THE RIGHT TO BE FORGOTTEN:
A SOUTH AFRICAN PERSPECTIVE

by

André Stephan Basson
Student Number: 27537252

Submitted in partial fulfilment of the requirement for the degree LLM

In the Faculty of Law,
University of Pretoria

October 2015

Supervisor: Ms. Sylvia Papadopoulos

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Law

Annexure G

UNIVERSITY OF PRETORIA

Declaration of originality

This document must be signed and submitted with every essay, report, project, assignment, mini-dissertation, dissertation and/or thesis

Full names of Student: **André Stephan Basson**

Student Number: **27537252**

Declaration:

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

2. I declare that this mini-dissertation is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.

3. I have not used work previously produced by another student or any other person to hand in as my own.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature of student: _____

Signature of supervisor: _____

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Law

Annexure M

Submission form for mini-dissertation/dissertation/thesis

1. Personal details

Title: **Mr.** Student number: **27537252**

Surname: **Basson**

First names: **André Stephan**

2. Home/postal address:

87A Herbert Baker Street, Groenkloof, Pretoria, Postal Code: **0181**

Tel.: **073 481 4693** Cell no: **073 481 4693**

3. Work address: **N/A** Postal Code: **N/A**

4. Details of mini-dissertation/dissertation/thesis

Degree: **LLM (Coursework) in Mercantile Law**

Department: **Mercantile Law**

Supervisor: **Ms. Sylvia Papadopoulos**

Co-supervisor: **N/A**

5. Statement by candidate:

I declare that the mini-dissertation/dissertation/thesis, which I hereby submit for the abovementioned degree at the University of Pretoria, is my own work and has not previously been submitted by me for a degree at another university. Where secondary material is used, this has been carefully acknowledged and referenced in accordance with University requirements. I am aware of University policy and implications regarding plagiarism.

Signature: …… **Date**: ……..

6. Statement by supervisor:

I declare that I hereby approve that (full names of student) **André Stephan Basson**

may submit his/her mini-dissertation/dissertation/thesis as well as the prescribed summary.

The co-supervisor has agreed to the submission (if applicable).

…… ……..

Supervisor **Co-supervisor** (if applicable)

Date: …… **Date**: ……

This document should be submitted to:

For LLM Coursework and LLM Research: Rina Deetlefs;

LLD: Jeanne-Kay Goodale.

André Stephan Basson
27537252
MND800: SUMMARY OF MINI-DISSERTATION

THE RIGHT TO BE FORGOTTEN: A SOUTH AFRICAN PERSPECTIVE

The purpose of this Mini-Dissertation is to determine whether or not a data subject in South Africa can rely on the "Right to be Forgotten" (RTBF) as is illustrated in the case of *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González* (*Google SL*).[1] This involves, *inter alia*, a critical analysis of the European Law as well as the provisions of the Protection of Personal Information Act (POPI).[2] The Mini-Dissertation is structured as follows:

Chapter 1: Introduction:

Introduction, purpose and overview of the Mini-Dissertation.

Chapter 2: An Overview of the European Law:

An analysis of the relevant legislation and case-law of the European Union as well as its application to the RTBF.

Chapter 3: *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González:*

A detailed analysis of Judgment in *Google SL* as well as commentary and criticism to the RTBF.

Chapter 4: The "Right to be Forgotten" in South Africa:

A detailed analysis of the law pertaining to the protection of personal information in South Africa and the applicability of the RTBF in South Africa. This entails an investigation of the provisions of POPI as well as South African commentary to the RTBF.

Chapter 5:

Conclusion and recommendations.

[1] (Case C-131/12) Judgment of the Court of Justice of the European Union (Grand Chamber) of 13 May 2014.

[2] Act 4 of 2013.

TABLE OF CONTENTS:

CHAPTER 1

INTRODUCTION

In the modern era the most valuable commodity is neither oil nor nuclear power, it is information, and perhaps its most expensive element is the massive treasure trove of personal data that is stored online.[3]

The recent judgment in the case of *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González*[4] (*Google SL*) concerned, *inter alia*, whether or not there exists a "Right to be Forgotten" (RTBF). The question surrounding the RTBF is whether or not a person has the right to request that certain personal information, or links thereto, pertaining to him/her be removed or erased based on the wish of that person to consign that information to oblivion. There are many further aspects to this question which will be discussed in detail throughout this dissertation.

This dissertation will investigate, in particular, whether the RTBF should find application in South African law. This evaluation will begin with the source of the right and consequently involve an overview of the European law[5] as well as a critical analysis of the judgment of the Court of Justice of the European Union (CJEU) in *Google SL*.[6] Thereafter the South African perspective will be investigated to determine whether the RTBF should find application in South Africa.[7]

The judgment in *Google SL* has far reaching implications regarding the RTBF which will without a doubt also affect South Africans in one way or another.

