systematic analysis of the application of the right to erasure. These steps include grasping the legislative framework, clarifying the scope of the right, balancing rights and interests, establishing grounds for erasure, assessing technological realities, and ensuring adequate remedies.

Keywords: Right of Erasure, Enforcement, Comparative Socio-Legal Study, Africa

1. Introduction

With the substantial increase in the rise of internet users in Africa, there is a growing consciousness that the personal data of consumers need to be protected and the regulation of the use of personal data by both public and private entities. This global trend has led to the emergence of *'*new forms of right*'*. The usage of the term, 'new', however, does not connote the traditional conception of novelty but rather speaks to the reformation of existing rights. One of these rights is the *'*Right to be Forgotten*'*. In simple terms, the Right to be Forgotten is the right of an individual to limit, de-link, delete or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant or anachronistic.[1] The, right to be forgotten, which has gained traction from major part of the west through legislation, policy formation and judicial enforcement, has it's root from the decision of the Court of Justice of the European Union ('CJEU') in *SL, Google Inc. v Agencia Espanela de Proteccion Gonzalez*[2]. One of the justifications for the propagation of this right is that an individual has a right to delete or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant or anachronistic. In some part of Africa particularly in Nigeria, where the municipal laws on freedom of information is still relatively weak and obtaining information about certain individuals and entities especially politically exposed persons and public servants has remained a challenge, the exercise of certain right to be forgotten or right of erasure has been counter argued to resulting to a potential hoarding of facts from the general public and may affect taking key political, socio-economic and developmental decisions. This research overarching aim is to identify backdrop to the right of erasure under extant legislative and sociological frameworks in Nigeria; evaluate the stark value clash between the European Union and Africa normative and structural design and explore the potential application of the freedom of Information to the right of erasure.

2. Historical Evolution of the Right of Erasure

The discussion of the historical evolution of the right to erasure would be incomplete without acknowledging the pivotal case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. This case served as a catalyst for the European Union (EU) to codify the right to erasure in the General Data Protection Regulation (GDPR). 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*,[3] 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 favor, the appellate Court later overturned the decision. However, in 2014, the right to erasure took center stage, this time in Europe during the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. The plaintiff, a Spanish citizen, lodged a complaint with the Spanish Authority for Personal Data Protection (AEPD) against Google Spain and Google Inc., contending that information about his foreclosed house on the search engine infringed upon his right to privacy. He argued that this data was detrimental to his reputation since the foreclosure matter had already been resolved. The case was subsequently referred to the European Union Court of Justice (CJEU), and in a landmark decision affirming the plaintiff's right to erasure, the court noted that: 'an internet search engine operator is responsible for processing that it carries out of personal data which appear on web pages published by the third parties as such, under certain circumstances, search engines can be asked to remove links to webpages containing personal data.'[4] The significant ruling by the CJEU in the mentioned case essentially introduced the right to be forgotten, commonly referred to as the right to erasure. This right has

***By Kachidobelu John BIELU, BL, LLM, PhD,** Senior Lecturer, Faculty of Law, Nnamdi Azikiwe University Awka, Anambra State, +2348037443753, email kachbielu@gmail.com, kj.bielu@unizik.edu.ng; and

***Onyemauche IBEZIM, LLM Candidate**, Faculty of Law, Nnamdi Azikiwe University Awka, Anambra State, Senior Associate at Kenna Partners, No. 8 Ogunyemi Road, Victoria Island, Lagos State, 07035373312, oibezim@kennapartners.com, ucheibezim32@gmail.com

[1] F Manjoo, 'Right to Be Forgotten', Online Could Spread, N.Y. Times (Aug., 5, 2015 cited in Lesile E. Minora, *'*US. Court Should Not Let Europe's Right to be Forgotten Force the World to Forget,' *Temple Law Revie,* (2017), (vol 89), (3), Pp. 609-642.

[2] [2014] European Court of Justice, C-131/12

[3] 99.613/06 (2014).

