UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

# The Concept of the 'Right to Be Forgotten', 'Right to Delete', 'Right to Erasure' In the Digital Age.

By

Mamoneuwa Maduna

(28202407)

Submitted in partial fulfilment of the requirements for the degree LLM Mercantile Law

In the

FACULTY OF LAW

At the

UNIVERSITY OF PRETORIA

Research Supervisor:

Prof. Sylvia Papadopoulos

Date of submission

May 2022

University of Pretoria

## PLAGIARISM POLICY

The University of Pretoria places great emphasis upon integrity and ethical conduct in the preparation of all written work submitted for academic evaluation.

While academic staff teaches you about referencing techniques and how to avoid plagiarism, you too have a responsibility in this regard. If you are at any stage uncertain as to what is required, you should speak to your lecturer before any written work is submitted.

You are guilty of plagiarism if you copy something from another author's work (e.g. a book, an article or a website) without acknowledging the source and pass it off as your own. In effect, you are stealing something that belongs to someone else. This is not only the case when you copy work word-for-word (verbatim), but also when you submit someone else's work in a slightly altered form (paraphrase) or use a line of argument without acknowledging it. You are not allowed to use work previously produced by another student. You are also not allowed to let anybody copy your work with the intention of passing if off as his/her work.

Students who commit plagiarism will not be given any credit for plagiarised work. The matter may also be referred to the Disciplinary Committee (Students) for a ruling. Plagiarism is regarded as a serious contravention of the University's rules and can lead to expulsion from the University.
The declaration which follows must accompany all written work submitted while you are a student of the University of Pretoria. No written work will be accepted unless the declaration has been completed and attached.

Full names of candidate: Mamoneuwa Maduna

Student number: 28202407

Date: 22 April 2022

## DECLARATION

1. I understand what plagiarism is and am aware of the University's policy in this regard.

Signature of candidate: .....…….

Signature of supervisor: ... ……

This document must be signed and submitted to the Head: Student Administration within two months of registering for the research component of the programme.

## EXECUTIVE SUMMARY

The recognition of the right to privacy has evolved greatly in the digital era where technological advancements have led to an increased scale of processing activities, cross border transfers, easy access to information and the development of the digital economy. Due to these developments, information has become easily accessible and retainable. The "right to erasure or delete" emanated from the ideal that persons should have a right to decide what information is processed and maintain control over their information.

In 2014, the Court of Justice of the European Union (CJEU) held for the first time that persons have a "right to be forgotten" in its judgement of *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*. Prior to this judgement, the "right to erasure" was recognised where personal information was irrelevant, excessive, outdated or the processing was unlawful. While the South African Protection of Personal Information Act 4 of 2013 (POPIA), does not expressly provide for a "right to be forgotten'", it does provide for the "right to delete" with requirements substantially similar to the "right to be forgotten or erasure" under European data protection legislation.

There are fundamental challenges identified in the paper regarding the implementation of this right, including the lack of interpretation from a technical perspective which will ultimately influence how successful it becomes in practice, the impact it has on other existing rights such as the right to freedom of expression, the right to access to information and how this balance will be achieved by entities who are obligated to fulfil these requests.

The paper further provides recommendations for South Africa to navigate the challenges and close the gap that currently exist in the exercise of the right to delete. Recommendations include the definition of a standard by the Information Regulator on what constitute the right to delete, journalistic, literary and artistic purposes as well as public interest. It also recommends more intrusive oversight by the Information Regulator on the entities that must fulfil this requirement. This is to ensure the correct balance is applied by responsible parties required to balance private and public interests.

# TABLE OF CONTENTS

# CHAPTER 1: INTRODUCTION

## 1.1 Background

The "right to be forgotten" or "right to erasure" gained much popularity and provoked debates across different spheres, legal, technology, social and the media fraternity alike since the judgement in the *Google Spain* case.[1] The idea of the "right to be forgotten" or "erasure" emanates from the fact that persons should have a choice, and determine who, how, when and the extent to which their personal information is disclosed to others and processed.[2] While the right may have found its origins in Europe, it has become one of the fundamental data subject rights across different jurisdictions, many referring to this right as the "right to delete" or "right to erasure".[3] This right exists as part of ensuring that the privacy of persons is respected, protected and persons have control over the processing of their personal information.[4]

This basic concept of control that has been conferred on persons has become the cornerstone of informational privacy in the digital era where there is a large scale of

---

1 *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*, Case C-131/12, Court of Justice of the European Union (CJEU).

2 Rolf HW "The Right to Be Forgotten: More Than a Pandora's Box?" (2011) 2 *Journal of Intellectual Property Information Technology and Electronic Commerce Law* 120.

3 The term 'data subject' is defined as *any person to whom the personal information belongs or relates in terms of* s1 of the Protection of Personal Information Act 4 of 2013 (hereafter POPIA). A person can be either a natural or juristic person in terms of POPIA. In contrast, the Regulation 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 (hereafter General Data Protection Regulation or GDPR), defines a person as a *natural living person*, and therefore their definition excludes juristic person, and their privacy law affords protection to individuals only.

4 See Organisation for Economic Co-operation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) [C (80)58/FINAL, as amended on 11 July 2013 (hereafter OECD Privacy Guidelines).

processing by a multitude of different parties.[5] This right is even more relevant in the digital space where people leave traces of themselves that permeates more places than we could ever imagine, and there are multitude of ways information can be collected and processed.[6] Studies show that in 2014 there were only 2.4 billion internet users, and the number had increased to over 4.4 billion in 2019 signifying an increase of 83% in just 5 years.[7] This staggering number reflects how widespread and overreaching the internet is in this era, and how quickly information can spread.

The value of personal information and the role it plays in making effective decisions cannot be underestimated.[8] The advancement of technology and data mining techniques has led to a breakthrough in understanding behaviours and preferences, even enabling the prediction of future events through predictive and prescriptive analytics.[9] It has also transformed society into an information society in which information has become core to the everyday life.[10] This enables organisations to develop targeted products and improve

---

5 *Id* 19.

6 *Id* 20.

7 Schultz J 'How Much Data is Created on the Internet Each Day?' June 2019 https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/ (accessed on 20 September 2020).

8 Harvard School Business Online 'The advantages of data-driven decision-making' 26 August 2019. https://online.hbs.edu/blog/post/data-driven-decision-making (accessed on 20 September 2020). The article defines what data driven decisions are, and how they are important in informing a course of action before making any commitments. The author of the article makes a comparison between decisions based on gut and feeling, and concludes that data driven decisions are more logical, concrete and are based on facts.

9 OHIO University 'Difference between Predictive and Prescriptive Analytics' Accessed on https://onlinemasters.ohio.edu/blog/predictive-vs-prescriptive-analytics-whats-the-difference/ (accessed on 17 August 2020). Predictive analytics 'forecast what might happen in future looking at current information and patterns. Prescriptive analytics is advanced predictive analytics and suggests a range of prescribed actions and the potential outcomes of each action'.

10 Papadopoulos S and Snail S *Cyberlaw@SA III: The Law of the Internet in South Africa* (2012) 1.

services they provide to data subjects.[11] Inherently, this advancement[12], in how personal information is processed has introduced some risks, one being the storage of large information in multiple platforms. This ability of computers and systems to store large amounts of information for long periods of time and sometimes even indefinitely has often been described as the main contributor to loss of power and control, which the "right to be forgotten, erasure or delete" seeks to revive.[13]

## 1.2 The South African Position

### *1.2.1 Evolution of Data Privacy*

The right to privacy in South Africa evolved from the common law, which recognised the right to privacy as an independent personality right.[14] A personality interest is a non-patrimonial interest that cannot exist separately from the individual.[15] In South Africa, the right to privacy is protected in terms of both the common law[16] which is informed by our *boni mores* and the Constitution (the Constitution of the Republic of South Africa, 1996, hereafter referred to as the Constitution).[17]

---

11 The free dictionary defines data mining as *the extraction of useful, often previously unknown information from large databases or data set,* https://www.thefreedictionary.com/Information-mining (accessed on 20 August 2020).

12 DP Van der Merwe, A Roos, S Eiselen and S Nel (2016) *Information and Communications Technology Law* 2nd Edition LexisNexis: South Africa, 366.

13 Graux H, Ausloos J and Valcke P "The Right to be Forgotten in the Internet Era" (2012) 11 *Interdisciplinary Centre for Law and ICT*. Also see Van der Merwe et al *Information and Communications Technology* Law 367.

14 *Bernstein v Bester* 1996 2 SA 751 (CC) par 68.

15 Neethling J "Personality Rights: A Comparative Overview" (2005) 38 *Comparative and International Law Journal of Southern Africa* 210.

16 The *locus classicus* for the recognition of an independent right to privacy is the case of *Argus Printing and Publishing Company Ltd. and Others v Esselen Estate* (447/92) [1993] ZASCA 205; 1994 (2) SA 1 (AD); [1994] 2 All SA 160 (A) (7 December 1993).

17 S14 Constitution 108 of 1996 clearly outlines that:

A few years after the enactment of the Constitution, the South African Law Reform Commission (SALRC) approved an investigation into the regulation of privacy and data protection and the possible enactment of a data protection legislation.[18] The rationale behind this investigation was based on the fact that while the right to privacy was protected by both common law and the Constitution of South Africa, the advancement of technology had revolutionised the manner in which information was being processed, resulting in cross-border processing of information and the ability of technologies to store large amounts of information. This in turn resulted in the abuse and manipulation of information.[19]

Another motivation raised by the SALRC was the fact that the common law right to privacy and the Constitution did not in any way deal with other aspects of the right to privacy, such as the balance to be sought between the right to privacy and right of private and public entities in processing information for business purposes or to fulfil legal mandate provided in terms of statute, and the extent of the control that individuals have with regards to their personal information.[20] The resultant legislation, the Protection of Personal Information Act (POPIA or POPI Act), was passed into law in 2013, and became fully effective from 1 July 2020 with the objective to give effect to the right to privacy as

---

"Everyone has the right to privacy, which includes the right not to have:
(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed."

18 The South African Law Reform Commission *Discussion Paper 109 Project 124 Privacy and Data Protection* October (2005) available at https://www.justice.gov.za/salrc/dpapers/dp109.pdf (accessed on 17 August 2020).

19 *Id* 5.

20 *Id* 6.

entrenched in the Constitution, govern the processing of personal information and uphold the rights of data subjects.[21]

POPIA has been described as South Africa's "…first comprehensive data protection legislation",[22] which aims to regulate the processing of personal information by private and public entities in a manner which is consistent with international standards.[23] The Act does this by drawing from internationally accepted data protection principles in order to establish a set of minimum requirements necessary to process personal information in South Africa.[24] A selected number of sections of POPIA commenced in April 2014,[25] and thereafter the office of the Information Regulator was established in December 2016. The objective of this law is to regulate the processing of personal information and provide for recourse where personal information has been processed in contravention of POPIA. [26]This new protection afforded through POPIA will be governed and enforced through an administrative body – the Information Regulator.[27]

---

21 Proclamation No R. 21 OF 2020 Protection of Personal Information Act (4/2013): Commencement of certain Sections of the Protection of Personal Information (Act 4 of 2013).