---

3 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 175.

4 (Case C-131/12) judgment of the CJEU (Grand Chamber) of 13 May 2014.

5 Chapter 2.

6 Chapter 3.

7 Chapter 4.

The predicament Mr. González found himself in, which is explained herein below, is not one which would be unique to individuals living in Spain or the EU but could relate to anyone, anywhere.

In our modern era where information is power, our personal information is continuously harvested. The methods used to obtain our personal information, which are often unscrupulous, include: viruses; trojan horses; spyware programs; hacking; spoofing, webpages; e-mails; subscriptions; action tags; cookies and data logging.[8] Other risks are also present in that the data so harvested may be inaccurate, incomplete, irrelevant, disclosed without authorisation, used for other purposes than initially intended or unlawfully destroyed, to name but a few.[9]

The right to freedom of expression and the right to access to information are encroaching ever further on our fundamental right to privacy. In this war between rights one has to ask whether South Africans can turn to the RTBF to provide some reprieve in this ever present battle.

[8] Papadopoulos et al *Cyberlaw@SA III* 3rd edition (2012) 292 – 294.
[9] Van der Merwe et al *Information and Communications Technology Law* (2008) 314.

CHAPTER 2

AN OVERVIEW OF THE EUROPEAN LAW

I. INTRODUCTION

The question of whether a person has the RTBF has not yet been directly pronounced upon by South African Courts. We must therefore turn to the judgment in *Google SL* and the European Union (EU) law surrounding it for guidance and to place us in a position to draw a meaningful comparison to South African Law.

Attorney General (AG) Jääskinen makes the point that even as early as 1890 there was a fear that the development in technology poses a threat to our right to privacy.[10] In those days it was the rise of instantaneous photographs and the proliferation of the newspaper industry.[11] In the modern era this effect has been amplified and is even more concerning than before.

The fundamental right to privacy is enshrined in Section 14 of the Bill of Rights of the Constitution of the Republic of South Africa[12] (the Constitution). Section 39(1) of the Constitution provides that: "…*When interpreting the Bill of Rights, a court, tribunal or forum- (b) must consider international law; and (c) may consider foreign law*." It is for this reason that a critical discussion of the judgment in *Google SL* and the EU law applicable is to be discussed.

Before the judgment in *Google SL* is investigated it is necessary to discuss the law as it stands in the EU surrounding data protection and privacy. The starting point in this investigation should be with the legislation which is applicable in the EU.

10 Par 1 of AG Jääskinen's opinion delivered on 25 June 2013 (Case C-131/12).
11 *Ibid*.
12 Act 108 of 1996.

II. EUROPEAN UNION LEGISLATION

Article 7 of the Charter of Fundamental Rights of the European Union[13] (the Charter), with the title "*Respect for private and family life*", reads as follows:

> "…*Everyone has the right to respect for his or her private and family life, home and communications*…"

"*Protection of personal data*" is provided for in Article 8 of the Charter and reads as follows:

> "…*1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access of data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority*…"

Of further significance is Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[14] (the Convention) which is headed "*Right to respect for private and family life*" and reads as follows:

> "…*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime,*

[13] 2000/C 346/01.
[14] Rome, 4.XI.1950 (Signed in Rome on 4 November 1950).

for the protection of health or morals, or for the protection of the rights and freedoms of others..."

The 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[15] (the Directive) will be of paramount importance to this discussion. AG Jääskinen points out that in the modern age almost any person who utilizes a smartphone or computer could potentially be engaged in activities on the internet which the Directive could apply to[16] and thus the Directive is extremely important. AG Jääskinen advocates that, although the Directive has a wide scope of application, it was not foreseen at the time it was developed that there would be such explosive development with the internet.[17] It appears therefore that the Directive may apply in some instances where it would not have been the legislator's intention for it to do so, and this may give rise to practical problems.

The preamble to the Directive encompasses many important principles that apply to the processing of personal information and in many respects mirrors the legislation applicable in South Africa, as is demonstrated herein below. Some of the most important principles can be briefly summarised as follows: Data-processing systems are there to serve people and must respect their fundamental rights, in particular the right to privacy.[18] Personal data should be able to flow freely while still safeguarding the individual's rights.[19] The Directive furthermore advocates for free flow of data by equalising the rights of individuals in all Member States.[20] The Directive seeks to ensure a high level of protection in the European Community[21] and recognises that there is significant progress being made in information technology.[22]

---

15 OJ 1995 L 281, p.31.
16 Par 10 of his opinion in *Google SL*.
17 Par 26, 27 *id*.
18 Par 2 preamble to the Directive.
19 Par 3 *id.*
20 Par 8, 9 *id*.
21 Par 10 *id*.
22 Par 4, 14 *id*.

