Africa in the digital age: a case for the right to be forgotten under the African Charter on Human and Peoples' Rights

*Takunda Gumbu**
https://orcid.org/0009-0006-0255-9299
*Panashe Nhekairo***
https://orcid.org/0009-0005-0049-5802

ABSTRACT: This article advances that the right to be forgotten (RTBF), which affords individuals a legal tool to erasure of personal digital data under certain circumstances, is an essential right in the digital age. It discusses the RTBF and traces its development to the European Union (EU) jurisprudence. The article argues that, although the RTBF was developed under the EU jurisprudence and despite it being not expressly recognised under the African Charter on Human and Peoples' Rights (Charter), it can be read into the Charter through three methods. First, it can be read into the Charter through the *SERAC* principle, namely, that some unenumerated rights are implied by the African Charter, as set in the Commission's decision in *Social and Economic Rights Action Centre and Center for Economic and Social Rights v Nigeria*. Second, the right can be read into the Charter through the progressive application principle as envisaged by articles 60 and 61 of the Charter. Third, the RTBF can also be read into the Charter by employing article 31 of Vienna Convention on the Law of Treaties. The article submits that although some African countries have made tentative steps in adopting the RTBF in their domestic jurisdiction and despite the recognition of the right in some of the continent's instruments, its recognition in the African human rights system is fragmented. This fragmentation hinders adequate protection of the right. The article ultimately argues that the superior status that the African Charter enjoys in the African human rights system justifies the need for the RTBF to be read into the Charter to ensure adequate protection and to create a pathway for robust law reforms related to the protection and autonomy over personal data in Africa's national jurisdictions.

TITRE ET RÉSUMÉ EN FRANÇAIS:

L'Afrique à l'ère du numérique: plaidoyer pour la garantie du droit à l'oubli dans le système de la Charte africaine des droits de l'homme et des peuples

RÉSUMÉ: Cette contribution soutient que le droit à l'oubli ou à l'effacement numérique, qui offre aux individus un outil juridique pour effacer les données numériques dans certains circonstances, est un droit essentiel à l'ère du numérique. Elle examine le droit à l'oubli et retrace sa genèse des politiques de l'Union européenne (UE). La contribution avance que, bien que le droit à l'oubli ait été développé au sein de l'UE et bien qu'il ne soit pas expressément garanti par la Charte africaine des droits de l'homme et des peuples (Charte), il peut en être déduit à travers trois méthodes.

* LLB, LLM candidate (Unam); ttgumbu@gmail.com
** LLB, LLM candidate (Unam); panashenhekairo@gmail.com

T Gumbu & P Nhekairo 'Africa in the digital age: a case for the right to be forgotten under the African Charter on Human and Peoples' Rights' (2023) 7 *African Human Rights Yearbook* 94-115
http://doi.org/10.29053/2523-1367/2023/v7a5

Premièrement, par le biais du principe juridique que certains droits non énumérés sont implicites dans la Charte africaine, développé dans l'affaire de la Commission africaine des droits de l'homme et des peuples *Social and Economic Rights Action Centre et Center for Economic and Social Rights v Nigeria*. Deuxièmement, le droit à l'oubli peut être déduit de la Charte à travers le principe de mise en œuvre progressive des droits garantis par la Charte tel qu'envisagé aux articles 60 et 61 de ladite convention. Troisièmement, ce droit peut être garanti par la Charte en mobilisant l'article 31 de la Convention de Vienne sur le droit des traités. La présente contribution relève que, bien que certains pays africains aient adopté des mesures pour reconnaitre le droit à l'oubli numérique dans leurs législations nationales et malgré la reconnaissance de ce droit dans certains instruments au niveau continental, sa reconnaissance dans le système africain des droits de l'homme est fragmentée. Cette fragmentation entrave la protection adéquate du droit. En conclusion, la contribution avance que la valeur normative de la Charte africaine dans le système africain de protection des droits de l'homme justifie la nécessité de garantir le droit à l'oubli à travers une lecture progressive de la Charte pour sa protection adéquate et de créer une voie pour des réformes législatives robustes relatives à la protection et à l'autonomie en matière de données personnelles en Afrique.

KEY WORDS: right to be forgotten, African Charter on Human and Peoples' Rights, privacy, personal data, digital age

CONTENT:

1 INTRODUCTION

In recent times the use of the internet, especially social media, has become an indispensable part of everyday life of an ordinary person.[1] Easier access to the internet coupled with the advancement of digital technologies, which provide immediate access and dissemination of any information, has brought about a unique form of information and data flow.[2] By the first quarter of the twenty-first century, internet technology had propelled the flow of information across greater distances than previously accomplished in human history.[3] Through internet technologies, people can easily share personal videos,

1 It is estimated that 60% of the world's population uses the internet and social media today. See B Wong 'Top social media statistics and trends of 2023' (2023), Top Social Media Statistics And Trends Of 2023 – Forbes Advisor (accessed 6 July 2023).

2 T Zarsky 'Privacy and manipulation in the digital age' (2009) 20(1) *Theoretical Inquiries in Law* 157.

3 D Waltz 'Privacy in the digital age' (2014) 48(1) *Indiana Law Review* 205, 207.

photographs, audio recordings and documents 'online',[4] which is accessible to anyone and everywhere without the restriction of geographical boundaries. Although it is easy to imagine the socio-economic benefits manifest in the free flow of data and information,[5] there is equally a damning impact – especially where information is used for a totally different and unintended purpose to that of its disclosure.[6]

Internet users often reveal personal information they instantly or eventually regret,[7] or have information about them shared that they wished had been kept a secret.[8] This may, among others, be because of the information posted in the heat of high emotion or under the influence of intoxicating liquor;[9] a post being seen by an unintended audience;[10] and experimenting with digital devices and services, which is quite prevalent among the youth.[11] Unlike human beings who possess the ability to forgive and forget over time,[12] the internet possesses the ability to remember indefinitely.[13] Thus, regrettable information and personal data will linger forever on the internet and will potentially haunt persons implicated in such information or personal data through, amongst others, potential reputational harm, loss of job opportunities, mental distress and strained personal relationships.[14] Undeletable data and information exposes persons to perpetual or at best periodical stigma because of an event performed in the past, thereby restricting individuals to their past.

4 According to the *Pocket Oxford English dictionary* the word 'online' simply means 'available on or carried via the internet'. See M Waite (ed) *Pocket Oxford English dictionary* (2013).