22 Hamann and Papadopoulos "Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa" 2014 *De Jure* 42 62 at 55.

23 Preamble and s2(b) POPIA; Roos in van der Merwe *et al* (2016) 434-435; Papadopoulos in van Eeden and Barnard (2018) 567-568.

24 Preamble and s2(b) POPIA; Papadopoulos in van Eeden and Barnard (2018) 567-568.

25 On 11 April 2014, the following sections of the Act came into effect: s1 containing the definitions; Part A of Chapter 5 relating to the establishment of the Information Regulator; s112 which empowers the issuing of Ministerial regulations; and s113 which prescribes the procedure for issuing regulations.

26 Van der Merwe et al *Information and Communications Technology* Law 368.

27 DP van der Merwe "A Comparative Overview of The (Sometimes Uneasy) Relationship Between Digital Information And Certain Legal Fields in South Africa and Uganda" (2014) 17 Potchefstroom Electronic Law Journal (PELJ) 1, page 304.

The Presidency announced on the 22nd of June 2020 that the heart of the POPIA, provisions would take effect from the 1st of July 2020.[28] The Act was signed into law in December 2013, but over the past 7 years, only a few parts of it have been implemented, such as establishing the office of the Information Regulator of South Africa.[29]

Under section 115 of the POPIA the President announced that (a) 1 July 2020 is the date on which: (i) sections 2 to 38; (ii) sections 55 to 109; (iii) section 111; and (iv) section 114(1), (2) and (3); and (b) will commence and that 30 June 2021 is the date on which sections 110 and 114(4), of the said Act become effective.[30] Section 114(1) is of particular importance as it states that all forms of processing of personal information must, within one year after the commencement of the section, be made to conform to the Act. This means that entities (both in the form of private and public bodies) must ensure compliance with the Act by 1 July 2021. The reason for the delay in relation to the commencement of sections 110 and 114(4), which commenced on 30 June 2021, is that these sections pertained to the amendment of laws and the effective transfer of functions of PAIA from the South African Human Rights Commission to the Information Regulator.[31]

---

28 See *Commencement of certain sections of the Protection of Personal Information Act, 2013* (22-06-2020) available at http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 (accessed 01-07-2020).

29 Proclamation No. R. 25 of 2014 *Commencement of Section 1, Part A of Chapter 5 and Sections 112 and 113 of The Protection Of Personal Information Act, 2013* (Act No. 4 of 2013) (Government Gazette 37544), 11 April 2014. See also https://www.justice.gov.za/inforeg/index.html for the Information Regulators activities (accessed 01-07-2020).

30 Proclamation No. R. 21 of 2020 *Commencement of Certain Sections of the Protection of Personal Information Act, 2013* (Act No. 4 of 2013) (Government Gazette 43461), 22 June 2020.

31 See *Commencement of certain sections of the Protection of Personal Information Act, 2013* (22-06-2020) available at http://www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 (accessed 01-07-2020).

### 1.2.2 *POPIA Explained*

POPIA applies to the processing of personal information by a responsible party[32] that has been entered into a record irrespective of whether the processing is automated or non-automated, for example, system based or manual processing.[33] The Act does not restrict application to responsible parties domiciled in South Africa, but also extends its application to responsible parties that are domiciled outside of South Africa who uses means (automated or non-automated) to process in South Africa.[34]

The processing of personal information by responsible parties must adhere to a set of minimum requirements (also known as lawful conditions) for the processing of personal information. The lawful conditions are briefly explained below to provide context to the foundational principles of POPIA. The scope of this paper does not include a detailed analysis of all lawful conditions of processing personal information. The focus of the paper will be on the analysis and interpretation of the right to delete which is encapsulated under the lawful condition of "Data Subject Participation" discussed below in section 1.2.2 (h).

a) *Accountability*

   The responsible party must ensure the requirements of the Act are met and complied with at the outset and during the lifecycle of personal information processing.[35] The responsible party is ultimately responsible and liable for ensuring that personal information is processed lawfully and remains accountable to the processing of personal information by its third parties. One of the accountability measures defined in the Act is to ensure that there is a dedicated individual in an organisation with the responsibility of ensuring compliance to the

---

32 S1 "Responsible party" is defined as "A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information."

33 S3(1)(a) POPIA.

34 S3(1)(b).

35 S8.

Act, referred to as the Information Officer. On 1 April 2021, the Information Regulator published the Guidelines for Information Officers and Deputy Information Officers to provide further guidance on the measures that must be implemented to ensure compliance[36], which measures include the encouragement of compliance by a responsible party, dealing with requests from data subjects, development and maintenance of a compliance framework and conducting of privacy impact assessment to identify risks to the processing of personal information.

b) *Processing limitation*

Personal information must be processed lawfully without infringing on the rights of persons. Excessive processing must be avoided, and only necessary, relevant and adequate information must be processed in line with the purposes defined ('principle of minimality'). The principle of minimality is premised on the basis that personal information must be closely linked to the purpose of processing.

Additionally, the Act requires that personal information must be collected directly from the data subject, unless under exceptional circumstances outlined in the Act.[37] Elizabeth de Stadler raises a much-debated view on the collection of personal information readily available on the internet and shares a view that the requirement to collect personal information directly from the data subject does not apply where information has been made public by the data subject, however, care must be taken with information on the internet due to the possibility that a data subject may have not intended for their information to be in the internet in the first instance.[38] Ultimately, the fact that information is collected publicly does not exonerate any responsible party from complying with the rest of the requirements

---

36 Guidance Note on Information Officers and Deputy Information Officers, 1 April 2021

37 S11 and 12.

38 E de Stadler *et al A Guide to the Protection of Personal Information Act* (2015) Juta 24.

from the Act, they would still have to comply with the other lawful conditions of processing.

c) *Purpose specification*

Personal information must be collected for a specific purpose and must not be kept longer than is necessary for the specified purpose.[39] Whilst a responsible party may have a purpose for collecting personal information, the purpose in itself must be lawful and justified. Failure to ensure that the purpose for collection is explicitly defined impacts on the other lawful conditions, for example, (i) a responsible party is only able to determine if processing is lawful through a defined purpose, (ii) the requirement regarding retention and deletion of information is dependent firstly on defining the purpose to assess if a responsible party must keep the information longer for fulfilling the defined purpose or delete the relevant records, and (iii) ensuring data quality and the measures commensurate to maintain quality can only be done if the purpose of processing is explicitly defined to assess the level of quality required given the purpose of processing.[40]

d) *Further processing limitation*

Any additional purposes or uses of personal information must be compatible with initial purpose of collection.[41] In order to assess compatibility between the initial and secondary purposes, consideration must be given to the relationship between the reasons of the further processing, the type and nature of information collected, the consequences of such processing, the manner in which the information was collected and any contractual relationship between the responsible party and data subject.[42]

---

39 S13 and 14.

40 De Stadler *et al.* (2015) 12.

41 S15.

42 Papadopoulos S and Snail S *Cyberlaw@SA III: The Law of the Internet in South Africa*, 303.

e) *Information quality*

Responsible parties must take reasonably practicable steps to ensure that personal information is complete, accurate, and not misleading. This means that responsible parties must implement processes and set a regular schedule to update personal information on a continuous basis, where necessary.[43] Other authors have argued that a responsible party should not wait for a request to correct the information from a data subject, but should take the initiative independently to maintain data quality, where necessary.[44] This is based on the fact that some information change over time, for example, physical addresses, work numbers, marital status and therefore may become inaccurate over a period of time as opposed to certain identity information which hardly changes, for example, identity number or biometric information.

f) *Openness*

Responsible parties must make data subjects aware of the processing activities when collecting their personal information or as soon as reasonably practicable after information has been collected.[45] This must include, among others, the purposes for collecting information, the security measures to protect information, any sharing of personal information with third parties, their rights and dispute or complaints resolution processes. The traditional manner in which this is achieved is through privacy notices or privacy policies which are usually provided to the data subjects through a link in an application form or web application. De Starler et al, provides suggestions on drafting a privacy notice or considerations including among others, that the notice must be in plain language, be visible to data subject, the same medium used to collect information should be used to provide the notice

---

43 S16. Also see de Stadler *et al* (2015) 28.

44 Papadopoulos and Snail *et al Cyberlaw@SA III: The Law of the Internet in South Africa* (2012) 305.

45 S18.

and that different notices must be provided to different data subjects such as employees, suppliers and consumers.[46]

g) *Security Safeguards*

The integrity and confidentiality of personal information must be maintained by taking appropriate, reasonably technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information, unlawful access to or processing of personal information.[47] The type of security measures should not be limited to system based measures, but should also extend to physical security measures to safeguard physical records, including securing physical infrastructures and training individuals that handle or process personal information.[48] The security measures to be implemented in any given processing activity is dependent on the nature of personal information and the harm which could result in the information being compromised, for example, the more sensitive the information, the more secure it should be. [49] Van der Merwe provides that information security measures involve a careful evaluation of the security risks and exposures to information assets and the implementation of security controls commensurate to the risk of exposure. These measures should be embodied in organisational policies and enforceable against all employees within an organisation.[50]

Additionally, the Act requires responsible parties to ensure that third parties who process personal information on their behalf do so through a written agreement and the security of the information is maintained. Lastly, it requires that when there are reasonable grounds to believe that there was a security compromise, the data

---

46 De Stadler *et al* (2015), 21.

47 S19.

48 De Stadler *et al* (2015) 35.

49 *Id* 38.

50 Van der Merwe (2014) (PELJ) 312.

subjects must be notified as well as the Information Regulator.[51] According to an Interpol report[52], a staggering number of 230 million threat detections were witnessed in South Africa from January 2020 to February 2021.The threats ranged from ransomware, business email compromise attempts, online scams to digital extortion.[53] Given the evolving and sophisticated cyber-attack vectors employed by criminals to infiltrate systems and exfiltrate personal information, improving and strengthening security measures is absolutely critical to any organisation that process personal information.

h) *Data subject participation*

The Act also provides data subjects with rights, such as the right to request access to their personal information or to confirm whether the responsible party holds personal information about them, the right to correct or delete their personal information.[54] Furthermore, where the responsible party has given effect to the rights of the data subject, and such action results in a change of information and the changed information has or will have an impact on decisions that will be taken in respect of the data subject, the responsible party must inform each person to whom the personal information has been disclosed.[55] In order to exercise this obligation effectively, responsible parties must document their records of processing activities which would include details of processing activities as well as third parties who are involved in such activities. Without these data flows or understanding of the processing operations, this obligation will be challenging to implement in practice.