[4]*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos* (AEPD) and Mario Costeja González [2014] European Court of Justice, C-131/12

since been formally incorporated into the legal framework of the European Union (EU) through the General Data Protection Regulation (GDPR).

3. Background to Right of Erasure in Nigeria before the Enactment of Data Protection Act 2023

In Nigeria, the pioneering legislation that acknowledged the right to be forgotten is the Nigeria Data Protection Regulation (*'*NDPR*'*). Issued by the National Information Technology Development Agency (NITDA) on January 25, 2019, in accordance with Section 32 of the NITDA Act 2007, the NDPR serves as subsidiary legislation to the NITDA Act 2007. Enacted in 2019, this regulation governs the processing of personal data concerning individuals in Nigeria. Within the NDPR, a data subject is empowered with the right to erase their personal data, commonly referred to as the right to be forgotten. According to the NDPR, this right can be exercised under various circumstances as provided for in Regulation 3.1(9) of the NDPR. However, there seems to be a new rave about data protection in Nigeria. With the enactment of the Nigeria's Data Protection Act 2023, there is a new provision for the legal framework for the protection of personal data and the establishment of a new commission for the regulation of the processing of personal data and other related matters.[5]

The provisions of the NDPA and NDPR as they relate to the right of erasure will be discussed below.

In Nigeria, the primary legislation that governs data protection is the Nigeria Data Protection Act, 2023 (*'*NDPA*'* or the *'*Act*'*) recently signed into law on June 23, 2023. The Act makes provision for the right of erasure, specifically, Section 34 (2) of the Act[6] provides that a data controller shall erase personal data without any delay in the following instances; '(a) the personal data is no longer necessary, in relation to the purposes for which it was collected or processed, or; (b) the data controller has no other lawful basis to retain the personal data'. However, before the enactment of the NDPA, the National Information Technology Development Agency (NITDA) had put in place the Nigeria Data Protection Regulation (*'*NDPR*'* or *'*the Regulation*'*) as the primary data protection regulation. The Regulation makes copious provisions for the right of erasure beyond the scope contained in the NDPA. Regulation 3.1(9)[7] in particular states that Data Subject may request a data controller to delete personal data without delay and the data controller shall delete such personal data in any of the following events;

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;
e) the Personal Data must be erased for compliance with a legal obligation in Nigeria.

Additionally, the Regulation mandates data controllers who have made such Personal Data public to delete the Personal Data and to inform Controllers processing the Personal Data of the Data Subject's request.[8] It might seem that the NDPA narrows down the grounds for a data subject to request the erasure of their data to two primary reasons, contrasting with the NDPR. This raises the question of whether the NDPA's provisions regarding the right to erasure take precedence over those of the NDPR. A closer examination of Section 64 of the NDPA indicates that the Act doesn't explicitly annul the NDPR; instead, it safeguards all regulations established by NITDA or the Nigerian Data Protection Bureau (NDPB) concerning data protection. This implies that all regulations pertaining to data protection, including the NDPR, formulated by these bodies, remain valid. Moreover, Section 63 anticipates potential conflicts and stipulates that if any law or enactment related directly or indirectly to the processing of Personal Data contradicts the provisions of the Act, the Act prevails. It is argued that the NDPR's provisions endure as long as they do not clash with the NDPA's stipulations. In our examination, the provisions of the NDPA and NDPR seem to align concerning the right to erasure.

4. Comparative Analysis between right of erasure in Nigeria and Selected Common Law Jurisdiction

For a comprehensive grasp of the right to erasure, it is essential to examine how other jurisdictions, akin to Nigeria, approach this matter.

United Kingdom

The primary data protection legislation in the United Kingdom is the General Data Protection Regulation (*'*GDPR*'* or *'*the Regulation*'*). Following the 2014 CJEU judgment in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, the right to erasure was formalized within the GDPR. Both the GDPR and the NDPR outline comparable grounds on which a Data Subject can seek the erasure of their data. However, the GDPR introduces two additional grounds, which are:

a) an organization is processing personal data for direct marketing purposes and the individual objects to this processing;
b) an organization has processed a child's personal data to offer their information society services.