5 K Walker 'Where everybody knows your name: pragmatic look at the costs of privacy and the benefits of information exchange' (2000) *Stanford Technology Law Review* 2-50; see examples outlined therein.

6 R Walker 'The right to be forgotten' (2012) 64(1) *Hastings Law Journal* 257. See particularly the illustration given therein whereby a newly-enrolled college student agreed to pose naked for the pictures intended to be used in a book publication but the pictures ended up on adult websites – which she only realised when she queried her name in an online search engine in preparation of her resumé.

7 Walker (n 6) 259.

8 As above.

9 Y Wang and others '"I regretted the minute I pressed share": a qualitative study of regrets on Facebook' (2011) *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 20-22 July 2011.

10 Wang and others (n 9) 1-6.

11 S Livingstone and others *Children's data and privacy online: growing up in a digital age. An evidence review* (2019) 6-7.

12 V Mayer-Schönberger *Delete: the virtue of forgetting in the digital age* (2009) 11.

13 As above.

14 JL Zittrain *The future of the Internet – and how to stop it* (2008) 44.

In an attempt to mitigate the potential pervasiveness of permanently-available data on the internet, the European Union (EU) through the General Data Protection Regulation (GDPR)[15] recognises the 'right to be forgotten' which affords individuals a legal tool to demand erasure of personal digital data in certain circumstances.[16] By taking to cognisance that the right to be forgotten (RTBF) under the GDPR is only available to mostly EU citizens, this article endeavours to critically examine the justiciability of the RTBF under the African human rights system, particularly the African Charter on Human and Peoples' Rights (African Charter).[17] The article is structured as follows: this first part provides a brief introduction to the article. Part 2 defines the RTBF and outlines its historical development under European law. Part 3 deals with the justiciability of the RTBF under the African Charter and other regional instruments. Part 3 further dwells on the challenges surrounding the implementation of the RTBF. Lastly, part 4 provides a conclusion to the article.

2 THE RIGHT TO BE FORGOTTEN

2.1 Defining 'the right to be forgotten'

In her proposal for the reform of EU data protection rules, the EU Justice Commissioner Viviane Reding defined the RTBF (also known as the right to erasure) as the right for individuals to have their personal data deleted when it is no longer needed for a legitimate reason.[18] However, Reding clarified that RTBF does not amount to 'total erasure of history'.[19] The underlying idea of the RTBF is not to allow individuals to alter their past and erase obnoxious traces of their lives,[20] but to ensure that an individual's present is not muddled up by their past. It therefore follows that the RTBF is a form of forced omission that mitigates against easy accessibility of personal information on the internet and makes such information more difficult to find.[21] Succinctly

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (GDPR).

16 GDPR (n 15) art 17.

17 Organisation of African Unity (OAU) African Charter on Human and Peoples' Rights (African Charter) 27 June 1981, CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982).

18 V Reding, Vice President, European Comission 'The EU Data Protection Reform 2012: Making Europe the standard setter for modern data protection rules in the digital age' (22 January 2012) 5, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF (accessed 11 July 2023).

19 As above.

20 C de Terwangne *The right to be forgotten and the informational autonomy in the digital environment* (2013).

21 H Ramesh & K Kancherla 'Unattainable balances: the right to be forgotten' (2020) 9(2) *NLIU Law Review* 400, 401.

put, 'the right to be forgotten does not mean erasure of the information. It rather means to stop bringing back data from the past.'[22]

2.2 Historical development

The early development of the RTBF in Europe may be traced back to the French legal system. In the late 1970s,[23] French law recognised 'the right to oblivion' (*le droit* à *l'oubli*) which entails 'the right to silence over past instances that are no longer transpiring'.[24] The right to oblivion is an innovation of the French criminal justice system that granted rehabilitated former convicts the right to demand erasure of personal data when the data no longer is relevant.[25] In essence, the right to oblivion allowed criminal convicts the right to object to the publication of information about their conviction and incarceration once they served their sentence.[26] Seemingly, the reason for allowing former convicts to object to the publication of information about their crimes is the realisation that maturation and transformation are part of people's lives and once rehabilitated, ex-convicts must not be restrained to the reputational damage of the past.

From the 1980s onwards, more European jurisdictions started to enact domestic data protection laws that ostensibly recognised the RTBF under the concept of privacy.[27] In 1995 the European Parliament and Council issued the Data Protection Directive (DPD),[28] in which the RTBF can possibly be inferred. Articles 12(b) and 14 of the DPD provided data subjects with the right to ask for erasure of personal information, and to object to processing of personal information on legitimate grounds, respectively. Zanfir asserts that the combination of the article 12(b) of the DPD and article 14 possibly is tantamount to the RTBF.[29]

Notwithstanding the earlier recognition of the right to oblivion in the French legal system, which closely resembles the RTBF, and the possible inference of the RTBF in the DPD, the right remained unclearly recognised. To that effect, in 2012 the European Commission (EC) proposed for a comprehensive review of the DPD to put

22 De Terwangne (n 20) 1.

23 Law 78-17/1978, art 40.

24 MJ Kelly & S David 'The right to be forgotten' (2017) 1 *University of Illinois Law Review* 25.

25 I Stupariu 'Defining the right to be forgotten: a comparative analysis between the EU and the US' unpublished LLM thesis, Central European University, 2015.

26 J Rosen 'The right to be forgotten' (2011-2012) 64 *Stanford Law Review Online* 88-92.

27 Eg, the Data Protection Act, adopted in 1984 by the British Parliament and Wet Persoonsregistraties, enforced in The Netherlands in 1989.

28 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ [1995] L281/31 (DPD).

29 G Zanfir 'Tracing the right to be forgotten in the short history of data protection law: the "new clothes" of an old right' in S Gutwirth and others (eds) *Reforming European data protection law* (2015) 227-249.

individuals in control of their personal data.[30] The draft proposal for the GDPR provided for the RTBF under article 17, which afforded data subjects the right to demand that their personal data be erased under certain conditions.[31] The draft GDPR was eventually made into law in 2016 and repealed the DPD. However, before the GDPR was made into law, the European Court of Justice (ECJ) effectively recognised the RTBF in the seminal case, *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* (*Google Spain* case).[32] The judgment of the *Google Spain* case was delivered in May 2014 and is considered the *locus classicus* to the official recognition of the RTBF in the EU.[33] It therefore is prudent to first delve into the judgment before illuminating on article 17 of the GDPR.