---

51 S20 and 21 POPIA.

52 Interpol 'African Cyberthreat Assessment Report Key Insight into Cybercrime in Africa' (October 2021) 9.

53 *Id.*

54 S23 and 24 POPIA.

55 S24(3).

The POPI Act does not apply to the processing of personal information solely for purposes of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile the right to privacy with right to freedom of expression.[56]

While the foundation of the POPI Act is based on the above 8 lawful conditions, the Act has other requirements that a responsible party must ensure adherence to, such as requirements on direct marketing, automated decision making as well as transborder flows of personal information.[57]

### 1.2.3 *The Right to Correct or Delete*

The focus of this dissertation will be on the last condition explained in paragraph 1.2.2 above, *Data Subject Participation*, specifically section 24 of POPIA which provides that a data subject may, request any entity that processes personal information to:

> "…*a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or*
>
> *b) the responsible party is no longer authorised to retain in terms of section 14 of the Act*."

The Act does not provide for an express right to be forgotten in its text, it does however, provide that a data subject has a right to request destruction and deletion of information that is "…inaccurate, irrelevant, excessive, out of date, misleading or obtained unlawfully." Unpacking the extent of this right becomes critical in the digital era due to the ubiquitous nature and complexity of processing taking place through digital platforms, and to enable effective application of deleting personal information. The practicality of this right, the impact it has on technical and non-technical means, the extent to which the right may be

---

56 S7(1).

57 S69, 71 and 72.

exercised, and what it truly means to give effect to the right are fundamental challenges that will be addressed in this paper.[58]

## 1.4 Research Questions

This paper seeks to analyse and investigate the following:

a) The concepts of the 'right to be forgotten, right to delete, right to erasure' both from a legal, social and technological perspective.
b) Interpretation through case law of the right and application in the European Union context and the application to South African law.
c) The limitations and the interaction with other fundamental rights, for example, freedom of expression.
d) Practical implementation challenges of the 'right to be forgotten, right to delete, right to erasure'.

## 1.5 Methodology/approach

The research paper uses a combination of approaches in understanding and unpacking the complexity of the right. It relies on socio-legal research to analyse these rights in the social context, and its impact on the social wellbeing of those concerned. The paper also uses comparative analysis looking at the interpretation of the rights in the European Union context.

The comparative overview with Europe is befitting, due to the wide and extra-territorial application of its privacy laws. Finally, a critical approach is employed to analyse the alternatives discussed in numerous scholarly articles, legal doctrine, political and social

---

58 See discussion in paragraph 2.2.2 *Technical Interpretation*, 3.2.4 *Analysis of the judgement* and 4.3 *Impact of the Right to be Forgotten on Freedom of Expression*.

debates to the challenges posed by the introduction of these right and its impact in the South African context.

## 1.6 Outline of the Chapters

The first chapter of the paper seeks to provide an overview of the concept of data privacy and its development in South Africa and introduces the focus of the paper.

The second chapter will introduce the legal and socio-philosophical concepts of the 'right to be forgotten, the right to delete, and the right to erasure' and the different views on the meaning of these concepts.

Chapter three will look at the interpretation of the right to be forgotten by the court in the European Union as no case has been decided in the South African context.

Chapter four focuses on the impact of this right on other constitutionally recognised rights, specifically the right to freedom of expression, and considerations in the balancing act between the two rights.

The fifth chapter concludes the paper and provides recommendations to address the challenges that are introduced by the introduction of the "right to delete" in South Africa.

## 1.7 Terminology

For consistency throughout the paper, the terms below will be used and defined as per the concepts in POPIA:

a) **Personal information/Personal data:** "Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person".[59]

b) **Process or Processing:** "Any operation or activity or any set of operations, whether or not by automatic means concerning personal information".[60]

c) **Data subject:** "A person to whom information belongs".[61]

d) **Operator/Processor:** "A person or body which process personal information on behalf of another responsible party".[62]

---

59 S1.

Personal information includes but is not limited to:

(a) "Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

60 S1.

Processing can include the following:

(a) "the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information."

61 *Id*.

62 *Id*.

e) **Responsible Party/Controller:** "A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[63]

f) **Digital Era:** Defined as the era in "which many things are done by computer and large amounts of information are available because of computer technology".[64]

g) **European Union General Data Protection Regulation**: The acronym used throughout the paper is GDPR.[65]

h) **Protection of Personal Information Act 4 of 2013**: The acronym used throughout the paper is POPIA or POPI Act.

## 1.8 Synopsis

To establish a foundation from which the challenges of the "right to be forgotten", "right to delete" and "right to erasure" can be discussed, it is critical that these concepts are first analysed. The next chapter analyses these rights from a legal, technical and socio-philosophical perspective.

---

63 *Id.*

64 The definition is taken from the Cambridge dictionary, which can be found on https://dictionary.cambridge.org/dictionary/english/digital-age (accessed 27 March 2021). This definition is not just focused on the use of computers or digital means but also illuminates the large-scale information processing in the digital era.

65 Regulation 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.

# CHAPTER 2: DEFINING THE CONCEPT OF THE RIGHT TO BE FORGOTTEN, RIGHT TO DELETE AND RIGHT TO ERASURE

## 2.1 Introduction

Defining the concept and extent of the "right to be forgotten", "right to delete" and "right to erasure" is critical as it establishes the context through which the practicality of the right is discussed.

It is also particularly important to investigate the existence of the right to be forgotten or delete from a historical context in South Africa, and the forms it has taken in other pieces of legislation. The concept of deleting or expunging records in the South African context is not new, it has been explored and exists in different ways in the South African legislative framework and may have a different interpretation. Some examples are briefly outlined below. Thereafter the concept or phrase is examined in greater detail from a socio-philosophical, technical and legal perspective to lay the foundation and unpack the different challenges introduced in the implementation of this right.

### *2.1.1 The Criminal Procedure Act*

The Criminal Procedure Act 51 of 1977 provides for a process of expunging criminal records in certain instances.[66] Let's consider a scenario where a person was convicted of an offence with no direct imprisonment, but 15 years later he is still unable to fully integrate into society and find employment due to their criminal record, the Act allows them to apply for criminal expungement if they meet the defined criteria.[67] The result of

---

66 S271(B) of Criminal Procedure Act 51 of 1977.

67 The Department of Justice and Constitutional Development has outlined circumstances under which the application for being pardoned can be reviewed and provides that "…10 years must have lapsed since the date of the conviction for that offence, the person must not have been convicted

this is that the criminal record is deleted and treated as if there was no criminal record to begin with. However, any reference to the name associated with the crime is not removed in other sources outside of the criminal system for example there will still be case law, and media articles if the case received such exposure. This is different to the possibility of a Presidential pardon that allows the President of South Africa, to "…forgive offenders and remit any fines, penalties or forfeitures."[68] Where a full pardon has been granted, this means the offender must be treated as a person who has not been convicted of the offence, and any legal consequences or effects of the conviction are removed.[69]

In both the two instances, the concept of forgetting or deleting is not a construct that allows a record to be completely forgotten as if it never existed. It does not change history or the occurrence, it is merely a mechanism that may ease or enable the integration of offenders back into the society and remove legal consequences of the offences.[70]

### *2.1.2 The National Credit Act*

The right to have your records expunged is also evident in the National Credit Act.[71] The NCA provides that a credit bureau must "…expunge from its records any consumer credit information that, in terms of the regulations, is not permitted to be entered in its records or is required to be removed from its records."[72] This is particularly relevant where a

---

of any other offence and sentenced to a period of imprisonment without the option of a fine during those 10 years. " *Cf* www.justice.gov.za (accessed on 30 June 2020).

68 S84(2)(j) of the Constitution.

69 *Masemola v Special Pensions Appeal Board and Another* (CCT260/18) [2019] ZACC 39; 2019 (12) BCLR 1520 (CC); 2020 (2) SA 1 (CC) (15 October 2019), para 31,37.

70 *Id* para 36.

71 The National Credit Act 34 of 2005 (hereafter NCA).

72 *Id* S70(2)(f).

person was in a debt re-arrangement[73] and has obtained a clearance certificate[74] and is not over-indebted[75] and in debt review anymore.[76] The Act requires the credit bureau or national credit register after receiving such certificate to expunge from its record the fact that the consumer was subject to the relevant debt re-arrangement order or any information that resulted in debt re-arrangement.[77]

It's important to note that while the credit bureau is required to remove any adverse information relating to the paid up judgements, the NCA Regulations do not require any amendment to the payment profile which reflects payment behaviour over a period of five years.[78] The position that is not clear from the Regulations is whether a credit provider

---

73 S86(7)(b),(c) Debt re-arrangement is where a consumer is "…*likely to experience, difficulty satisfying all the consumer's obligations under credit agreements in a timely manner" And their obligations are re-arranged by "…(a) extending the period of the agreement and reducing the amount of each payment due accordingly; (b) postponing during a specified period the dates on which payments are due under the agreement; (c) extending the period of the agreement and postponing during a specified period the dates on which payments are due under the agreement; or (d) recalculating the consumer's obligations."*

74 S71(1) A Clearance certificate is a certificate that is issued if the *"consumer has satisfied all the obligations under every credit agreement that was subject to the debt re-arrangement order or agreement, in accordance with that order or agreement".*

75 S79(1) Over-indebtedness is defined as: "A *consumer is over-indebted if the preponderance of available information at the time a determination is made indicates that the particular consumer is or will be unable to satisfy in a timely manner all the obligations under all the credit agreements to which the consumer is a party, having regard to that consumer's-*

*(a) financial means, prospects and obligations; and*

*(b) probable propensity to satisfy in a timely manner all the obligations under all the credit agreements to which the consumer is a party, as indicated by the consumer's history of debt repayment*."

76 S86(1) Debt review is a process where "*a consumer applies to a debt counsellor in the prescribed manner and form to have the consumer declared over-indebted."*

77 S71(5) NCA.

78 Proclamation No. R. 144 of 2014 *Removal of Adverse Consumer Credit Information and Information Relating to Paid-up Judgements* (National Credit Act) (Government Gazette 37386), 26 February 2014, S3(d).

may rely on its own credit record which it obtains on its internal records even though it alludes to the negative credit judgement.[79] Kelly-Louw explains that the Regulations only prohibits the credit provider from using the information that has been removed and was obtained from the credit bureau, it does not prohibit use of internal records.[80] If a credit provider can still rely on its own records, and the credit information presented by the credit bureau indicating the pattern and behaviour or even repayment history, one wonders whether this would constitute 'deletion' and whether the availability of such information will not equate to remembering? With this background, it is important to unpack what the "right to be forgotten", "right to delete" or "right to erasure" means in the context of information privacy.

## 2.2 Interpretations

### *2.2.1 Socio-Philosophical Interpretation*

Mayer-Schonberger describes the historical and psychological foundations of the concept of forgetting and remembering and analyses the potential impact of the two concepts to society in general, and seeks to define the right to be forgotten in the context of forgetting and remembering.[81] This author argues that advancement of digital technology and global

Also See *Magadze v ADCAP, Ndlovu v Koekemoer* (57186/2016) [2016] ZAGPPHC 1115 (2 November 2016), where the court ordered the credit bureau to remove the applicant's debt review status from applicant's credit records (among other things). This was done after the applicants applied to have themselves declared over- indebted in terms of s86(1) of the NCA. The applicants as a result of the debt review process managed to pay off some of their some of their debts and wanted to be cleared from the debt review process.