The law in force in a Member State will govern the processing of personal data where the processing is carried out under the responsibility of a controller who is established in a Member State.[23] The Directive explains the establishment of the territory of a Member State in this regard.[24] Importantly the issues of the lawfulness, fairness and rationale behind the processing of the data are addressed.[25] Exceptions apply in some instances, for example, in the literary or artistic fields or by virtue of the right to freedom of expression enshrined by Article 10 of the Convention or consent by the data subject.[26] The right of a data subject to access the information in order to identify the accuracy thereof and the lawfulness of the processing are also addressed.[27] Mention is made of the requirement to have a judicial remedy,[28] for the establishment in Member States of supervisory authorities[29] and provisions regarding when the Member states should have implemented the provisions of the Directive.[30]

The interpretation of certain of the provisions of the Directive was at issue in the case of *Google SL* and accordingly one has to examine those Articles referred to by the CJEU in more detail.

Article 2 of the Directive contains the definitions for the purposes of the Directive and naturally one must start with the definition of "personal data". "Personal data"[31] is defined in the Directive as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or*

23 Par 18 preamble to the Directive.
24 Par 19, 20 *id*.
25 Par 28 to 31 *id*.
26 Par 37, 58 *id*.
27 Par 41 *id*.
28 Par 55 *id*.
29 Par 62, 63, 64 *id*.
30 Par 69 *id*.
31 Art 2(a) of the Directive.

social identity." This definition is quite broad and would apply to a significant amount of data.

Article 2 also defines "processing of personal data" or "processing"[32] as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*" This definition includes the significant amount of conduct within the ambit of processing in order to give the data subject the most protection possible.

Article 2 also defines "controller"[33] as "*the natural or legal person, public authority, agency or any 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 processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*."

The Directive applies to the processing of personal data by automatic or other means should such data form part, or be intended to form part, of a filing system.[34] Member States are required to apply the national provisions it adopts pursuant to the processing of personal data,[35] such as the fact that controllers are compelled to comply with the national law of the territory of the Member State in which it is established.[36] The other instances Member States have to provide for are when international public law would bind it[37] and where the controller uses equipment

32 Art 2(b) of the Directive.
33 Art 2(d).
34 Art 3(a).
35 Art 4(1).
36 Art 4(1)(a).
37 Art 4(1)(b).

which is situated on the territory of the Member State, unless such equipment is used only for transit purposes.[38]

The Directive sets standards for data quality and requires that Member States ensure that personal data be: processed fairly and lawfully;[39] collected for specified and legitimate purposes while allowing for processing of data for historical, statistical or scientific purposes should safeguards be in place;[40] the personal data must furthermore be kept in a form which permits identification of data subjects for no longer than is necessary for its purpose[41] and the controller will be responsible for compliance with the data quality requirements as set out above.[42]

The Directive requires that personal data may only be processed in instances where the data subject has unambiguously consented[43] or the processing is necessary for the performance of a contract to which the data subject is a party or wishes to become a party[44] or if the processing is necessary for the compliance with a legal obligation to which the controller is a subject[45] or where it is necessary to protect the vital interests of the data subject[46] or necessary for the performance of a task which is in the public interest[47] or where the processing is necessary for purposes of legitimate interests pursued by the controller, except where such interests are trumped by the fundamental rights and freedoms of the data subject.[48]

Member States are obliged to provide for exemptions to the restrictions on the processing of personal information found in Chapters 2, 4 and 6 of the Directive in instances where such processing is carried out solely for journalistic or artistic or

38 Art 4(1)(b), (c) of the Directive.
39 Art 6(1)(a).
40 Art 6(1)(b).
41 Art 6(1)(e).
42 Art 6(2).
43 Art 7(a).
44 Art 7(b).
45 Art 7(c).
46 Art 7(d).
47 Art 7(e).
48 Art 7(f).

literary expression.[49] Of further significance is the right of a data subject to access the data, which right is guaranteed by the Directive.[50]

Special importance and emphasis should be placed on Article 12(b), Article 14(a) and Article 6(1) due to the fundamental role they played in the reasoning of the CJEU in the *Google SL* case with regards to the RTBF.