2.3 The *Google Spain* case and emergence of the RTBF

By formally recognising the RTBF, the *Google Spain* case changed the terrain of the right to privacy in this digital age with far-reaching implications. At the pith of this case was the question of whether or not an individual is entitled to have personal information or links to such information totally erased or deleted upon request. Put alternatively, the ECJ was faced head-on with the question of whether the 'right to be forgotten' exists and is enforceable.

In this case, a Spanish national lodged a complaint with the Spanish Data Protection Agency (AEPD) against a local newspaper, Google Spain and Google Inc.[34] The gist of the Spanish national's complaint was two-fold. First, he sought to compel the local newspaper to remove or alter the pages relating to the publication in which his name appeared for a real estate auction connected with attachment proceedings for the recovery of social security debts.[35] Second, the Spanish national also sought to compel Google Spain or Google Inc to remove or conceal links to the concerned article with the effect that such information ceases to appear in the search results.[36] The Spanish national's argument was that referencing web links to the concerned article had become irrelevant as the attachment proceedings concerning him had been fully resolved for a long period of time. The AEPD upheld the Spanish national's complaint insofar as it concerns

30 V Reding 'The European data protection framework for the twenty-first century' (2012) 2(3) *International Data Privacy Law* 119, 199-129.

31 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11.

32 CJEU, Case C-131/12, *Google Spain v APED*, ECLI:EU:C:2014:317 (*Google Spain* case).

33 F Fabbrini & E Celeste 'The right to be forgotten in the digital age: the challenges of data protection beyond borders' (2020) *German Law Journal* 55-65.

34 *Google Spain* (n 32) para 14.

35 As above.

36 *Google Spain* (n 32) para 15.

the complaint against Google Spain and Google Inc, and dismissed the complaint against the local newspaper citing that it was intended for a legitimate reason.[37]

Google Spain and Google Inc then appealed against the decision of the AEPD before the Spanish National High Court which ultimately reached the ECJ. Essentially, the ECJ was tasked to interpret the provisions of the DPD, which was then applicable to the municipal dispute between Google and AEPD together with the Spanish national. With respect to the RTBF, the following question was posed:

> [Mu]st it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?[38]

It is noteworthy that the DPD under article 2(d) imposed responsibility for the use of data on the 'controller' of such data. The ECJ ruled that Google as a search engine, not only is a processor of personal data, but is also a 'controller' within the meaning of the DPD as it located information published by third parties, indexed such information and ultimately made it available to users.[39] On that basis, the ECJ observed that name searches through the Google search engine potentially affects the individual's right to privacy and data protection in a significant way as 'that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life'.[40] Consequently, it held:[41]

> The operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

By delivering the ruling in the *Google Spain* case, the ECJ practically recognised and enforced a new right which empowered data subjects to request erasure or removal of their personal information from the internet, thereby imposing a corresponding obligation on the search engine operators to conceal links to websites published by third parties that contain information on a person from the list of results displayed

37 As above. The AEPD asserted that 'the publication … of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible'.

38 *Google Spain* (n 32) para 20(3).

39 *Google Spain* (n 32) para 41.

40 *Google Spain* (n 32) paras 80-81.

41 *Google Spain* (n 32) para 88.

after a search based on that person's name.[42] The ECJ summarily asserted the RTBF. The ECJ's judgment in the *Google Spain* case paved the way for the full-blown codification of the RTBF under the EU law. The RTBF is now expressly recognised under article 17 of the GDPR, which is discussed in the succeeding part.

2.4 Article 17 of the EU GDPR

Following the *Google Spain* case, the RTBF was codified under article 17 of the GDPR which is titled 'Right to erasure (right to be forgotten)'. The chapeau to article 17(1)(a) reverberates the RTBF as articulated in the *Google Spain* case and provides that '[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay'.[43]

However, the same provision clarifies that the RTBF is not absolute as it is only applicable in six circumstances,[44] including where the personal data is no longer necessary in the context of the purpose of its collection and procession; where personal data have been unlawfully collected; and where personal data has to be erased in compliance with other laws to which the controller is subject.

The underlying rationale of the right to erasure as provided in article 17(1) is that the data subject's personal information ought to be erased upon the presence of the above highlighted conditions among other conditions as specifically mentioned in the GDPR.[45] Further, article 17(2) places a positive obligation on the controller of personal data to take all reasonable steps to erase such information upon request and to inform third-party controllers of such request.

42 See E Frantziou 'Further developments in the right to be forgotten' (2014) 14 *Human Rights Law Review* 761; H Kranenbourg 'Google and the right to be forgotten' (2015) 1 *European Data Protection Law* 70.

43 GDPR art 17(1).

44 GDPR arts 17(1)(a)-(f).

45 Notably, art 4(1) of GDPR defines personal data as 'any information relating to an identified or identifiable natural person ("data subject")'. According to the EC, this information can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address' – see European Commission's press release announcing the proposed comprehensive reform of data protection rules, 25 January 2012, bing.com/ck/a?!&&p=edace6f6f0f584e1JmltdHM9MTY5MDU4ODgwMCZpZ3VpZD0xOTk1MWE0My1iNDFkLTY4NTYtMzkyMi0wOGUxYjU2ZjY5Y2YmaW5zaWQ9NTQzMA&ptn=3&hsh=3&fclid=19951a43-b41d-6856-3922-08e1b56f69cf&psq=European+Commission%27s+press+release+announcing+the+proposed+comprehensive+reform+of+data+protection+rules%2c+25+January+2012&u=a1aHR0cHM6Ly9lYy5ldXJvcGEuZXUvY29tbWlzc2lvbi9wcmVzc2Nvcm5lci9hcGkvZmlsZXMvZG9jdW1lbnQvcHJpbnQvZW4vaXBfMTJfNDYvSVBfMTJfNDZfRU4ucGRmIzp-OnReHQ9Q29tbWlzc2lvbiUyMHByb3Bvc2VzJTIwYSUyMGNvbXByZWhlbnNpdmUlMjByZWZvcm0lMjBvZiUyMGRhdGElMjBwcm90ZWN0aW9uLG9ubGluZSUyMHByaXZhY3klMjByaWdodHMlMjBhbmQlMjBib29zdCUyMEV1cm9wZSUyN3MlMjBkaWdpdGFsJTIwZWNvbm9teS4&ntb=1 (accessed 15 July 2023).