79 *Id*.

80 Kelly-Louw M "The 2014 credit-information amnesty regulations: What do they really entail?" (2015) 48 *De Jure* 92-115.

81 Mayer-Schonberger V (2009) *Delete: The virtue of forgetting in the digital Age* Princeton and Oxford: Princeton University Press.

networks have shifted the scale and forgetting has become the expensive and difficult while remembering is cheaper and easier.[82] It is further stated that there are four drivers that have led to this shift, namely; "…digitisation, cheap storage, easy retrieval, and global reach".[83]

Firstly, digitisation has transformed our lives, we live in a digitized society where any activity can be done through digital means. For example, businesses operate across borders through the internet and e-commerce, most banking services are provided through digital means and branches are becoming less value driven and more of a convenience for those that can't operate digitally, restaurants are now digitised and food can be ordered at the click of a button and delivered to your home, public transportation has also evolved, companies such as Uber provide digital service which at the click of a button provides you with transport to your chosen destination.[84]

Secondly, the concept of remembering requires that you are able to retrieve the information later. Over the years, retrieval through digital means has made it easier to find information, by typing what you want in a search box, a click, and then results matching your search appear.[85]

Thirdly, global digital networks eliminate the constraint of locations, one needs to be connected to the applicable network, and they can retrieve the information irrespective of the jurisdiction they operate in.[86]

---

The author argues that forgetting in todays' world is extremely difficult due to digital remembering, he notes that retaining information is now becoming the default and not the rule because it requires less effort and money due to the technological advancements that enable retention of information.

82 *Id* 59.

83 *Id* 43-58.

84 See the Uber business model on *How to use Uber app* found on https://www.uber.com/za/en/about/how-does-uber-work/ (accessed 25 March 2021).

85 Mayer-Schonberger (2009) 49.

86 *Id* 52.

In Ambrose's research on digital oblivion there is a discussion about "…forgiveness, re-establishment, and re-invention…" as the foundations of the right to be forgotten.[87] This school of thought is based on the fact that our past impacts the future, affects your prospects of employment and your right to a good reputation, for example, most prospective employers research their prospective employees to understand their behaviours, online presence, their criminal records, credit history etc., and impacts to a large extent on whether they get the job or not.

This same understanding was described by Solove.[88] Solove describes how the internet is so influential in changing one's reputation, and the enormous impact and extent of reach that the internet has as compared to the traditional paper-based processing. Further to that, Solove draws the picture of the internet as an 'obstruction to recreation of oneself', and that the cause of the negative effects emanating from keeping information on the internet stay longer due to its easy retrieval, and this in turn threatens the ability to recreate and re-invent self.[89]

The concept that computers can keep information for an indefinite period, are able to store large amounts of information, retrieve it, and share it across jurisdictions threatens this forgiveness principle.[90] The perspective on this school of thought is that humans need to forget in order to forgive, and that if you are constantly reminded of the past, it hinders your ability to move past historic experiences.[91] However, the idea that forgetting is a

---

87 Ambrose ML. *Digital Oblivion: The Right to be Forgotten in the Internet Age,* (2013) University of Colorado Boulder, Alliance for Technology, Learning and Society (ATLAS) Institute. Available from https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/0v8380833 (accessed 4 September 2020).

88 Solove JD (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* Yale University Press, 33.

89 *Id* 5.

90 Westin AF and Baker MA *Databanks in a free society* Times Books (1972) 267.

91 See article Wickramasinghe S "The Oblivious Oblivion: A Critique on the EUCJ's Right to Be Forgotten" (25 November 2015) https://ssrn.com/abstract=2782746 (accessed on 13 April 2020).

prerequisite for forgiveness may somewhat not be entirely accurate, one may argue that forgiveness is not forgetting, but acceptance to move past the experience notwithstanding any reminder of the event.[92]

Contrary to this school of thought, Paul-Choudhury narrates a story about his wife who was on her death bed, and requested him to ensure that she is remembered not as a woman who was sick and weak, but as the beautiful and ambitious woman she was before her last year of life which was defined by her illness, cancer.[93] To the author, internet seemed to be the only way to fulfil his wife's wishes, and he built a memorial website to celebrate his wife's life that would last decades after her death. He makes a distinction between the divided opinions on the right to be forgotten, and refers to two school of thoughts, one as 'deletionists' or those who believe that the internet should learn how to forget, and 'preservationists' or those who believe that that internet should preserve and keep information that will later have an influence on future generations.[94] While there are different perspectives of the foundations and motivations of the right to be forgotten, the common theme across is based on the notion of choice and control that is provided to persons to decide what information remain in the public domain, even internally within institutions.[95]

### *2.2.2 Technical Interpretation*

Technology is a critical role player in the enforcement of the right to be forgotten in the digital era. Without proper technology, the right to be forgotten will not be enforceable.[96]

---

92 *Id.*

93 Sumit P 'Digital legacy: The fate of your online soul' featured story on New Scientist 19 April 2011 www.newscientist.com (accessed on 13 April 2020).

94 *Id*.

95 See OECD *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) 67.

96 Druschel P, Backes M, Tirtea R "The right to be forgotten – between expectations and practice" (2011) 3 European *Network and Information Security Agency (ENISA)* 1-22.

The definition of the concept influences the technological functionalities that must be developed and built-in digital platforms.[97] In a technical space, forgetting information can have different meanings. It can be interpreted as meaning that all records of the information in question must be deleted from any medium, they exist they in, possibly including disaster recovery sites and any backups of the information.[98] If this strict definition is the intention of the legislature, a capability must be developed by organisations to track and delete information in such a manner that it cannot be recovered or reconstructed in any intelligible form.[99] This strict interpretation introduces challenges, particularly in an open system where information and the resultant use outside of the platforms cannot be tracked.[100] It also presents challenges of tracking the existence of the information in unstructured sources of information, such as e-mail, presentations.[101]

The other interpretation that has been suggested is based on access restriction, and suggest that the information should be encrypted, and access restricted and information removed from any public domain, or any database that can be queried or accessed by others.[102] This lenient interpretation means that the information still exists however it is not accessible to the public or others depending on the circumstance. The United Kingdom Office of the Information Commissioner (ICO) provides that a valid erasure request means that steps must be taken to ensure erasure from live and backup systems. It also provides that there may be instances where the erasure cannot be fulfilled in respect of the backup and that such information must be restricted from use until such time it can be overwritten.[103] This explanation by the ICO is implying that the first price is

---

97 *Id* 12.

98 *Id.*

99 *Id* 13.

100 *Id* 15.

101 *Id.*

102 Guide to General Data Protection Regulation, UK Information Commission Office (ICO) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (accessed 24 October 2020).

103 *Id.*

to apply the right to erasure in its strictest form, and in exceptional technical circumstances a more lenient interpretation can be adopted. However, the guidance from the ICO fails to provide the exceptions under which the lenient interpretation must be adopted.[104]

The ICO further makes a distinction between the right to be delete and the right to destruction. It states that the right to delete means that the information is no longer available or cannot be easily recovered. In contrast, data destruction is a permanent removal of information with no chance of recovery. This is an interesting distinction and may be applicable for electronic records, but this interpretation will present a challenge from a physical record perspective. Where this right is exercised in relation to physical records, one may assume that deletion will mean destruction, and not necessarily restriction of access.[105]

Bernal suggest that the right to delete and right to be forgotten are different both in their focus and effect.[106] The author makes a distinction between intention to erase history and control of information being held about a person. It is noted that the right to delete is a right to act, and right to be forgotten appears to be a right to control someone else. Xanthoulis shares the same sentiments as Bernal and provides that the two concepts differ from a technical perspective, the concept of the right to delete means that we are limiting access by anyone other than the holder of information, and forgetting means complete removal of control.[107] While the above submissions merely talk about the right

---

104 *Id.*

105 *Id.*

106 Bernal PA "A Right to Delete?" (2011) 2 E*uropean Journal of Law and Technology (EJLT)* 2.

107 Xanthoulis N "The right to Oblivion in the Information Age: A Human Rights Based Approach" (2013) 10 *US-China Law Review* 84. The English Dictionary defines "Delete" as *remove from a computer's memory, Erasure* means *removal of all traces of something, obliteration*, and 'Forget' as *failure to remember, deliberately cease to think of something*.

to be forgotten as a link between the past and present, there is a wider application that links the right to be forgotten to purpose.[108]

### *2.2.3 Legal Interpretation*

#### *2.2.3.1 International Data Protection Instruments*

In 1980, the Organisation for Economic Cooperation and Development (OECD) defined and adopted Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data (OECD Guidelines), these have since been amended in 2013.[109] However, the OECD Guidelines marked one of the first initiatives to provide guidance on the handling of personal information to the OECD member countries and influenced and served as a foundation for the development of legislation across jurisdictions. Nearly 40 years back, the right to challenge data and have such data erased was recognised as one of the principles that OECD member states had to give effect to.[110]

In 1981, the Council of Europe adopted the Data Protection Convention (Treaty 108), which recognised the need to balance the respect for privacy and the free flow of information between member states and signatories of the treaty.[111] This Convention marked one of the first legally binding international instrument in data protection which required signatories to implement the principles and take steps to incorporate the

---

108 De Terwangne C *The Right to be Forgotten and the Informational Autonomy in the Digital Environment* (2013) Publications Office of the European Union, available from http://dx.doi.org/10.2788/54562 (accessed on 20 August 2020).

109 OECD *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) 79.

110 Art 13 (d) of the OECD Guidelines (1980) read as follows: "…...An individual should have the right to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended."

111 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, European Treat Series, No 108. (hereafter referred to as the Convention).

principles in their domestic legislation.[112] Article 8 of the Convention provided for additional safeguards for data subjects which included the right to erasure and rectification if the personal data was processed contrary to quality of data[113] provisions and special categories of information.[114]

The example of the two international instruments is evidence to the fact that the right to erasure or rectification is not a new concept, it is an evolving concept that has now featured in many jurisdictional data protection legislations as a result of these instruments that became the foundation for data protection.[115]

---

112 See brief history of the European Treat No 108, and Protocols on https://www.coe.int/en/web/data-protection/convention108-and-protocol (accessed on 27 March 2021).

113 *Id*, Art 5 headed "*Quality of data*" read as follows:

"…….. Personal data undergoing automatic processing shall be:

a) obtained and processed fairly and lawfully;

b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

d) accurate and, where necessary, kept up to date;

e) preserved in a form which permits identification of the data subjects for no longer than is require for the purpose for which those data are stored."

114 *Id*, Art 6 headed "*Special categories of data"* read as follows: "…...Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

115 See discussion on European Data Protection Instruments in paragraph 2.2.3.2. There is currently 27 countries which form the European Union, see the list on https://europa.eu/european-union/about-eu/countries_en (accessed 27 March 2021).