Article 12(b) states that "*Member States shall guarantee every data subject the right to obtain from the controller: (b) 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;*"

While Article 14(a) states that "*Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;*"[51]

Article 6(1) specifically requires that personal data must be adequate, relevant and not excessive in relation to its purpose[52] while also being accurate and kept up to date and, should this not be the case, such data is to be rectified or erased.[53]

Member States are to establish one or more public authorities tasked with monitoring the application, within its territory, of the provisions adopted by the Member State

49 Art 9 of the Directive.
50 Art 12.
51 See fn 47, 48 *supra* regarding Art 7(e) and (f).
52 Art 6(1)(c).
53 Art 6(1)(d).

pursuant to the Directive.[54] The Agencia Española de Protección de Datos (AEPD) is the supervisory authority in Spain where Mr. González initially laid his complaint. A supervisory authority in terms of Article 28 of the Directive has certain investigative powers to access data and to collect all the necessary information in performance of its duties.[55] The supervisory authority also has the power of intervention which includes, *inter alia*, the power to order the blocking, erasure or destruction of data.[56] The supervisory body is further tasked with hearing claims lodged by persons concerning the protection of his/her rights and freedoms with regard to the processing of personal information[57] and is competent to exercise, on the territory of its own Member State, the powers it is endowed with in terms of Article 28(3) of the Directive.[58]

III. CASE LAW

The European case law pronouncing on the interpretation of the rights and obligations contained in the Directive, the Convention or the Charter are naturally of importance to this dissertation. What follows is a brief discussion of some of the major decisions in the field and particularly those cases which the CJEU in *Google SL* rely on when coming to its conclusions.[59]

The procedure of the CJEU can be briefly summarised as follows: The CJEU may sit as a full court, in a Grand Chamber of 15 Judges or in Chambers of three or five Judges.[60] The role of the AG is to present, with complete impartiality and independence, an opinion in each case which is assigned to them.[61] The AG will deliver his/her opinion to the CJEU before the CJEU delivers its judgment

54 Art 28(1) of the Directive.
55 Art 28(3).
56 *Ibid*.
57 Art 28(4).
58 Art 28(6).
59 All judgments of the CJEU and opinions of the AGs referred to herein are freely available at www.curia.europa.eu. The judgments of the European Court of Human Rights (ECHR) are also freely available at www.hudoc.echr.coe.int/eng.
60 The composition of the CJEU is explained in full at http://curia.europa.eu/jcms/jcms/Jo2_7024/ (accessed 30 October 2015).
61 *Ibid.*

(accordingly the CJEU is not bound by the opinion of the AG).[62] The Judges deliberate on the basis of a draft judgment drawn up by the Judge-Rapporteur and decisions are taken by majority while no record is made public of dissenting opinions.[63]

Bodil Lindqvist

In the case of *Bodil Lindqvist*[64] the CJEU held that the act of referring on an internet page to various persons and identifying them by name or by other means and the operation of loading personal data on an internet page must be considered to be the processing of personal data within the meaning of Article 3(1) of the Directive.[65]

The CJEU recognised that information on the internet can be accessed by an extremely large number of people living all over the world, at almost all times and by using simple equipment.[66] The case of *Bodil Lindqvist* perfectly illustrates the clash between the right to freedom of expression and the right to privacy.[67] The CJEU in *Bodil Lindqvist* concluded that the Directive does not in itself conflict with the general principles of freedom of expression, such as contained in Article 10 of the Convention wherein the right to freedom of expression is enshrined, but that it is for the national authorities to ensure that a fair balance between rights and interests is found.[68]

62 The composition of the CJEU is explained in full at http://curia.europa.eu/jcms/jcms/Jo2_7024/ (accessed 30 October 2015).
63 *Ibid.*
64 (Case C-101/01) judgment of the CJEU (Grand Chamber) of 6 November 2003.
65 Par 25, 27 *id*.
66 Par 58 *id*.
67 Par 86 *id*.
68 Par 90 *id*.

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy

The matter of *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy*[69] involved finding the balance between data protection and freedom of the expression, in particular of the media, and hence the relevance to the focus of this dissertation.[70]

Of significance to the *Google SL* case, the question was discussed as to whether the Directive is to be interpreted as meaning that personal data containing material which has already been published in the media falls outside its scope.[71] In this regard the CJEU notes that this processing is not excluded by the Directive and falls within its ambit.[72] The CJEU found that a general derogation from the application of the Directive in respect of published information would largely deprive the Directive of its effect.[73]

L'Oréal SA & 3 Others v eBay International AG & 9 Others

In the matter of *L'Oréal SA & 3 Others v eBay International AG & 9 Others*[74] AG Jääskinen opined that the "effects doctrine" implies that conduct outside the territory of the EU, but which directly produces legally relevant effects on the subject-matter of EU legislation, cannot fall outside the ambit of application of EU legislation just because the conduct causing such effects takes place outside the Union territory.[75]

This doctrine has to be qualified otherwise, due to the ubiquitous nature of the internet, an array of legislation from all around the world would apply simultaneously, which is untenable.[76] This approach was accepted by the CJEU.[77] This principle is applied by the CJEU in the *Google SL* case.