However, it is worth noting that the RTBF as envisaged under article 17 of the GDPR is not absolute as it is subject to the limitations identified in article 17(3). Article 17(3) expressly stipulates that the data subject's right is not applicable where the processing is necessary for 'exercising the right of freedom of expression and information'.[46] Article 17(3) further provides that the right to erasure shall not apply for a few other reasons such as compliance with a legal obligation; for reasons of public interest, public health, and reasons for scientific or historical research and legal defence. It follows that the right to erasure under article 17 of the GDPR must be proportionate to the legitimately recognised interests and rights, such as the right to freedom of expression. In the *Google Spain* case the ECJ confirmed that the fundamental right to erasure ordinarily trumps the economic interest of the operator of the search engine and the public interest in finding such information unless justified by 'preponderant interest of the general public in having … access to the information'.[47]

3 RTBF AS A HUMAN RIGHT UNDER THE UNITED NATIONS HUMAN RIGHTS SYSTEM

Under the United Nations (UN) human rights system the RTBF falls within the ambit of the right to privacy.[48] As Ramesh and Kancherla observed, the RTBF effectively affords individuals a certain level of control over their personal information and availability of such information for public perusal.[49] Although the RTBF cannot be located as a standalone fundamental human right under any United Nations legal instrument, the right to privacy is expressly recognised under article 12 of Universal Declaration of Human Rights (Universal Declaration)[50] and article 17 of the International Covenant on Civil and Political Rights (ICCPR).[51] Article 12 of the Universal Declaration and article 17 of ICCPR are a mirror image of each other and they guarantee individuals' right to privacy and protection of the law against interference with the right to privacy.

The provisions of article 12 of the Universal Declaration and article 17 of ICCPR are both narrowly formulated and there is nothing much to be gleaned insofar as the scope of the right to privacy entails. Given that these instruments predate the digital age, it seems odd and inadequate

46 GDPR art 17(3)(a).

47 *Google Spain* (n 32) para 79. See also BVerfG, order of 6 November 2019, 1 BvR 16/13, press release 83/2019 of 27 November 2019 where the German Federal Constitutional Court applied the EU law and held that the RTBF had to be balanced with freedom of information and freedom of expression.

48 D McGoldrick 'Developments in the right to be forgotten' (2013) 13(4) *Human Rights Law Review* 761, 764.

49 H Ramesh & K Kancherla 'Unattainable balances: the right to be forgotten' (2020) 9(2) *National Law Institute University Law Review* 400, 402.

50 UN General Assembly Universal Declaration of Human Rights, 10 December 1948.

51 UN General Assembly International Covenant on Civil and Political Rights, 16 December 1966.

to rely on these provisions to effectively assert the RTBF and data protection in this digital age. Be that as it may, General Comment 16 of the UN Human Rights Committee (Committee)[52] sheds light on the extent of privacy in relation to electronic devices. In their interpretation of the right to privacy, the Committee recognises that the right to privacy guarantees against all interference and attacks from either the state or natural and legal persons.[53] The Committee further called upon states to 'adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right'.[54] Insofar as technology is concerned, General Comment 16 recognised that individuals should have a right to request rectification or elimination of personal information gathered on electronic devices that contain incorrect information or have been collected or processed contrary to the provisions of the law.

General Comment 16 implies that the right to privacy under article 17 of ICCPR essentially affords individuals the RTBF to the extent that personal information on digital devices such as computers and smartphones is inaccurate or was unlawfully obtained. In addition, the office of the UN High Commissioner for Human Rights (UNHCHR) recognised the implications manifest from the new data-driven technologies on the right to privacy and recommended promulgation of robust and comprehensive privacy laws protecting the right to privacy including data privacy.[55]

4 RTBF AS A HUMAN RIGHT UNDER THE AFRICAN HUMAN RIGHTS SYSTEM

Since the RTBF was developed under the EU laws, it is essential to investigate whether it is justiciable under the African human rights system. Unlike the EU, Africa does not have a treaty or regulatory framework specific to data protection. Nonetheless, the *Google Spain* case placed the RTBF under the umbrella of the right to privacy with respect to the processing of personal data.[56] It thus follows that an investigation into the justiciability of the RTBF under the African human rights system will require an investigation into the right to privacy and protection of personal information laws on the continent. The main human rights treaty applicable to the entire African continent is the African Charter. It established the African Commission on Human and Peoples' Rights (African Commission)[57] that is mandated to, among others, interpret and apply the African Charter and to ensure

52 Human Rights Committee General Comment 16 (32nd session, 1994), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc.HRI\GEN\1\Rev.1 at 21 (1994) (General Comment 16).

53 General Comment 16 (n 52) para 1.

54 As above.

55 UN High Commissioner for Human Rights paras 61(a)-(b).

56 *Google Spain* (n 32) paras 53 & 58.

57 African Charter on Human and Peoples' Rights art 30.

the protection of human and peoples' rights.[58] The African Commission's role to interpret and apply the African Charter is complemented by the African Court on Human and Peoples' Rights (African Court) which shares the same responsibility.[59] The parts below thus discuss the justiciability of the RTBF under the African Charter.

4.1 The right to privacy and RTBF under the African human rights system

The African Charter is a progressive human rights instrument that includes a plethora of civil-political and socio-economic rights such as the rights to dignity,[60] security of person,[61] physical and mental health[62] and education.[63] However, it fails to provide for the right to privacy, despite this right being included in several international and other regional human rights instruments adopted before it. These include article 12 of the Universal Declaration; article 8 of the European Convention on Human Rights; and article 11 of the American Convention on Human Rights. Senegalese jurist and former judge of the International Court of Justice, Kéba M'baye, who is considered the father and drafter of the African Charter,[64] had included the right to privacy in his draft charter.[65] It is however not clear why this provision was not included in the final Charter which was adopted by African states in 1981. According to Plagis and Riemer,[66] the drafting of the African Charter was influenced by several factors, including 'the prominence of the notion of sovereignty; the focus on the African nature of the Charter; the tensions between the factions that supported civil and political rights and those that supported economic, social and cultural rights; and the minimalist approach to drafting a human rights treaty'.

These factors most likely contributed to the exclusion of the right to privacy and subsequently the RTBF. More so, in the late 1970s when the African Charter was being discussed by states, privacy concerns linked to technology and the internet were not yet as prominent as they are

58 African Charter on Human and Peoples' Rights arts 46-59.

59 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights art 3(1).

60 African Charter on Human and Peoples' Rights art 5.

61 African Charter on Human and Peoples' Rights art 6.

62 African Charter on Human and Peoples' Rights art 16.

63 African Charter on Human and Peoples' Rights art 17.

64 H Sipalla 'Towards an African professional history of international law: the life and work of Kéba M'baye' in F Viljoen, H Sipalla & F Adegalu (eds) *Exploring African approaches to international law: essays in honour of Kéba M'baye* (2022) 13.