*2.2.3.2 European Data Protection Instruments*

*2.2.3.2.1 Directive 95/46/EC*

In 1995, the European Union issued a Directive 95/46/EC in 1995 to provide guidance to member states on the handling of personal information and to enable cross border sharing of information between members.[116] The Directive followed after much consideration regarding the impact of the Convention (Treaty 108) to member states, and the resultant divergences which existed in member states on the applications of the data protection principles.[117] The objective of the Directive was to coordinate and ensure consistent manner of processing personal data and cross-border flows of information while allowing member states room to further specify the application of the requirements in their respective states.[118]

Significance will be placed on the provisions of the Directive in respect of the right to "…rectification, erasure and blocking…". due to its role in the evolution and interpretation of this right by the courts.[119].

Article 12 (b) provides for the right to access to information and states that *"Member States shall guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;".*

---

116 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 (hereafter referred to as Directive 95/46/EC).

117 *Id,* Recital par 8.

118 *Id.*

119 See Chapter 3 for a detailed discussion on the interpretation of the Art 12 (b) of the Directive in *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPF) and Mario Costeja Gonzalez*, CJEU Case C-131/12.

Article 32 (2) adds and provides that *"Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller*."

Additionally, Article 12(c) then requires *"notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with Article 12(b), unless this proves impossible or involves a disproportionate effort."*

Whilst the above articles did not explicitly recognise the right to be forgotten, the "right to rectification, erasure and blocking" laid the foundation through which the right to be forgotten developed and evolved in the current era and form.[120]

*2.2.3.2.2 General Data Protection Regulation*

The General Data Protection Regulation (hereafter GDPR) was adopted as a regulation applicable to European Union (EU) in April 2016 and supersedes the Data Protection Directive.[121] The GDPR was adopted to align to the complexity of processing, rapid technological advancement and globalisation, and to eliminate the fragmented approach to implementation of data protection requirements across EU.[122] Unlike the Directive, the GDPR is a regulation and therefore is self-executing and does not necessarily require

---

120 Alessi S "Eternal Sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation" (2017) 32 (1) *Emory International Law Review* 145.

121 Regulation 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 (General Data Protection Regulation or GDPR). The GDPR became enforceable on 25 May 2018 (Recital par 171).

122 *Id*, Recital par 6,7,9.

domestic implementation by the member states, it automatically forms part of the member state legal system.[123]

The GDPR provides rules for the processing of personal data and free movement of information.[124] It is applicable for any processing of personal data by a processor[125] or controller[126] established in the Union regardless of whether the processing takes place in EU or any other jurisdiction.[127] It is also applicable where the processor or controller is not established in the EU but processes personal data of data subjects in the EU for the offering of goods or services or the monitoring of their behaviour as far as their behaviour takes place within the Union.[128]

The data protection principles outlined in GDPR are centred on ensuring that the personal data is processed lawfully, fairly and openly.[129] It must be processed for a defined purpose, and processing must be minimal and necessary considering the purposes defined.[130] Personal data must be kept accurate and relevant[131], and controllers should have mechanisms to give effect to data subject rights.[132] GDPR also requires that throughout the lifecycle of processing, adequate security safeguards must be applied to

---

123 Alessi (2017) 145.

124 *Id*, Art 1(1).

125 Art 4(7) Processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

126 Art 4(8) Controller is defined as the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

127 *Id,* Art 3 (1).

128 *Id*, Art 3 (2).

129 Art 1(a).

130 Art 1(b).

131 Art 1(d).

132 Chapter 3 (Art 12-23).

the personal data[133], and personal data should not be retained longer than is necessary to fulfil the purpose of processing.[134]

Focus and significance will be placed on the provisions of GDPR that addresses the right to erasure or delete. Article 17(1) which is headed "Right to erasure ('right to be forgotten')" read as follows:

*"…. The 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 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 otherwise processed;*

*(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing*

*(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*

*(d) the personal data have been unlawfully processed;*

*(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*

*(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."*

Additionally, the GDPR obligates a controller that had made the personal data public to inform where reasonably feasible, other controllers which are processing the data in question to erase any links to, copies or replication of the personal data.[135] However, this

---

133 Art 1(f).

134 Art 1(e).

135 Art 17(2). Also see Art 19 which states that "t*he controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this*

right to be forgotten is not absolute, and there are exceptions for example, where the processing is necessary for (a) exercising freedom of expression or information, (b) for achievement of a public interest, (c) necessary for exercise, establishment or defence of legal claims.[136] In the text of the GDPR, the word "right to be forgotten" seem to be used interchangeably with the "the right to erasure".[137]

Article 18 also provides for the "right to restriction of processing", while this right is independent it can also be seen as an alternative to the right to erasure. It can be exercised where the data cannot be rectified, and the accuracy is being contested[138], processing is unlawful and data subject is against the data being erased[139], where data is no longer required to be retained but must be kept for legal claims.[140]

In explaining what this right entail, the Recital provides that the right to be forgotten is the right to have personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed.[141] The expectation is that the controller will inform other parties who are processing the same information to erase "…any links to, copies or replication of those personal data".[142] Druschel *et al*, notes that whilst the nature of EU regulations and laws tend to be broad and general to enable various interpretations for different circumstances, the right to be forgotten requires a precise definition of its scope and applicability to be implemented effectively.[143] The author then provides various possible interpretations of

---

*proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it."*

136 Art 17(3).

137 Recital 65 and 66.

138 Art 18(1) (a).

139 Art 18(1)(b).

140 Art 18(1)(c).

141 Recital 65 and 66.

142 *Id.*

143 Druschel P, Backes M, Tirtea R, "The Right To Be Forgotten – Between Expectations And Practice", European Network and Information Security Agency (ENISA)" (2011) 3.

this right in the context of technology. Firstly, the right to delete can be interpreted to have a strict interpretation which requires that all copies of the data is erased and removed from all assets to the extent that it is no longer recoverable any means possible. Secondly, this right could also be interpreted to mean that where the information records are encrypted without unauthorised access this right can be limited, with a view that data kept away from public sources or from being readily available does not pose a risk and can therefore survive. In a nutshell, Druschel et al argues that the ability to enforce a "right to be forgotten" depends on the technical capabilities of information systems and to avoid different interpretations, the law must be clear on the scope of this right from an implementation perspective.[144]

*2.2.3.3 South Africa*

The scope of application and data processing conditions of the POPI Act were discussed above in paragraph 1.2.2 and 1.2.3 respectively. This section focused on section 24 which uses the words "…right to delete…" and not 'right to erasure'.[145] This right can be exercised where information is "…inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or where it should not be retained…".

Similarly, to the repealed Directive and GDPR, the responsible party is required to take reasonably practicable steps to inform persons to whom the information was shared.[146] There is no guidance in the Directive or GDPR on the application of notifying other controllers of this requirement. It is therefore important in the South African context to define what this obligation entails, to what extent it is deemed unreasonable to inform downward consumers of information, and under what circumstances responsible parties need to notify original publishers of the information to ensure that the right is considered in the entire value chain.

---

144 *Id.*

145 S24.

146 S24(3).

## 2.3 Synopsis

Notwithstanding the historical recognition of the “right to delete” or “right to erasure in the different legal instruments, none of the legal instrument delineate what it means to erase or delete information and how to enforce the right. From the interpretation of GDPR, the right to be forgotten is merely an extension or another term to refer to the right to erasure. The Convention (Treaty 108) also refers to “erasure or rectification” without providing or defining the word “erasure”.

On the other hand, the right to erasure or delete may also have different technical interpretations, such as restriction of access, and perhaps even complete removal of information without the ability to retrieve such information. The POPI Act requires that where a record of personal information is no longer required to be retained it must be deleted in a manner that prevents its reconstruction again.[147] If the same interpretation is applied to section 24, this will mean that POPI Act requires the record to be completely deleted without being reconstructed again.

To avoid misalignment in the implementation of this right, it is critical that the Information Regulator[148] delineate extensively through regulations what constitute the right to delete from a technical perspective and the extent to which this right must be implemented, for both automated and non-automated processing. Without this guidance, each responsible party will interpret this requirement differently. Based on the maturity of data protection in Europe, the next chapter assesses how the European courts have interpreted this right to date and how the developments will impact on South Africa.

---

147 S14(5).

148 See S39, The Information Regulator is an independent body established in terms of the POPI Act, responsible for enforcement.

# CHAPTER 3: GOOGLE SPAIN SL AND GOOGLE INC. V AGENCIA ESPANOLA DE PROTECCION DE DATOS (AEPD) AND MARIO COSTEJA GONZALEZ

## 3.1 Introduction

The case of *Google Spain* marked one of the first case in Europe in which the Court of Justice of the European Union (CJEU) held that persons have a right to be forgotten.[149] Therefore, the analysis of this case is critical when considering what the right to be forgotten entails, and the circumstances under which the right can be exercised. This case was decided based on the provisions of the EU Directive 95/46/EC which has since been repealed by the GDPR. This judgement is of significance as it sets the tone for the development and interpretation of the right to be forgotten globally.

The previous chapter looked at the different interpretations of the right to delete, erasure or forgotten from a socio-philosophical, technical and legal perspectives. The aim of this chapter is to evaluate the interpretation by the court in the *Google Spain,* and the potential impact of this decision globally as well as a benchmark for how other jurisdiction may interpret the right to be forgotten, erasure or delete.

## 3.2 *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez*

### *3.2.1 Factual Background*

The matter started in 2010, when the complainant (Mario Costeja Gonzalez) lodged a complaint with the Spanish Data Protection Authority (hereafter referred to as the AEPD)

---

149 *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez,* 2014, Case C-131/12, Court of Justice of the European Union (hereafter referred to as Google Spain SL).

against a daily newspaper, and against Google Spain and Google Inc. The complaint was related to information that would appear when an internet user searched his name in the Google search engine. The information that would appear related to a real estate auction connected with an attachment proceeding for the recovery of social security debts, which incident took place in 1998.[150]

The complainant requested that the publisher of the newspaper of the articles remove the pages so that the information does not appear or alternatively employ technological tools provided by search engines to protect the data.[151] The complainant also requested Google Spain or Google Inc. to remove or hide the search results related to him when an internet user searches his name. The argument relied upon by the complainant was the fact that the matter had been fully resolved which rendered this information irrelevant. The Spanish Authority rejected the complaint against the publisher of the information and provided that such publication was justifiable and lawful.[152] However, the Spanish Authority held that Google Spain and Google Inc must remove the links from its search engine.[153]

Both Google Spain and Google Inc. brought actions against the decision of the AEPD. The AEPD decided to refer the matter to the CJEU for a preliminary judgement.[154]

### *3.2.3 CJEU Judgement*

The court held that search engines are considered 'controllers', meaning that they determine the means and purpose of processing of personal data.[155] The court further

---

150 Google Spain SL, par 14-15.

151 *Id* par 16.

152 *Id*.