---

69 (Case C-73/07) judgment of the CJEU (Grand Chamber) of 16 December 2008.
70 Par 1, 43 of AG Kokott's opinion delivered on 8 May 2008 (Case C-73/07).
71 Par 33 of the judgment (Case C-73/07).
72 Par 49 *id*.
73 Par 48 *id*.
74 (Case C-324/09) judgment of the CJEU (Grand Chamber) of 12 July 2011.
75 Par 125 of AG Jääskinen's opinion delivered on 9 December 2010 (Case C-324/09).
76 Par 126 *id*.
77 Par 61, 62, 63 of the judgment (Case C-324/09).

ASNEF & FECEMD v Administración del Estado

The direct effect of Article 7(f) of the Directive was at issue in the joined cases of *ASNEF & FECEMD v Administración del Estado.*[78] The CJEU found that Article 7(f) of the Directive sets out two requirements that must be met before the processing of personal data is lawful: firstly, the processing must be necessary for the purposes of the legitimate interests pursued by, *inter alia*, the controller and secondly such interest must not be overridden by the fundamental rights and freedoms of the data subject.[79] The CJEU noted that the second of these conditions involves a balancing of the opposing rights and interests which will depend on the circumstance of the case.[80] Significant to *Google SL* the CJEU stated that, when performing this balancing act, one can take into consideration the fact that where data is already contained in public sources it may not be as serious an infringement as when such data is "non-public" and is thereafter made known.[81]

Times Newspapers LTD (Nos.1 and 2) v The United Kingdom

In the case of *Times Newspapers LTD (Nos.1 and 2) v The United Kingdom*[82] the Court noted the importance of the press who are saddled with the task of imparting information and ideas, but also the right of the public to receive those ideas, and in so doing fulfilling its vital role as the public's watchdog.[83] The Court also noted the substantial importance of internet archives to preserving and making available news and information because such archives constitute an important source of education and historical research, which is readily accessible to the public and is normally free.[84] The Court however noted that more care should be taken when considering news archives of past events as opposed to current affairs as there is no urgency in publishing historical articles.[85]

---

78 (Cases C-468/10 and C-469/10) judgment of the CJEU (Third Chamber) of 24 November 2011.
79 Par 38 *id*.
80 Par 40 *id*.
81 Par 44, 45 *id*.
82 (Application Numbers 3002/03 and 23676/03) judgment of the ECHR (Fourth Section) of 10 March 2009.
83 Par 40 *id*.
84 Par 45 *id*.
85 *Ibid*.

Aleksey Ovchinnikov v Russia

In the case of *Aleksey Ovchinnikov v Russia*[86] the Court noted that in certain instances a limitation on the reproducing of information that has already entered the public domain may be justified, for example to prevent further airing of the details of an individual's private life which do not come within the scope of any political or public debate on a matter of general importance.[87]

IV. CONCLUSION

What is particularly striking in light of the legislation and case law discussed is the almost supreme importance given to the right to privacy and the stringent requirements to the processing of personal data. Another common theme seems to be the unforeseen implications of the legislation due to the blistering pace at which technology is advancing.

It appears that the legislator has attempted to pre-empt this by creating broad encompassing definitions of, *inter alia*, "personal data", "processing of personal data or processing" and "controller". One can appreciate the need for this approach because it is becoming increasingly difficult to protect our right to privacy.

The aforementioned approach does, however, become problematic because it inevitably entails the clashing of rights. Freedom of expression and the interests of the public in accessing information, to name a few, can be just as important as the right to privacy of the data subject. This will depend on the circumstances and involves the weighing of rights, which can be more complex than it appears.

A great amount of emphasis is placed on the application and interpretation of the Directive. It is therefore important to take cognisance of the fact that the EU has already identified, in the General Data Protection Regulation (GDPR), that the

86 (Application Number 24061/04) judgment of the ECHR (First Section) of 16 December 2010.
87 Par 50 *id*.

Directive will have to be re-evaluated and replaced due to developments in information technology.[88] The GDPR specifically seeks to provide for the RTBF and lays down requirements for the application thereof.[89]

The GDPR does however provide for exceptions to the erasure of data due to the application of the RTBF.[90] The exceptions include the following: (i) for the exercise of the right to freedom of expression and information; (ii) for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority; (iii) for reasons of public interest in the area of public health; (iv) for archiving purposes in the public interest or for scientific, statistical and historical purposes; (v) for compliance with a legal obligation to retain the personal data.[91]

It is clear therefore that the EU is actively attempting to regulate the RTBF and its proactive approach will in all likelihood create more certainty regarding the application of the RTBF. It will almost certainly have a ripple effect worldwide. It is therefore critical for South African Courts to carefully scrutinise the EU developments in this field.

88 Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) 2012/001 (COD) 9565/15 of 11 June 2015 pg 1, 2.