65 Y Ayalew 'Untrodden paths towards the right to privacy in the digital era under African human rights law' (2022) 12 *International Data Privacy Law* 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3993942 (accessed 6 July 2023).

66 M Plagis & L Reimer 'From context to content of human rights: the drafting history of the African Charter on Human and Peoples' Rights and the enigma of article 7' (2021) 23 *Journal of the History of International Law* 556.

today. At that time the digital world was a mere dream. For example, the World Bank only started collecting data on internet usage around 1990,[67] and some reports suggest that in 1980, a year after the African Charter was drafted in Monrovia, only 200 people were connected to a much limited version of today's internet.[68] The biggest social media platform, Facebook, was launched 25 years after the African Charter. In this context, the RTBF would have not been within the view of the drafters of the African Charter.

Nine years after the African Charter was adopted by African Heads of State and Government, they adopted the African Charter on the Rights and Welfare of the Child (African Children's Charter) that grants the right to privacy to African children. Article 10 provides as follows:[69]

> No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.

While the African Children's Charter bestows a right to privacy, which is justiciable under the African human rights system, it is only applicable to children to the exclusion of adults. Notwithstanding the African Children's Charter's efforts to entrench children's right to privacy, privacy is a fundamental right which is equally important to children as it is to adults. The *lacuna* created by the African Charter to a large extent is filled by the constitutions of most African countries that provide for the full right to privacy.[70] This includes the Constitutions of Algeria,[71] Burundi,[72] Kenya,[73] Nigeria[74] and Zimbabwe.[75] These constitutions are buttressed by African states assenting to international instruments that provide for the right to privacy, in particular ICCPR.[76] More so, the interpretation and implementation of human rights under international and regional human rights instruments is guided and directed by different organs and agencies of the UN, such as General Comments of the Human Rights Committee and reports of Special Rapporteurs.

Despite the omission of the right to privacy and ancillary data protection rights under the African Charter, the RTBF is expressly

67 https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2021&start=1960&view=chart&year=1973 (accessed 19 July 2023).

68 https://www.computerhistory.org/internethistory/1980s/ (accessed 19 July 2023).

69 Organisation of African Unity (OAU) African Charter on the Rights and Welfare of the Child, 11 July 1990.

70 A Singh & M Power 'The privacy awakening: the urgent need to harmonise the right to privacy in Africa' (2019) 3 *African Human Rights Yearbook* 202. Singh and Power point out that the constitutions of 52 out of 54 countries incorporate the right to privacy.

71 See art 47 of the Constitution of Algeria 2020.

72 See art 28 of the Constitution of Burundi 2018.

73 See art 31 of the Constitution of Kenya 2010.

74 See sec 37 of the Constitution of Nigeria 1999.

75 See sec 57 of the Constitution of Zimbabwe 2013.

76 ICCPR art 17.

recognised under the African Union Convention on Cybersecurity and Personal Data Protection 2014 (Malabo Convention).[77] Article 19 of the Malabo Convention refers the RTBF as the right to rectification or erasure and provides that '[a]ny natural person may demand that the data controller rectify, complete, update, block or erase, as the case may be, the personal data concerning him/her where such data are inaccurate, incomplete, equivocal or out of date, or use collection, use, disclosure or storage are prohibited'.

Although the Malabo Convention recognises the RTBF under article 19, it is not a binding and enforceable treat. This is because the Convention aims at harmonising cybersecurity and personal data protection legislation among AU member states and not to guarantee a human right upon a group of people.[78] More so, the prospects of states implementing the Malabo Convention are low as it has taken nine years for only 15 states to ratify it. As such, it only came into effect on 8 June 2023.[79]

Further, the Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted by the African Commission on 10 November 2019 in The Gambia (Gambia Declaration) recognises every person's right to exercise autonomy in relation to their personal information.[80] Even though the Gambia Declaration was adopted in response to the developments of the internet age,[81] it does not expressly recognise an individual's RTBF. Instead, under principle 39(3), the Declaration provides that states shall impose on internet intermediaries the duty to mainstream human rights safeguards into their processes of filtering online content and ensuring transparency on all requests of the removal of content. Principle 39(4) further outlined circumstances under which it would be acceptable for states to require the removal of online content by internet intermediaries. A closer look at Principle 39 of the Gambia Declaration, it appears that it is not meant to buttress an individual's RTBF but rather to reinforce that states should not arbitrarily interfere with the individuals' right to access information online. However, principle 40(1) of the Gambia Declaration acknowledges every individual's right to privacy and protection of personal information and Principle 42(4) the right to exercise autonomy in relation to their personal information under which the RTBF may be inferred.

It follows that the *lex imperfecta* within the African Charter persists as the RTBF can only be read into the right to privacy provisions in different international instruments and the Malabo Convention, but the latter is only ratified by a few countries. The following parts show

77 Amnesty International *Malabo Protocol: legal and institutional implications of the merged and expanded African Court*, 22 January 2016 (Malabo Convention) art 19.

78 Malabo Convention, Preamble.

79 https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281 (accessed 20 July 2023).

80 African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information (2019), Introduction.

81 As above.

how this *lex imperfecta* can be rectified through the reading of the RTBF into the African Charter through three methods.

4.2 Recognising the right to be forgotten under the *SERAC* principle

The RTBF may be justiciable under the African Charter by invoking the *SERAC* principle set in the African Commission's decision in *Social and Economic Rights Action Centre & Another v Nigeria* (*SERAC*).[82] The brief facts of the communication were that the military government of Nigeria had been directly involved in oil production through the state oil company, the Nigerian National Petroleum Company, the majority shareholder in a consortium with Shell Petroleum Development Corporation, and that these operations had caused environmental degradation and health problems resulting from the contamination of the environment among the Ogoni people. It was alleged that the oil consortium had disregarded the health or environment of local communities by dumping toxic waste into the environment and local waterways. It was further alleged that the Nigerian government had condoned the degradation by failing to take measures to protect the health and environment of the Ogoni people. Further, Nigerian security forces attacked Ogoni villages following lawful protests to the degradation of the health and environment, by the Ogoni people.