153 *Id* par 17.

154 *Id* par 20.

155 *Id* par 34.

held that the activity of search engines should be considered as processing when it involves personal data.[156] It concluded that the right to delist the information are paramount to the economic interest of Google and the right of the public to find that information.[157] The court acknowledged the right of data subjects to directly exercise their right to be forgotten against search engines.[158] Therefore requiring search engines to adopt technology and mechanism to enable the assessment of the requests, apply judgement and give effect to those rights where it deems the request justifiable.

### *3.2.4 Analysis of the judgement*

This judgement has a significant impact on the operations of search engines and potentially all information in digital mediums accessible to the public, on the right to freedom of expression and right to access to information on the internet.[159] It has significantly changed the dynamics of what can be accessible to the public by giving the data subject the right to be forgotten where they believe that the information is irrelevant, excessive, or out of date.[160]

---

156 *Id.*

157 *Id* par 97.

158 *Id* par 62, the court concluded that "…[A]rticle 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, 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."

159 *Id* par 71 and 81.

160 It is reported that less than 2 months after the Google Spain SL case, had received 91,000 takedown requests in total, relating to 300,000 pages. This number is evidence of the implication of the right to be forgotten. See Juliette Garside, "Wikipedia link to be hidden in Google under 'right to be forgotten' (2 August 2014)" http://www.theguardian.com/technology/2014/aug/02/wikipedia-page-google-link-hidden-right-to-be-forgotten (Accessed 27 March 2021).

The judgement is also not devoid of criticism on a range of matters including:[161]

a) whether search engines are in fact controllers in the context of the facts of the case,[162]
b) the balancing act utilised by the court to assess invasion of the privacy rights of data subject versus the right to freedom of information and the interest of the public to have access to the information in question,[163]
c) whether the rights to rectification, erasure, blocking and objection provided in the Article 12(b) and 14(a) of Directive amount to a right to be forgotten.[164]

In his opinion on this case (Advocate General Jääskinen) acknowledged the context under which the 1995 Directive was developed.[165] It was noted that the internet as we know it today was just a new phenomenon when the Directive was developed in 1995 and acknowledges that today the internet has a far greater reach in terms of access and dissemination of information.[166] Because the Directive was not developed with today's technology in mind, its application in this digital era is likely to become too wide.[167] Therefore, it's noted that the court should apply the law using a reasonableness test to

---

161 See Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21 (6) *Computer and Telecommunications Law Review* 44.
Also see Ausloos J "The 'Right to be Forgotten' — Worth remembering?" (2012) 28(2) *Computer Law and Security Review* 144.

162 Cofone I "Google v. Spain: A Right To Be Forgotten?" (2015) 15 *Chicago-Kent Journal of International and Comparative Law* 10.

163 Ausloos J "The 'Right to be Forgotten' — Worth remembering?" (2012) 28(2) *Computer Law and Security Review* 144.

164 *Supra* note 143.

165 Opinion of Advocate General Jääskinen delivered on 25 June 2013 Case C-131/12 *Google Spain SL Google Inc. v Agencia Española de Protection de Datos (AEPD) Mario Costeja González* par 28.

166 *Id*.

167 *Id* par 30.

avoid excessive and unnecessary legal consequences and compliance burden to those involved.[168]

The court provided that a search engine operator must be regarded a controller in respect of the processing of personal data that is carried out by that engine in the context of the activities in the main proceedings.[169] The court did not make a distinction between the activities of search engines to index information and on the other hand the activity to make the information available to an internet search user. One can argue that the activities of the search engine to index and find information on the internet can qualify as controller because it determines the means and purpose of the activity, it determines how it will be carried out and for what purpose.[170] However, the ability of search engines to make information available on a web search is done solely on the instruction of the internet user, and therefore the search engine acts on behalf of the user.[171] Cofone[172]argues that search engines are intermediaries, and they help internet users to find information they looking for. Therefore, if information appears in the top search results it is because users deem that information relevant.

The judgement then makes a generalisation that the activities of the search engine will render the search engine a controller without making a distinction between the different roles involved in the activities of the search engine.[173]

---

168 *Id* par 31.

169 *Id*.

170 *Id* par 63. Google Spain and Google Inc argued that the removal of information must be addressed to the publisher of the website concerned as it merely provides links to the website where the information is published.

171 *Supra* note 143.

172 *Id.*

173 The Opinion of Advocate General Jääskinen states that *"…[I]n my opinion the general scheme of the Directive, most language versions and the individual obligations it imposes on the controller are based on the idea of responsibility of the controller over the personal data processed in the sense that the controller is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their*

The court also chose to deal only with the issue of search engines and their obligations to remove links to information that is deemed irrelevant by data subject and did not address the implications of not erasing or blocking the same information on the third-party website where it was originally published.[174] Cofone provides that it is difficult to determine the relevancy of information if the outcome of the Google Spain case is such that the information is not removed in the original publication because its rendered legal.[175] However, it is made inaccessible by the removal of the links in the Google search engine. The fact that the information still exists in the original publication may arguably imply that it is still relevant.[176]

While the court justified the publication as lawful and qualifying under the derogation of 'journalistic purpose', this oversight by the court raises questions on the exact meaning of the 'right to be forgotten' and whether the right to erasure and blocking of data as provided for in Article 2(b) amounts to right to be forgotten or carries the same consequences.[177]

It is not surprising that some authors have referred to this judgement as the right to delist as opposed to the right to be forgotten.[178] This is because an obligation on Google to

---

*processing as personal data."* It is further provided in par 84 of the opinion that "…*[T[he internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way*."

174 Google Spain SL, par 88.

175 *Supra* note 143 ,10.

176 *Id.*

177 Google Spain SL, par 85.

178 Dulong de Rosnay M. and Guadamuz A. "Memory Hole or Right to Delist? Implications of the right to be forgotten on web archiving" (2017) 6 *RESET* ISSN 2264-6221.

remove links to third party website does not necessarily imply that the information is forgotten, it will still exist in the third-party websites where it was originally published.[179] In the opinion on this case, the Advocate General applies the wording of Article 2(b) of the Directive 95/46/EC to the facts of the case.[180] Article 2(b) provides that the right to erasure or blocking shall be guaranteed where the processing of data in question does not comply with the Directive or where it's incomplete or inaccurate. The Advocate General concludes that the information appearing on web pages cannot be incomplete or inaccurate. It is noted that when one interprets this provision it would mean that this right will only arise if Google's processing from third party source web pages is incompatible with the Directive.[181]

The court also does not clearly articulate the test to assess which interest overrides the other.[182] Instead the court in numerous occasions makes reference to 'public interest' and fails to look at access to information, freedom of expression as an independent right with equal weighting which deserves to be balanced against the right to privacy.[183] Furthermore, in the absence of clear assessment on how these rights must be balanced it is difficult to reach an outcome that will serve all rights.[184] The court lowered the right to

---

179 Google Spain SL, par 88.

180 Art 2(b) provides that "…[*M]ember States shall guarantee every data subject the right to obtain from the controller as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data*." Art 2(c) further states that the data subject has the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance to subsection (b), unless this proves impossible or involves a disproportionate effort.

181 Opinion of Advocate General Jääskinen (2013) par 85.

182 Google Spain SL, par 81.

183 Frantziou E "Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*" (2014) 14 Issue 4 *Human Rights Law Review* 761.

184 *Cf* art 11 of the Charter of Fundamental Rights of the European Union (2000/C 364/01) which provides for a right to freedom of expression and provides that: 1. "Everyone has the right to

freedom of expression and access to information and favoured the right to privacy without adequately balancing the rights. Additionally, the court then concluded that this outcome would have been different if the complainant was a public figure.[185] It would seem like the court was establishing a test on whether to give effect to the right to erasure and thereby protect the right to privacy, on the other hand what would outweigh the right to privacy.[186] While we recognize the prominence of certain public figures, assuming that a private individual can claim more rights than a public figure without qualifying the statement is disturbing.[187]

Wickramasinghe provides the opinion that the court seems to provide autonomy to the data subject to determine the relevancy of the information in question.[188] By allowing a user to determine irrelevancy of content that is lawfully published in the first place, would hamper other users to exercise the right to access to information, and those that publish the information to exercise the right to freedom of expression.[189]

Ausloos[190] is of opinion that this judgement constitutes some form of censorship in which people remove their personal data at will which may result in important information becoming inaccessible.[191] In addition, the decision-making responsibility conferred upon Google or any search engine to decide the merits of the right to be forgotten, the balance

---

freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.*"*

185 Google Spain SL, par 97.

186 *Id* par 81.

187 *Id*.

188 See an independent article by Wickramasinghe S. "The Oblivious Oblivion: A Critique on the EUCJ's Right to Be Forgotten" 6 (25 November 2015) found on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2782746 (accessed 15 August 2020).

189 *Id*.

190 Ausloos J "The 'Right to be Forgotten' — Worth remembering?" (2012) 28(2) *Computer Law and Security Review* 144.

191 *Id.*

with other rights, what information has future value is contrary to the objective of the "right to be forgotten".[192] Ausloos provides that the main purpose of the right to be forgotten was to balance the scales of power between controllers and data subjects and authorising controllers to decide what should not be viewed online is arguably achieving the opposite effect. This is because the economic interest of the controller may not align with individual interest.[193]

Furthermore, Article 12(c) of the Directive required *"notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with Article 12(b), unless this proves impossible or involves a disproportionate effort."* The Court did not address the obligation to notify other controllers or how to determine whether the notification involves a disproportionate effort. This means that while the links are removed by the search engine, the information might have been copied or transferred to other platforms which are untraceable.[194] This results in technical implementation challenges but also raises the question of the true meaning of the right to be forgotten.[195]

## 3.3 Synopsis

During the course of the preceding discussion, this chapter has highlighted a number of issues in the judgement of *Google Spain*.[196] Until this point, the right to be forgotten refers to the removal of links to personal information on specified sites and not the actual

---

192 *Id.*

193 *Id.* Also See Alessi S "Eternal Sunshine: The Right t Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation" (2017) 32(1) *Emory International Law Review* 145.

194 *Id.*

195 See discussion in Chapter 2 on the technical interpretation, par 2.2.2.

196 See discussion in 3.2.4.

information.[197] This is supported by the fact that the obligation on Google or search engines to delist links to information only applies to versions of the search engine corresponding to member state, and not to all the search engines domain name extensions.[198] This position was to uphold the right to freedom of expression that exist in different jurisdictions.

The balancing act between the right to privacy and freedom of expression is a critical one in the exercise of the right to be forgotten, due to the obligation of achieving the balance that must be sought by search engines or responsible parties. The balancing act has more significance to South Africa as a country that has its foundations in a democratic and open society.[199] The next chapter will assess the balancing act between the right to be forgotten and freedom of expression.

---

197 *Id.*

198 *Google LLC, successor in law to Google Inc. v Commission Nationale de l'informatique et des libertés* (CNIL), CJEU Case C 507/17 24 September 2019, par 39.