89 Art 17 pg 100, 101, 102 *id.*

90 Art 17(3) pg 101, 102 *id.*

91 *Ibid.*

CHAPTER 3

Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González

I. INTRODUCTION

A critical analysis of the judgment in the case of *Google SL* is of paramount importance when considering the question of whether one does have the RTBF. The arguments in favour and against the RTBF are particularly significant to note as these arguments are not just relevant to the EU, they have universal application and are important to keep in mind when we move on to a discussion of a South African perspective. The CJEU in *Google SL* is not faced with just this question but with many others which include territorial implications and how previous publication affects future publication. These concepts are interwoven to the main relief sought by Mr. González and will in all likelihood manifest in most instances of people approaching a Court for similar relief. Accordingly one has to evaluate the judgment in its entirety to get a proper perspective of how the RTBF should be applied, if it is applied at all.

II. THE FACTS

Essentially the facts at issue in the case of *Google SL* are as follows: On the 5th of March 2010 Mr. González lodged a complaint at the Agencia Española de Protección de Datos (AEPD).[92] The complaint was lodged against a newspaper publisher (La Vanguardia Ediciones SL), against Google Spain SL and against Google Inc.[93]

Mr. González is a Spanish national residing in Spain and his complaint concerned the fact that if one were to enter his name in the Google search engine one would obtain links to two pages of La Vanguardia's newspaper, of 19 January 1998 and of 9 March 1998.[94] The newspaper articles contain real-estate auction announcements

92 Par 14 of the judgment in *Google SL.*
93 *Ibid.*
94 *Ibid.*

pursuant to attachment proceedings for the recovery of social security debts which Mr. González owed and the article mentions Mr. González by name as the debtor.[95]

Mr. González felt aggrieved due to the fact that the attachment proceedings were fully resolved for numerous years and that the reference to such proceedings was now completely irrelevant. He therefore sought from the AEPD to compel La Vanguardia to remove or alter those pages containing his personal data, alternatively to use tools to protect the personal data.[96] He furthermore requested that Google Spain SL or Google Inc. be required to remove or conceal the personal data relating to him so that they no longer appeared on search results or links to La Vangaurdia.[97]

The AEPD however rejected his complaint against La Vanguardia, reasoning that the publication of the information was legally justified as it took place upon the order of the Ministry of Labour and Social Affairs and was intended to make the auction as effective as possible.[98] The complaint against Google Spain SL and Google Inc. was upheld however, and the AEPD reasoned that operators of search engines are subject to data protection legislation due to the fact that they engage in data processing for which they are responsible.[99] The AEPD further reasoned that it has the power to compel Google Spain SL and Google Inc. to withdraw the data and prohibit access to certain data by the operators of the search engine where the data concerned are liable to compromise the fundamental right to data protection and the dignity of persons.[100] The AEPD concluded that a search engine can be directly responsible without it being necessary to erase the data from the website where they appear.[101]

Google Spain SL and Google Inc. brought actions against the decision of the AEPD before the National High Court of Spain, Audiencia Nacional.[102] The Audiencia Nacional decided to stay the proceedings before it and to refer questions to the

95 Par 14 of the judgment in *Google SL*.
96 Par 15 *id*.
97 *Ibid*.
98 Par 16 *id*.
99 Par 17 *id*.
100 *Ibid*.
101 *Ibid*.
102 Par 18 *id*.

CJEU for a preliminary ruling.[103] The request for the preliminary ruling concerned the interpretation of Article 2(b), Article 2(d), Article 4(1)(a), Article 12(b) and Article 14(a) of the Directive and Article 8 of the Charter.[104]

III. JUDGMENT OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

The CJEU summarised the EU law[105] with particular reference to the definitions of "personal data", "processing of personal data" and "controller."[106]

The CJEU explained that search engines, such as Google, find information on the internet published by third parties and thereafter index it automatically, store it temporarily and then make it available to internet users in a particular order of preference.[107] One of the questions referred to the CJEU is whether Article 2(b) of the Directive is to be interpreted as meaning that this activity of a search engine is "processing of personal data" within the meaning of the Directive when that information contains personal data.[108] If this is the case, then is the operator of the search engine the "controller" in respect of that processing of personal information in terms of Article 2(d) of the Directive.[109]

Google Spain and Google Inc. argued that this cannot be the case because they, as search engines, process all information available on the internet without effecting a selection between personal data and other information.[110] They furthermore argued that they cannot be regarded as the "controller" because they have no knowledge of the data and that they do not control the data.[111]

The CJEU, having regard to the definition of "processing of personal data" in terms of the provisions of Article 2(b) of the Directive, then also referred to the principle enunciated in *Bodil Lindqvist* that the mere loading of personal information on an internet page is considered to be "processing of personal data" within the meaning of

103 Par 20 of the judgment in *Google SL*.
104 Par 1 *id*.
105 Par 3 to 13 *id*.
106 Par 4 *id*.
107 Par 21 *id*.
108 *Ibid*.
109 *Ibid*.
110 Par 22 *id*.
111 *Ibid*.