SERAC thus alleged that the Nigerian government's conduct violated, among others, the right to housing or shelter, and the right to food. Both these rights are not explicitly provided for under the African Charter. SERAC alleged that the right to housing or shelter is implicitly recognised by the African Charter as it could be read into article 14 (the right to property), article 16 (the right to physical and mental health), and article 18(1) (the right to family). The African Commission agreed with SERAC's assertions and held that:[83]

> Although the right to housing or shelter is not explicitly provided for under the African Charter, the corollary of the combination of the provisions protecting the right to enjoy the best attainable state of mental and physical health, cited under Article 16 above, the right to property, and the protection accorded to the family forbids the wanton destruction of shelter because when housing is destroyed, property, health, and family life are adversely affected. It is thus noted that the combined effect of Articles 14, 16 and 18(1) reads into the Charter a right to shelter or housing which the Nigerian Government has apparently violated.

SERAC further argued that the right to food is implicitly recognised under the African Charter as it could be read into article 4 (the right to life), article 16 (the right to physical and mental health), and article 22 (the right to economic, social and cultural development). The African Commission decided in SERAC's favour as it found that the right to food was inseparably linked to human dignity. The Commission held:[84]

82 *Social and Economic Rights Action Centre (SERAC) & Another v Nigeria* (2001) AHRLR 60 (ACHPR 2001) (*SERAC*).

83 *SERAC* (n 82) para 60.

84 *SERAC* (n 82) para 65.

> The right to food is inseparably linked to the dignity of human beings and is therefore essential for the enjoyment and fulfilment of such other rights as health, education, work and political participation. The African Charter and international law require and bind Nigeria to protect and improve existing food sources and to ensure access to adequate food for all citizens.

It therefore follows that a human right can be implicitly read into the African Charter if a violation of that right is tantamount to a violation of a combination of rights explicitly provided under the African Charter. In so far as the RTBF is concerned, we submit that it is inextricably linked to some of the rights expressly provided by the African Charter, which includes article 5 (right to dignity), article 9 (freedom of information and expression), article 10 (freedom of association), article 16 (right to physical and mental health), and article 22 (right to economic, social and cultural development).

The RTBF is premised on erasing or rectifying information that moulds public perception about people – thus its main focus is on the dignity and honour of a person. The right to dignity is an important right within the global human rights system. According to the Court in *Mugesera v Rwanda*[85] (*Mugesera* case) the purpose of protecting human rights is to preserve human dignity. Regarding a violation of article 5 of the African Charter in particular, the Court agreed with the Commission's view that it 'can be interpreted as extending to the broadest possible protection against abuse, whether physical or mental'.[86] In *International Pen v Nigeria* it was held that 'the prohibition in article 5 included not only actions which cause serious physical or psychological suffering, but also actions which humiliate the individual or force him or her to act against his will or conscience'.[87]

In considering whether the right to dignity protected in article 5 of the African Charter has been violated, the Court held that it considers that 'the cruelty or inhumanity of the treatment must involve a certain degree of physical or mental suffering on the part of the person, which depends on the duration of the treatment, the physical or psychological effects of the treatment, the sex, age and state of health of the person. All this must be analysed on a case-by-case basis.'[88]

The jurisprudence of the African Commission and African Court indicates that where a data processor or controller refuses to erase or rectify personal information which causes physical or mental suffering on a person it may be in violation of articles 5 and 16 of the African Charter. Take, for example, a newspaper article published on the internet that reveals the name and home address of an alleged fraudster. Even if such a person were to be acquitted by a competent court the newspaper article will remain on the internet available to readers forever. A simple search of the acquitted person's name will likely reveal the article containing allegations of fraudulent activities

85 *Mugesera v Rwanda* (judgment) (2020) 4 AfCLR 834 (*Mugesera*).

86 *Mugesera* (n 85) para 80.

87 *International Pen & Others (on behalf of Saro-Wiwa) v Nigeria* (2000) AHRLR 212 (ACHPR 1998), cited in *Zimbabwean Human Rights NGO Forum v Zimbabwe* (2006) AHRLR 128 (ACHPR 2006).

88 *Mugesera* (n 85) para 81.

thus imputing a reputation of criminal behaviour on the acquitted person. This in turn will cause serious mental suffering on the acquitted person as inaccurate information about them is available for the entire world to see. If their personal information is not erased, particularly their home address, this will likely lead to retribution from victims of the alleged fraud who may assume that the acquitted person 'got away with it'.

Article 9(1) of the African Charter provides that every individual shall have the right to receive information. Data processors protect and promote this right by providing information via the internet. However, it would undermine the purpose of granting a right to receive information if an individual was to receive inaccurate information or information that violates the dignity and honour of another. Furthermore, article 9(2) provides the right to freedom of expression. The African Court has on several instances held that the right to freedom of expression is fundamental to human development as it is the vehicle in which humans exchange opinions.[89] Information that is inaccurate or perpetuates the violation of human dignity cannot foster accurate or humane opinions. Subsequently, human development is undermined meaning that the right to freedom of expression would fail to achieve the purpose for its inclusion in the African Charter. More so, the right to freedom of expression is intrinsically linked to the right to freedom of association protected under article 10 of the African Charter. As such, a violation of article 9 can surmount to a violation of article 10 of the African Charter.[90]

Under article 22 of the African Charter all people have a right to their economic, social, and cultural development which is rooted in their freedom and identity. Jurisprudence on the African Charter shows that where a person is disrupted from participating in their own economic, social and cultural development such conduct may constitute a violation of article 22.[91] It thus follows that when information available on the internet disrupts a person from participating in activities that bring about their economic, social or cultural development it may violate article 22. Human rights are interdependent and the number of rights under the African Charter that may possibly be violated by violating the RTBF cannot be exhausted in this article. Needless to say, it is important that the RTBF is proportionally protected, and this should be done within the confines of the law. Generally, this ought to be within boundaries granting the

89 See *Ajavon v Benin* (2020) 4 AfCLR 133; *Umuhoza v Rwanda* (Merits) (2017) 2 AfCLR 165; *Zimbabwean Human Rights NGO Forum v Zimbabwe* (2006) AHRLR 128 (ACHPR 2006).

90 *Zimbabwean Human Rights NGO Forum* (n 89).

91 See *African Commission on Human and Peoples' Rights v Kenya* (Merits) (2017) 2 AfCLR 9; *XYZ v Benin* (Judgment) (2020) 4 AfCLR 83; *Good v Botswana* (2010) AHRLR 43 (ACHPR 2010); African Commission on Human and Peoples' Rights Principles and Guidelines on the Implementation of Economic, Social and Cultural Rights in the African Charter on Human and Peoples' Rights adopted in November 2010 at the 48th ordinary session.

erasure or rectification of information available on the internet that is incorrect, inaccurate, outdated or perpetuates the violation of human dignity and honour.