199 The Preamble, Constitution of the Republic of South Africa,1996.

# CHAPTER 4: IMPACT OF THE RIGHT TO BE FORGOTTEN ON FREEDOM OF EXPRESSION AND FREEDOM OF MEDIA IN THE DIGITAL ERA

## 4.1 Introduction

The internet has revolutionised how society interacts and communicates with one another and has significantly changed how information is accessed and disseminated. It has enabled people to freely express their views and opinions and impart information to the public, and to a large extent influence the views and opinions of others. The right to be forgotten as discussed in Chapter 3 introduces the concept that this information that is made public may be erased or links to it may be removed.

To enable ease of access and dissemination of information, there are several parties involved in the value chain. Let's consider a publication of an article about divorce proceedings of a prominent public figure in an online news platform. There are three parties, there is the publisher of the article, the prominent public figure and his family, and the public that receives the information. All parties have equal rights in the chain, the publisher has the right to freedom of expression and to impart information to the public. The prominent figure has the right to have their privacy and personal affairs respected, and lastly the public has the right to receive information of a public interest nature.

The complexity of balancing all these rights cannot be understated. This chapter seeks to analyse the interplay between the right to freedom of expression and the right to be forgotten, and considerations for the balancing act between the two rights suggested in case law and by scholars.

## 4.2 Freedom of Expression Explained

Section 16(1) of the Constitution provides for a right to freedom of expression and reads as follows:

> "…[E]veryone has the right to freedom of expression, which includes: (a) freedom of the press and other media; (b) freedom to receive or impart information or ideas; (c) freedom of artistic creativity; and (d) academic freedom and freedom of scientific research..."

For purposes of this chapter, focus will be on the right to freedom of the press and other media, as well as the right to receive or impart information or ideas.[200]

Venter is of the opinion that there is a connection between the role of freedom of expression in a democratic system and argues that effective democracy cannot exist in a country that does not adequately give effect to the right to freedom of expression.[201] Other authors have also expressed a similar view that freedom of opinion and expression plays a critical role in a fair and open society, but also recognised that such right is not absolute and comes with limitations.[202]

The role that the press, media and digital platforms play in enabling expression is a fundamental one. The press (both print and electronic), including other media such as broadcasting are at the fore front in the dissemination of information, creating dialogue on matters of public interest, influencing and shifting the minds of citizens. The ability and liberty of society to engage in such dialogue, is dependent on the extent to which the media is given freedom.[203] The court in the case of the *Government of the Republic of South Africa v Sunday Times Newspaper* recognised and defined the role of the press as a function that exposes corrupt activities and dishonesty, acting as a "…watchdog of the government."[204]

---

200 The word expression in the oxford dictionary means an 'act of showing emotions, feelings or ideas'. The right to freedom of expression includes any type or form of expression and is not restricted to those listed in section 16.

201 Venter R "The Role Of Freedom Of Expression In A Democratic System" (part 1)" (2018) 1 *Tydskrif vir Suid Afrikaanse Reg* (TSAR) 52.

202 Papadopoulos and Snail (2012) 251.

203 *Id*.

204 *Government of the Republic of South Africa v Sunday Times Newspaper* 1995 2 SA 221 (T) at 227.

In *Midi Television (Pty) Ltd v Director of Public Prosecutions (Western Cape)*, the court had this to say about the right of freedom of press:[205]

> *"…The constitutional promise is made rather to serve the interest that all citizens have in the free flow of information, which is possible only if there is a free press. To abridge the freedom of the press is to abridge the rights of all citizens and not merely the rights of the press itself..."*

In *Khumalo v Holomisa,* the Constitutional Court recognised the important role media plays in a democratic society, where O'Regan referred to media as "…primary agents…" in dissemination of information and creating platforms for expression of opinions and ideas.[206] Although the media has an important function to play in the dissemination of information, this right is not absolute and must be interpreted against the values of 'human dignity, freedom and equality'.[207] The case law discussed above exemplifies what "freedom of expression" really means in the democratic system of South Africa. Moreover, in today's world, the internet plays an important role in facilitating access, sharing and dissemination of information generally.[208]

## 4.3 Impact of the Right to be Forgotten on Freedom of Expression

There are a few ways in which the "right to be forgotten" and "right to delete" may impact on the right to freedom of expression.

Firstly, the existing interpretation of the right to be forgotten is that it provides persons with the right to request a search engine to delist links to articles or information about

---

205 *Midi Television (Pty) Ltd v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) par 6.

206 *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC) par 24.

207 *Id* par 25.

208 See discussion in Chapter 1, par 1.1.

them, if the information is considered irrelevant.[209] This does not mean the information ceases to exist, it is just not visible when searching on search engines. If a person has knowledge of the original source, they can still access the information.[210] The very fact that the visibility of the information is limited impacts on the right to freedom of expression, it makes it difficult for any person to find information unless they already have knowledge of the original source.[211] Publishers have a right to freedom of expression, and therefore those offering or publishing information may be impacted and their expression limited.

Secondly, one of the objectives of the right to freedom of expression is that it serves as a channel through which truth is realised.[212] When that right is limited, it directly impacts on the ability of the public to know the truth and the rights of citizens to access information.[213] If a strict interpretation of the right to be forgotten or delete is applied where delete or forget means that the information is wiped out and cannot be retrieved, this will not only limit freedom of expression but seriously undermine that right.[214]

---

209 Google Spain SL, CJEU Case C-131/12 par 85, 88.

210 *Id.* The judgement of the Google Spain case provided that there was a legal basis for the publisher to process and keep the article, and therefore did not have to delete the information. By interpretation this means that the article still does exist if a searcher goes straight to the publisher site.

211 *Id* par 85.

212 See *South African National Defence Union v Minister of Defence and Another* 1999 (6) BCLR 615 (CC); 1999(4) SA 469 (CC) par 7. The court stated the objective of freedom of expression as "…*valuable for many reasons, including its instrumental function as a guarantor of democracy, its implicit recognition and protection of the moral agency of individuals in our society and its facilitation of the search for truth by individuals and society generally. The Constitution recognises that individuals in our society need to be able to hear, form and express opinions and views freely on a wide range of matters*…"

213 Google Spain SL, CJEU Case C-131/12 par 63.

214 See discussion in Chapter 2, par 2.2.2.

In principle the right to freedom of expression and right to delete have equal weighting in law.[215] In the *Google Spain*, the court made a ruling that an individual's privacy outweighed the right of the public to receive information even when the information was lawfully justified.[216] The court also acknowledged that there is no blanket approach, and each case must be decided on its own merits. The court made an assertion that if the data subject was a public figure, there would be compelling public interest to deny the exercise of their right to be forgotten.[217] The court also provided that the balancing inquiry between the rights at issue will also depend on the sensitivity of information.[218]

Van Hoboken submits that balancing the right to be forgotten with the right to freedom of expression will always remain contentious and difficult. [219] This is because each case must be decided on its merit based on the circumstances. [220] While there is limited guidance on how the balance will be achieved, it is noteworthy to assess how the South African courts have balanced the right to freedom of expression and the right to privacy. This will provide a basis on some factors that courts have relied on in the balancing act and how the two rights co-exist if ever possible.

In a recent judgement, Sutherland recognized the interplay between privacy and freedom of expression and noted that exceptions to privacy can only succeed where the justification for the infringement outweigh the value of the right to privacy, and that there shouldn't be other means present to achieve the objective.[221] In addition, the

---

215 See discussion in Chapter 4, par 4.1 and 4.2.

216 *Id* par 97.

217 See consideration to take into account when deciding delisting requests in J Ausloos and A Kuczerawy "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling" (2016) 14(2) *Colorado Technology Law Journal* 219.

218 *Id* par 81.

219 J.V.J van Hoboken "Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines *Kluwer Law International* (2012) 350.

220 *Id.*

221 *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* 2020 (1) SA 90 (GP) par 35.

considerations for achieving the balance had to comply with the principles of 'legality, necessity and proportionality'.[222]

The concept of "proportionality" in the balancing act seems to be a prominent feature in most cases that seeks to balance the right to privacy with freedom of expression. Consider the *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*, where the court defined the limitation and balancing of constitutional rights as follows:

> "*…The balancing of different interests must still take place. On the one hand there is the right infringed; its nature; its importance in an open and democratic society based on human dignity, equality and freedom; and the nature and extent of the limitation. On the other hand, there is the importance of the purpose of the limitation. In the balancing process and in the evaluation of proportionality one is enjoined to consider the relation between the limitation and its purpose as well as the existence of less restrictive means to achieve this purpose*."[223]

These cases showcase the mutually inclusive nature, as well as conflict that can arise between the right to privacy and freedom of expression, particularly where personal information is both private and in the public interest.

In the EU, the Article 19 Data Protection Working Party, which is an independent European advisory body on data protection matters issued guidelines or a test for balancing the right to freedom of expression and right to be forgotten.[224] In addition to the consideration above, it provides the following additional test:

---

222 *Id.*

223 *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* 1999 (1) SA 6 par 35.

224 Article19 Working Party was established under Article 29 of Directive 95/46/EC. It is an independent advisory body on data protection and privacy. Its roles and responsibilities are defined in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Also see the balancing consideration

- Assessment of the private nature of the information, for example information about the health or intimate details of a person and its relevancy in being made public[225];
- The harm suffered by the applicant due to the information being made public must be considered[226];
- The fact that an applicant is a child or the information in question relates to children's information[227];
- Whether the information in question is part of a public record which publishes information for journalistic, artistic, literary, or academic purposes.[228]

The guidance provided by earlier case law and scholarly work is helpful, however, it lacks the practical implementation guidance that a responsible party needs to effectively discharge their obligation to give effect to the right to delete.[229] There is an acknowledgement that the interpretation of any right expands and becomes clearer as more judgements are given. However, what is peculiar in this instance is that the balancing act is not done by the courts, but responsible parties.

## 4.4 Synopsis

It is important that a standard defining the parameters of the exception to the right to delete must be outlined, for example, what would constitute journalistic, literary and

---

in the Article 19 Working Party *Guidelines on the implementation of the court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12,* 14/EN WP 225 *(*Adopted on 26 November 2014).

225 *Id* 13.

226 *Id*.

227 *Id* 14.

228 *Id* 16.

229 See J.V.J van Hoboken "Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines (2012) *Kluwer Law International* 350.

artistic purposes, and what is deemed to be in the 'public interest'. This is important to differentiate information publicized for journalistic purpose and information published by a blogger which does not fall under the category of journalistic purpose. This will also enable data subject to predict whether their request or wish qualifies as a legitimate request that will be honoured.[230]

230 See J.V.J van Hoboken "Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines (2012) *Kluwer Law International* 350.