Article 2(b) of the Directive.[112] The parties in *Google SL* were *ad idem* that the data in question was indeed "personal data" within the meaning of Article 2(a) of the Directive[113] and the CJEU therefore held that in light of the activity which a search engine conducts, it must be considered as "processing of personal data", when it is indeed personal data in question.[114]

The CJEU applied the finding in *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy* by stating that the fact that data has already been published on the internet and was not altered by the search engine does not result in such an activity falling outside the scope of Article 2(b).[115] If this was not so then it would deprive the Directive in a large part of its effect.[116] The CJEU found that the operator of the search engine can be defined as the "controller" in respect of such processing carried out by the search engine because it is the search engine operator who determines the purposes and means of the processing of the personal data and therefore the search engine falls squarely within the ambit of the definition of a "controller" as is found in Article 2(d) of the Directive.[117] AG Jääskinen was however of the opinion that normally the search engine is merely an information location tool and does not exercise control over the personal data on a third party's web pages.[118] AG Jääskinen reasoned that there should be a line drawn between the entirely passive and intermediary functions of a search engine and the situation where the activity undertaken represents real control over the personal data processed.[119] AG Jääskinen concluded that national data protection authorities cannot require a search engine to withdraw information from its indexes (except in instances where the search engine has not complied with exclusion codes or where a request from a website regarding the update of cache memory has not been complied with).[120]

AG Jääskinen's opinion was that a search engine does process personal data in the sense of Article 2(b) of the Directive but that the search engine should not be

112 Par 25, 26 of the judgment in *Google SL.*
113 Par 27 *id*.
114 Par 28 *id*.
115 Par 29, 30 *id*.
116 Par 30 *id*.
117 Par 32, 33 *id*.
118 Par 84 of his opinion in *Google SL*.
119 Par 85 *id*.
120 Par 99 *id*.

considered as the "controller" of the processing in the sense of Article 2(d) of the Directive, except for a few exceptions.[121] The CJEU, however, concluded that a search engine can be regarded as the "controller" and is therefore burdened by the responsibilities imposed by the Directive and must comply therewith.[122] Significantly, the CJEU identified the fact that the activity of a search engine plays a decisive role in the dissemination of data.[123] Search engines render data accessible to a plethora of internet users who can merely enter a data subject's name into a search engine, such as the name of Mr. González, and are able to compile a detailed profile on such a person.[124] Those internet users would in all likelihood not have found the web page on which the data was initially published had it not been for the activities of a search engine.[125]

The CJEU concluded that Article 2(b), defining "processing", and Article 2(d), defining "controller", are to be interpreted as meaning that the activity of a search engine must be classified as "processing of personal data" and that the search engine is considered as the "controller" in respect of that information.[126]

The CJEU was also tasked to establish whether it is possible to apply national legislation transposing the Directive in instances such as those in question,[127] particularly whether Article 4(1)(a) of the Directive is to be interpreted as meaning that processing of personal data is carried out in the context of activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when certain conditions are met.[128]

Google Search is ubiquitous worldwide in various languages and is particularly widely used in Spain.[129] Google Search is operated by Google Inc. which is situated in the United States of America and makes its business through advertising.[130]

121 Par 100 of his opinion in *Google SL*.
122 Par 33, 38 of the judgment in *Google SL*.
123 Par 36 *id*.
124 Par 37 *id*.
125 Par 36 *id*.
126 Par 41 *id*.
127 Par 20, 42 *id*.
128 Par 45 *id*.
129 Par 43 *id*.
130 *Ibid*.

Google Spain however possesses its own legal personality and is situated in Madrid, Spain, and its activities are targeted at undertakings in Spain itself, while acting as commercial agent for Google Inc. in that Member State.[131]

The CJEU confirmed that the requirement for establishment is whether there is effective and real exercise of activity (the legal form of the establishment is not determinative).[132] The fact that Google Spain commands effective and real exercise of activity through stable arrangements in Spain and has legal personality made the CJEU not hesitate in finding that Google Spain is an "establishment" within the ambit of Article 4(1)(a) of the Directive.[133] The question of whether the processing of personal data by the controller is carried out in the context of the activities of the establishment could also not be evaded by Google because Article 4(1) of the Directive does not require that the processing of personal data be carried out "by" the establishment itself but only that it is carried out in the context of the activities of the establishment.[134]