4.3 Recognising the right to be forgotten under the progressive application principle

Articles 60 and 61 of the African Charter provide flexibility in interpreting and applying human rights by the African Commission and the African Court when called upon to do so. Both articles enable the Commission and the Court to draw inspiration from international human rights law when interpreting, applying or developing human rights under the African Charter. Article 60 of the African Charter essentially affords the Commission and the Court by extension the liberty to draw motivation from various instruments on human and peoples' rights, including the Universal Declaration, UN instruments and other human rights instruments adopted by African countries such as those adopted by the regional economic communities (RECs).

Article 61 of the African Charter supplements the provisions of article 60 as it allows the African Commission and the African Court to consider – when called upon to do so – the applicable rules laid down by other general and international conventions recognised by AU member states, general African practices aligned to international norms on human rights, customary law, general principles of law recognised by African states and judicial precedents.

The purpose of including the above provisions in the African Charter is to provide the Court and the Commission in its general role of promoting human and peoples' rights with a source for contemporary human rights standards whenever the African Charter does not contain applicable human rights provisions.[92] In *Good v Botswana* it was held that the African Charter must be interpreted in light of international norms and consistently with the approach of the other regional and international human rights bodies.[93] The Court has on several occasions borrowed from different international instruments and other regional human rights courts or forums. It has frequently referred to judgements of the ECJ.[94] In the context of RTBF, this means that the Court can cure the *lex imperfecta* created by the African Charter by referring to the jurisprudence of the ECJ on the RTBF in its advisory opinions when called upon to do so, particularly the *Google Spain* case discussed above. More so, while the Convention on Data Protection 1981, which was succeeded by the GDPR, is a European treaty, five African countries have signed the treaty, namely,

92 R Murray *The African Charter on Human and Peoples' Rights: a commentary* (2019) 782.

93 *Good v Botswana* (n 91) para 113.

94 See *William v Tanzania* (Merits) (2018) 2 AfCLR 426; *Kambole v Tanzania* (Judgment) (2020) 4 AfCLR 460; *Bissangou v Republic of Congo* (2006) AHRLR 80 (ACHPR 2006) 74.

Cabo Verde, Mauritius, Morocco, Senegal and Tunisia.[95] Burkina Faso has also requested to accede to the treaty.[96] Over and above the Malabo Convention and the Gambia Declaration, this shows that African states and the African Union are recognising the need for a regulated autonomy over personal data on the internet.

4.4 Adopting the RTBF under the Vienna Convention

Whenever an international court or other international dispute settlement body has to interpret and apply an international treaty it must do so in terms of the Vienna Convention on the Law of Treaties (VCLT). The VCLT has played a critical role in assisting the Commission and later the Court in the interpretation and application of the African Charter. In its deliberations the African Court has on several instances adopted and adhered to article 31 of the VCLT,[97] which requires a holistic approach to interpreting and applying treaty provisions. Article 31 of the VCLT provides for contextual interpretation of the treaty considering its objects and purpose.[98] Article 31 of the VCLT further provides that together with the context of the treaty, the relevant rules of international law applicable between the parties' relations and subsequent agreement and practice in the interpretation and application of the treaty shall be taken into account.[99]

As far as locating the RTBF under the African Charter is concerned, this means that the African Charter must be interpreted holistically as an instrument which aims to, as enunciated in its preamble, promote and protect human rights in Africa and that such rights are not limited to those contained in the African Charter only. The approach of the Commission in the *SERAC* case shows that the African Charter is not the beginning and end of all human rights in Africa. More so, where some human rights provisions are non-existent in the African Charter they can be drawn from the subsequent agreements or actions of the parties to the African Charter. The International Law Commission's Draft Conclusions on Subsequent Agreements and Subsequent Practice in Relation to The Interpretation of Treaties 2018 (Draft Conclusions) provide for an expanded meaning to subsequent agreements and practices.[100] The Draft Conclusions extend the meaning to include external and internal acts of parties to the treaties. This includes legislative acts, executive acts, judicial acts, official acts, voting in

95 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (accessed 25 July 2023).

96 http://rm.coe.int/doc/0900001680700194 (accessed 25 July 2023).

97 See Request for Advisory Opinion by the Socio-Economic Rights and Accountability Project (Advisory Opinion) (2017) 2 AfCLR 572; *Mkandawire v Malawi* (review and interpretation) (2014) 1 AfCLR 299; *Good v Botswana* (n 91) para 113.

98 Vienna Convention on the Law of Treaties 1969 (VCLT) art 31(1).

99 VCLT art 33(3).

100 These draft conclusions are binding on the Court in terms of art 61 of the African Charter.

international organisations and pronouncements of expert treaty bodies. In this context, the Malabo Convention and the Gambia Declaration are prime examples of a subsequent agreement and practice advocating for the RTBF and personal data autonomy to be applied and recognised in Africa.

Moreover, different legislative efforts show that the RTBF is being adopted in African states. Data protection legislations in Ghana,[101] Kenya,[102] Nigeria,[103] South Africa[104] and Zimbabwe[105] show that African states are adopting the RTBF as part and parcel of their domestic law. However, there is no universal approach to the inclusion of the right.

4.5 Challenges to enforcing RTBF

Although the RTBF possibly is justiciable through inference from the privacy provisions under the above-highlighted treaties and conventions, the fact that the right is not expressly recognised exposes it to some implementation barriers. The inference of the right from the inter-linked rights deprives individuals, the domestic courts and the African Commission of the broader understanding of the scope and limitations of the RTBF. With the exception of the Malabo Convention, all other instruments under which the RTBF may be inferred do not outline the nature of personal data that can be erased and/or the circumstances of removal. In terms of article 19 of the Malabo Convention, for the RTBF to be enforced, the personal data must be 'inaccurate, incomplete, equivocal or out of date, or [its] use collection, use, disclosure or storage are prohibited'.[106] However, some concepts such as 'equivocal or out of date' are not universally defined nor is there any established precedent on what constitutes equivocal or out of date data. This quandary becomes more apparent when removal or erasure concerns newspaper articles, considering that newspapers also serve as archives of historical data on past events for research and statistical purposes.[107] Thus, it is difficult to draw a line on when newspaper articles are considered out of date.