# CHAPTER 5: CONCLUSION

The foundations of the "right to be forgotten, erasure or delete" is centred on ensuring that persons have control over their personal information.[231] This is relevant in the digital era which has enabled large amounts of information to be retained indefinitely through automated means. The interpretation of applicable sections in the repealed Directive, GDPR, POPI Act as well as the earlier case of *Google Spain SL* revealed some gaps or drawbacks that must be addressed to implement this right effectively and adequately.[232]

Having regard to the challenges that have been presented throughout this paper in the exercise of the "right to be forgotten" in the European Union context and possible interpretation issues in the POPIA, it is important that South Africa considers and pro-actively deal with these imminent issues as they are bound to be experienced in the application of the "right to delete".

The current regulatory framework is insufficient to enable the effective implementation of the "right to delete" in South Africa. As such, it is recommended that the Information Regulator delineate extensively through regulations:

a) what constitute the "right to delete" from a technical perspective, and the extent to which this right must be implemented;
b) how to assess adequacy, relevancy, accuracy of information and under what circumstance those requirements will be met;
c) to what extent should responsible parties inform downward consumers of information and under what circumstances the responsible parties need to notify original publishers of the information to ensure that all rights in the value chain are considered;

---

231 *Supra* at Chapter 2, par 2.2.1.

232 *Id.*

d) what constitute journalistic, literary, and artistic purposes, and what is deemed to be in the 'public interest'.

These are critical factors in the implementation of this right, without the standard each responsible party will have to define what the right to delete mean. This will result in inconsistency in the application of the law.[233]

Additionally, there must be a strengthened regulatory oversight in respect of "right to delete" requests. There must be an obligation by entities to report deletion request similarly to how responsible parties are required to report on "access requests".[234] The reporting must cover which requests were granted, denied, internal appeals and the basis of such decisions. This is not only important to the data subjects, but also critical for the Information Regulator to ensure that proper balance is being struck by entities in its assessment of whether to give effect to the right to delete. [235]

The right to delete in the context of data privacy is new in SA,[236] and there are no easy solutions to these issues. The recommendations provided in this paper are by no means conclusive, but they will provide a standard within which this right can be exercised consistently and uniformly by all responsible parties to ensure that it is respected, promoted, and maintained.

---

233 *Supra* at Chapter 4, par 4.3.

234 Section 6.3. of the *Guidelines on the Registration of Information Officers, 2021.* The requirement obligates the Information Officers of private and public entity to annually report to the Regulator: the number of access requests received, granted, denied, internal appeals lodged with the authority and those lodged to a court.

235 *Id.*

236 *Supra* at Chapter 1 par 1.2.1.

# BIBLIOGRAPHY

## BOOKS


- Alan F. Westin and Michael A. Baker (1972) *Databanks in a free society* Times Books
- De Stadler E, Esselaar P (2015) *A Guide to the Protection of Personal Information Act* Juta.
- Mayer-Schonberger V. (2009) *Delete: The virtue of forgetting in the digital Age* Princeton and Oxford: Princeton University Press.
- Papadopoulos S and Snail S (2012) *Cyberlaw @ SA III: The law of the internet in South Africa* 3rd edition Van Schaik Publishers.
- Solove J.D. (2007) The Future of Reputation: Gossip, Rumor, and Privacy on the Internet Yale University Press.
- De Terwangne C. (2013) *The Right to be Forgotten and the Informational Autonomy in the Digital Environment* Publications Office of the European Union, Available from http://dx.doi.org/10.2788/54562 (accessed on 20 August 2020)
- Van der Merwe DP, Roos A, Eiselen S, and Nel S (2016) *Information and Communications Technology Law* 2nd Edition LexisNexis: South Africa.


## JOURNAL ARTICLES


- Ahmed F “Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm” (2015) 21 (6) *Computer and Telecommunications Law Review* 44.
- Alessi S “Eternal Sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation” 2017 32 (1) *Emory International Law Review* 145.
- Ausloos J "The ‘Right to be Forgotten’ — Worth remembering?" (2012) 28(2) Computer Law & Security Review 144

- Ausloos J and Kuczerawy A "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling" (2016) 14(2) *Colorado Technology Law Journal* 219.
- Bernal P.A. "A Right to Delete?" (2011) 2 *European Journal of Law and Technology* 2.
- Cofone I "Google v. Spain: A Right To Be Forgotten?" (2015) 15 *Chicago-Kent Journal of International and Comparative Law* 10.
- D van der Merwe "A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda" (2014) 17 *Potchefstroom Electronic Law Journal (PELJ)* 1.
- Druschel P, Backes M, Tirtea R. "The right to be forgotten – between expectations and practice" (2011) 3 European *Network and Information Security Agency (ENISA)*1.
- Dulong de Rosnay M. and Guadamuz A. "Memory Hole or Right to Delist? Implications of the right to be forgotten on web archiving" (2017) 6 *RESET* ISSN 2264-6221.
- Frantziou E. "Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos" (2014) 14 Issue 4 *Human Rights Law Review* 761.
- Graux H, Ausloos J. and Valcke P. "The Right to be Forgotten in the Internet Era" (2012) 11 *Interdisciplinary Centre for Law and ICT*.
- J.V.J van Hoboken "Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines(2012) *Kluwer Law International* 350.
- Kelly-Louw M. "The 2014 credit-information amnesty regulations: What do they really entail?" (2015) 48 *De Jure* 92.
- Neethling J. "Personality rights: a comparative overview" (2005) 38 *Comparative and International Law Journal of Southern Africa* 210.

- Rolf H.W "The Right to Be Forgotten: More Than a Pandora's Box?" (2011) 2 Journal of Intellectual Property Information Technology and Electronic Commerce Law 120.
- Singleton S. "Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v AEPD" (2015) 44 *GA.J.INT'L COMP.L.* 165.
- Venter R. "The role of freedom of expression in a democratic system (part 1)" (2018) 1 Tydskrif vir Suid Afrikaanse Reg (TSAR) 52.
- Wickramasinghe S. "The Oblivious Oblivion: A Critique on the EUCJ's Right to Be Forgotten" (2015) https://ssrn.com/abstract=2782746 [Accessed on 15 August 2020].
- Xanthoulis N. "The right to Oblivion in the Information Age: A Human Rights Based Approach" (2013) 10 US-China Law Review 84.


## ACADEMIC DISSERTATIONS AND THESES


- Ambrose, M. L. (2013) *Digital Oblivion: The Right to be Forgotten in the Internet Age,* University of Colorado Boulder, Alliance for Technology, Learning and Society (ATLAS) Institute. Available from https://scholar.colorado.edu/concern/graduate_thesis_or_dissertations/0v8380833


## ACTS OF PARLIAMENT

### *South Africa*


- Constitution of South Africa Act 106 of 1996.
- Criminal Procedure Act 51 of 1977.
- National Credit Act 34 of 2005.
- Protection of Personal Information Act 4 of 2013.
- Promotion of Access to Information Act 2 of 2000.

- Regulation 3(d) of the 2014 Amnesty Regulations.

***International***

- 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.
- Regulation 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 (General Data Protection Regulation).

## OFFICIAL PUBLICATIONS AND RESEARCH REPORTS

- Article 19 Working Party Guidelines on the implementation of the court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12, 14/EN WP 225 (Adopted on 26 November 2014).
- Article 19 Policy Brief, The right to be forgotten: Remembering freedom of expression (2016) ISBN: 978-1-910793-33-6.
- De Terwangne C. (2013) The Right to be Forgotten and the Informational Autonomy in the Digital Environment Publications Office of the European Union, Available from http://dx.doi.org/10.2788/54562 (accessed on 20 August 2020)
- Guidance Note on Information Officers and Deputy Information Officers, 1 April 2021
- Guidelines on the Implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" (2014) Article 29 Data Protection Working Party.
- Guide to General Data Protection Regulation, UK Information Commission Office (ICO) https://ico.org.uk/for-organisations/guide-to-data protection/guide to-the-

general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#ib [Accessed on 24 October 2020].

- Interpol "African CyberThreat Assessment Report Key Insight into Cybercrime in Africa", October 2021.
- OECD "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] available at http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm
- Opinion of Advocate General JÄÄSKINEN delivered on 25 June 2013 Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protection de Datos (AEPD) Mario Costeja González (Reference for a preliminary ruling from the Audiencia Nacional (Spain).
- The South African Law Reform Commission Discussion Paper 109 Project 124 October (2005) Privacy and Data Protection, ISBN 0-621-36326-X.

## CASE LAW

### *South African*

- Argus Printing and Publishing Company Ltd. and Others v Esselen Estate (447/92) [1993] ZASCA 205; 1994 (2) SA 1 (AD); [1994] 2 All SA 160 (A) (7 December 1993).
- Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others (25978/2017) [2019] ZAGPPHC 384; [2019] 4 All SA 343 (GP); 2020 (1) SA 90 (GP); 2020 (1) SACR 139 (GP) (16 September 2019).
- Bernstein v Bester 1996 (2) SA 751 (CC).
- Government of the Republic of South Africa v Sunday Times Newspaper 1995 (2) SA 221(T).
- Johncom Media Investments Limited v M and Others (CCT 08/08) [2009] ZACC 5; 2009 (4) SA 7 (CC); 2009 (8) BCLR 751 (CC) (17 March 2009).

- Khumalo v Holomisa CCT 53/01 [2002] ZACC 12; 2002 (5) SA 401 (CC); 2002 (8) BCLR 771 (CC).
- Magadze v ADCAP, Ndlovu v Koekemoer (57186/2016) [2016] ZAGPPHC 1115 (2 November 2016).
- Midi Television (Pty) Ltd v Director of Public Prosecutions (Western Cape) [2007] ZASCA 56; 2007 (5) SA 540 (SCA); 2007 (9) BCLR 958 (SCA).
- National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others (CCT11/98) [1998] ZACC 15; 1999 (1) SA 6; 1998 (12) BCLR 1517 (9 October 1998).
- South African National Defence Union v Minister of Defence and Another 1999 (6) BCLR 615 (CC); 1999 (4) SA 469 (CC).

***International***

- Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez 2014, Case C-131/12, Court of Justice of the European Union (CJEU).
- Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) 2019, Case C 507/17, Court of Justice of the European Union (CJEU).


## INTERNET SOURCES


- Harvard School Business Online, Business Insights 'The advantages of data-driven decision-making', 26 August 2019, https://online.hbs.edu/blog/post/data-driven-decision-making [accessed on 17 August 2020].
- OHIO University 'Difference between Predictive and Prescriptive Analytics' https://onlinemasters.ohio.edu/blog/predictive-vs-prescriptive-analytics-whats-the-difference/, [accessed on 17 August 2020].

- Schultz J. ‘How Much Data is Created on the Internet Each Day?’ June 2019 https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/ [accessed on 20 September 2020].
- Sumit P., ‘Digital legacy: The fate of your online soul’ featured story on NewScientist 19 April 2011 on www.newscientist.com [accessed on 13 April 2020].
- The free dictionary https://www.thefreedictionary.com/Information-mining, [accessed on 20 August 2020].
- Expungement of a Criminal Record in terms of the Criminal Procedure Act, 1977 (Act 51 of 1997) https://www.justice.gov.za/expungements.html [accessed on 30 June 2020].