Additionally, the GDPR unlike the NDPA and the NDPR goes further to outline specific circumstances where the data controller is obliged not to erase the data. These instances include where:

a) the data is being used to exercise the right of freedom of expression and information;
b) data is being used to comply with a legal ruling or obligation;
c) the data is being used to perform a task that is being carried out in the public interest or when exercising an organization's official authority;
d) the data being processed is necessary for public health purposes and serves in the public interest;
e) the data being processed is necessary to perform preventative or occupational medicine (this applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy);

[5] Nigeria Data Protection Act 2023. S 4(1)
[6] Nigeria Data Protection Act 2023
[7] Nigeria Data Protection Regulation
[8] NDPR, R 3.1(10)

f) 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 to impair or halt progress towards the achievement that was the goal of the processing;
g) the data is being used for the establishment of a legal defense or in the exercise of other legal claims.
h) The data is being used for the establishment of a legal defense or in the exercise of other legal claims.

Based on the above, it seems that concerning the right to erasure, the GDPR aims to reconcile this right with the rights of freedom of expression and information. In contrast, the NDPA and NDPR do not explicitly address this aspect.

South Africa
In South Africa, the predominant data protection law is the Protection of Personal Information Act (POPIA). POPIA acknowledges the right to erasure, but unlike its Nigerian and EU counterparts, its application is notably restricted. The Act allows Data Subjects the right to prompt destruction or deletion of their personal data only when the data is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or lawfully obtained. Similar to the NDPA and NDPR, POPIA does not specifically address scenarios where the right to erasure is not applicable.

Ghana
The Data Protection Act of 2012 in Ghana ('DPA') includes provisions for the right to erasure. However, this right, as outlined in the DPA, seems to have a more restricted scope, especially when contrasted with the NDPR. According to the Act, data subjects are permitted to rectify or remove personal data controlled by a data controller if the data is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or acquired unlawfully. Similar to the NDPA and the NDPR, the Act does not offer exceptions to the right to erasure.

5. Comparative Analysis of Right to Erasure and Right of Information under Current Data Protection Regime
Following the incorporation of the right to be forgotten, doubts remain about the effective scope of the right to erasure and the right to be forgotten, especially as regards the relationship with the right to report and the right to information. Generally, it can be said that the requirements of the right of information insofar as it is a correct exercise of this right, whereas instead it must necessarily leave room for the right to privacy and the right to be forgotten when the news is no longer relevant and of public interest. The right to be forgotten has been criticised by the representatives of the American doctrine, jurisprudence, and journalists, considering the potential breaches of the freedom of speech. The right to be forgotten had been criticized for being antithetical towards the free expression and as distorting the benefits attending unfiltered access to information.[9] The Court of Justice of the European Union has developed a fair balance test in the *Google v. AEPD & Gonzalez judgement*. It provided equality of individual's right to privacy and the freedom of expression.[10] Its main aim was to safeguard interests of both parties. In fact, very few fundamental rights are absolute. In most of cases, one right can be limited, so the other right can be ensured. The right to be forgotten and the right to information represent different facets of the balance between privacy and transparency in the digital age. The former focuses on personal data control, particularly in online contexts, while the latter emphasizes citizens' access to information held by public authorities. Achieving a harmonious coexistence of these rights involves careful consideration of legal frameworks and a nuanced understanding of the societal implications of both.