101 See the Data Protection Act 2012 (Act 843) sec 44.

102 See the Data Protection Act 24 of 2019 (Act 843) sec 40.

103 See Nigeria Data Protection Act 2023 sec 34(1)(a)(v).

104 See Protection of Personal Information Act 4 of 2013 sec 18(1)(h)(iii).

105 See Data Protection Act 5 of 2021 sec 13(f).

106 Malabo Convention art 19.

107 FU Ahmed 'Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm' (2015) 21(6) *Computer and Telecommunications Law Review* 175, 182. See also R Franzosi 'The press as a source of socio-historical data: issues in the methodology of data collection from newspapers' (1987) 20(1) *Historical Methods: A Journal of Quantitative and Interdisciplinary History* 5.

Moreover, the absence of a clearly defined scope and limitations of RTBF sets it up for a clash with other established rights such as the right to freedom and expression on the internet and access to information.[108] The enforcement of the RTBF without guiding parameters can potentially have negative repercussions on free speech on the internet as it may lead to removal of necessary and important public interest information. For example, Google previously acknowledged to have erroneously removed links to some newspaper articles by the *Guardian* newspaper.[109] Thus, reading the RTBF in the African Charter without giving it content and guarding it against malpractice, renders it susceptible to abuse.

Another challenge to the implementation of the RTBF in Africa is the jurisdictional issue. Notwithstanding that some African states have adopted national laws expressly providing for the RTBF, its enforcement remains a challenge considering the borderless nature of the internet and the fact that corporations that control personal data on the internet such as Google have no offices in most African countries.[110] Thus, should corporations that control personal data refuse to honour the request to remove links to personal data, individuals in most African countries cannot enforce the right in their municipal courts due to jurisdiction barriers unless those corporations agree to submit to domestic jurisdiction. In the matter of *X v Privacy Commissioner of Personal Data*[111] the Hong Kong Administrative Appeals Board (AAB) was, among others, tasked with determining the territorial boundary of Hong Kong's Personal Data (Privacy) Ordinance (PDPO) within the context of the RTBF. The AAB upheld the decision of the Privacy Commissioner that the territorial jurisdiction of the PDPO is only limited to the data controllers operating or situated in Hong Kong. In this instance, the data controller was Google LLC and was operating from the United States of America and not in Hong Kong, hence it had no obligation to remove online content in Hong Kong on the sole ground of RTBF.[112] Given that data-controlling corporations operate outside of most African countries, most subjects of personal data in Africa may run in the same predicament as the data subjects in Hong Kong. However, data subjects can still enforce the RTBF in national courts as precedent in Latin America shows that in most cases data controlling corporations easily submit to the national jurisdictions.[113]

108 M Fazlioglu 'Forget me not: the clash of the right to be forgotten and freedom of expression on the internet' (2013) *3*(3) *International Data Privacy Law* 149, 153.

109 J Ball 'Google admits to errors over Guardian "right to be forgotten" link deletions' *The Guardian* (2014), http://www.theguardian.com/technology/2014/jul/10/google-admits-errors-guardian-right-to-be-forgotten-deletions (accessed 17 September 2023).

110 Eg, Google has only one office in the entire Africa situated in Johannesburg, South Africa.

111 *X v Privacy Commissioner of Personal Data* (Appeal 15/2019) (*Privacy Commissioner* case).

112 *Privacy Commissioner* case (n 111) para 57.

113 See *DCV v Yahoo de Argentina SRL y otro s/ Daños y Perjuicios*, (National Civil Appeals Chamber) 10 August 2010; *Peña Maria Florencia v Google s/Art. 250 CPC Incidente* Civil (National First Instance Civil Court 72) file 35.613/2013;

Notwithstanding the above challenges, the regulated RTBF is essential in the digital age to counter the damning impact of perpetual storage of data on the right to self-autonomy over personal information and susceptibility to misuse and misinterpretation.[114] Currently, the RTBF under the right of privacy or as a stand-alone right is recognised in a fragmented manner across the African human rights system, hence inadequately protected. The recognition of the RTBF by reading it into the African Charter is essential as it would create a pathway for robust law reforms related to the protection and autonomy over personal data in Africa's national jurisdictions.[115] As Singh and Power advanced, the prevalence of the African Charter in the African human rights system rendered it 'both a binding and persuasive advocacy tool'.[116] The superior status the African Charter enjoys in the African human rights system justifies the need for the RTBF to be recognised as part and parcel of the Charter to ensure adequate protection. The recognition of the RTBF under the Charter will further enable the African Commission to carry out its general role of promoting human and peoples' rights by providing soft law guidance to the realisation of the RTBF through declarations and model laws.

5 CONCLUSION

The times and technology are constantly evolving and raising new issues that human beings had not previously contemplated. Just as they are evolving, so must the human rights landscape, particularly in Africa where the significant majority is the youth. The preceding discussion shows how the African Charter is lagging behind technological advancement by not recognising privacy rights, let alone the RTBF. Millions of Africans exchange personal data over the internet daily, thereby placing themselves in a situation where their personal data will adversely affect their dignity in the near future but without legal recourse. It is sacrosanct that the RTBF be promoted and protected under the African human rights system. The justiciability of the RTBF under the African Charter bolsters the protection and reinforcement of several human rights in the African Charter, particularly the right to dignity as the RTBF is interlinked to multifarious other rights.

The article shows that the RTBF is not an abstract idea but a real-world phenomenon that has been justiciable in Europe for nearly a decade. African human rights practitioners can take a leaf from the EU jurisprudence in developing and adapting the RTBF to the African context. However, a fully-developed RTBF must not grant an unfettered right to rectify or erase personal information in the public domain but be a right exercised within certain legal limits in order to establish an equilibrium with competing rights such as the right to

Da Cunha, Virginia v Yahoo de Argentina SRLY otro s/ daños y perjuicios (National Supreme Court of Justice) 30 December 2014.

114 See para 1 above.

115 Singh & Power (n 75) 219.

116 As above.

freedom of expression and access to information. Further research still needs to be carried out to see what such limits to the right can be in Africa. For example, unlike in the EU, the African Charter in chapter 2 requires that any rights be exercised with due regard to the duties an individual owes to society. This is an area that still needs to be explored. Nonetheless, the right can at present be realised under the African Charter through applying the *SERAC* principle, progressive application principle under articles 60 and 61, and adopting a holistic approach to the interpretation of the African Charter. The adoption of the RTBF under domestic legislation in different African jurisdictions shows that different states recognise the need to respond to the evolution of the online landscape and grant citizens autonomy over the availability of their personal information within the public domain and particularly, the online world.