In the era of rapid technological advancement and increasing digitization, the delicate balance between individual privacy and the public's right to information has become a focal point in legal discussions. Two fundamental rights underpin this discourse: the Right to Information often associated with transparency and accountability, and the Right to Erasure, commonly known as the right to be forgotten, emphasizing individual control over personal data. The Right to Information serves as a cornerstone of democratic societies, facilitating transparency, citizen empowerment, and government accountability. Enshrined in various legal frameworks globally, the right allows individuals to access information held by public authorities and, in some cases, private entities performing public functions. The GDPR acknowledges the importance of this right but also recognizes the need to balance it with other fundamental rights, including privacy. Under the GDPR, individuals are granted the right to request access to their personal data held by organizations. This transparency aims to foster trust and empower individuals to understand and challenge the processing of their information. However, the regulation acknowledges that certain exemptions may be necessary, such as protecting national security or individual privacy. Conversely, the Right to Erasure, introduced prominently in the GDPR, focuses on individual control over personal data. Also known as the right to be forgotten, this right empowers individuals to request the removal of their personal data under specific circumstances. These circumstances include situations where the data is no longer necessary for its original purpose, the individual withdraws consent, or the data processing is unlawful. The Right to Erasure aims to address the permanence and ubiquity of information on the internet. It recognizes that individuals should have the ability to manage their online identity and prevent outdated or inaccurate information from negatively impacting their lives.

6. Conclusion and Recommendations
As Nigeria navigates the intricate terrain of data protection and privacy, the courts play a pivotal role in shaping the contours of the right to erasure. By following a systematic roadmap that encompasses a thorough understanding of the legislative framework, clarification of the right's scope, balancing competing interests, establishing clear grounds for erasure, staying abreast of technological realities, and ensuring adequate remedies, Nigerian courts can contribute significantly to the development of a robust and responsive legal framework for the protection of individuals' right to erasure. This proactive approach will not only fortify privacy rights but also foster a digital environment that respects the dignity and autonomy of individuals in the face of advancing technologies. In an age dominated by digital advancements and an unprecedented influx of information, the right to erasure has emerged as a crucial component of data protection frameworks worldwide. In Nigeria, as the legal landscape grapples with the challenges of safeguarding individual privacy, it becomes imperative for the courts to

[9] A Carbone, Chelsea E, 'To be or not to be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age' Va. J. Soc. Pol'y & L. 22 (2015): 525.
[10] *Google v. AEPD & González case* (n 2) para 81, 88

chart a roadmap for the systematic analysis of the application of the right to erasure. Below are the key steps that the Nigerian courts should consider in navigating this evolving terrain:

Grasping the Legislative Framework
The foundation of any legal analysis begins with a comprehensive understanding of the legislative framework. In the case of the right to erasure, Nigerian courts should delve into existing data protection laws, such as the Nigeria Data Protection Regulation (NDPR). An intricate examination of these statutes will enable the judiciary to identify the legal provisions that govern the right to erasure, ensuring that the legal analysis is firmly grounded in the established legal framework.

Clarifying the Scope of the Right to Erasure
A nuanced understanding of the scope of the right to erasure is fundamental to its application. Nigerian courts should define the parameters within which the right operates, including the types of personal data covered and the specific circumstances under which individuals can invoke this right. Clarity on the scope will serve as a guiding principle for courts when adjudicating cases involving the erasure of personal data.

Balancing Rights and Interests
The right to erasure does not exist in isolation; it must be harmonized with other fundamental rights and societal interests. Courts in Nigeria should undertake a meticulous balancing exercise, weighing the right to erasure against competing rights, such as freedom of expression and public interest. Striking a delicate balance is essential to ensure that the application of the right to erasure is fair, just, and in harmony with broader societal goals.

Establishing Grounds for Erasure
To provide clarity and consistency, Nigerian courts should delineate the specific grounds on which individuals can seek the erasure of their personal data. Whether based on inaccuracies, expiration of the purpose of data processing, or withdrawal of consent, courts should articulate a clear framework for evaluating the legitimacy of erasure requests.

Assessing Technological Realities
Given the dynamic nature of technology, Nigerian courts must remain attuned to the evolving landscape of data processing. Understanding the intricacies of data storage, retrieval, and dissemination is crucial for courts to make informed decisions when adjudicating erasure cases. Collaboration with technology experts and staying abreast of technological advancements will enhance the court's ability to render judgments that are both legally sound and technologically relevant.

Ensuring Adequate Remedies
Courts should consider the availability of effective remedies when the right to erasure is violated. Establishing a robust system of remedies, including injunctions and damages, will incentivize compliance with data protection laws and reinforce the importance of respecting individuals' rights to control their personal information.