The CJEU referred further to the doctrine of effectiveness, enunciated in the case of *L'Oréal SA & 3 Others v eBay International AG & 9 Others*. By application of this doctrine the CJEU held that the Directive must be interpreted in light of its objectives of ensuring effective and complete protection of fundamental rights and cannot be interpreted restrictively.[135] The CJEU, by considering the objectives of the Directive and the wording of Article 4(1)(a), found that the processing of personal data by a search engine, which is operated by an undertaking that is situated in a third State but has an establishment in a Member State, is subject to the Directive.[136] This is due to, *inter alia*, the fact that activities of the operator of the search engine and those of its establishment in the Member State are inextricably linked.[137]

The CJEU also had to determine whether Article 12(b) and 14(a) of the Directive are to be interpreted as meaning that a search engine is compelled to remove from its

131 Par 43 of the judgment in *Google SL*.
132 Par 48 *id*.
133 Par 49 *id*.
134 Par 52 *id*.
135 Par 53 *id*.
136 Par 55 *id*.
137 Par 56 *id*.

list of search results, 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 prior to or simultaneously from those web pages, and even when its publication on those pages is lawful.[138] This question is closely intertwined to the RTBF and therefore many of the points made by the CJEU with regard to this question can equally apply to the RTBF.

Google argued that by virtue of the principle of proportionality any request seeking the removal of information must be addressed to the publisher of the website because it is that person who makes the information available to the public and who is in the best position to determine the validity of the request and can easily remove the information.[139] Mr. González and others argued that a search engine may be ordered to withdraw said information without having to first, or simultaneously, approach the publisher of the web page.[140] Mr. González and others argued that the lawfulness of the publication and the fact that it still appears on the web page has no effect on the duty imposed by the Directive on the search engine.[141]

The CJEU noted that, subject to the exceptions permitted in terms of Article 13 of the Directive, all processing of personal data must firstly comply with the principles relating to data quality in terms of Article 6 of the Directive and secondly with one of the criteria, listed in Article 7 of the Directive, for making data processing legitimate.[142]

Furthermore application of the case of *ASNEF & FECEMD v Administración del Estado* informed the CJEU that Article 7(f) of the Directive sets out two requirements that must be met before the processing of personal data is lawful: firstly, the processing must be necessary for the purposes of the legitimate interests pursued by, *inter alia*, the controller and secondly such interest must not be overridden by the fundamental rights and freedoms of the data subject.[143] The second requirement

138 Par 20, 62 of the judgment in *Google SL*.
139 Par 63 *id*.
140 Par 65 *id*.
141 *Ibid*.
142 Par 71 *id.*
143 Par 74 *id*.

involves a balancing of the opposing rights and interests which will depend on the circumstances of the case.[144]

Article 14(a) of the Directive is instructive in that Member States are to grant a data subject, at least in the instances mentioned in Articles 7(e) and 7(f) of the Directive, the right to object at any time on compelling and legitimate grounds relating to his/her particular circumstances, and thus where there is a justified objection the controller will be bound by it.[145]

The CJEU pointed out the serious potential impact on the fundamental right to privacy of a data subject when a search of his/her name is conducted in a search engine.[146] Such information would most likely not have been found by your average person had it not been for the easy access provided by the search engine, and allows for almost any person to do profiling of an individual and therefore may constitute a more significant interference with the data subject's fundamental right to privacy than the publication on a web page.[147] This effect is amplified by the important role played by the internet and search engines in our society.[148] This point resonated strongly in favour of Mr. González.

The CJEU stressed that infringements of fundamental rights cannot be justified purely on the economic interest of the search engine.[149] Of course the removal of links may impact on the legitimate interest of internet users and therefore a fair balance should be struck between that interest and the data subject's fundamental rights.[150] The CJEU pointed out that as a general rule the interests of the data subject in such instances override the interests of the internet users, but this may depend on the nature of the information in question as well as its sensitivity for the data subject's private life and on the interest of the public in having that information.[151] The balancing of the interests will naturally depend on the

144 Par 74 of the judgment in *Google SL*.
145 Par 76 *id*.
146 Par 80 *id*.
147 Par 80, 87 *id*.
148 Par 80 *id*.
149 Par 81 *id*.
150 *Ibid*.
151 *Ibid*.

circumstances of each case but saddling a private company with this task is, as is discussed herein below, not necessarily the best solution.

The CJEU concluded that the operator of a search engine may be ordered to remove from the list of results displayed following a search made on the basis of a person's name, links to a web page published by third parties and containing information relating to that person, without an order having to be made prior to or simultaneous to the removal of that name and information from the publisher's web page.[152]

The CJEU stated that a further practical reason exists for holding the search engine to account, being that information on a website can be easily replicated and in some instances the publishers are not subject to the law of the EU.[153] There may also be differences between the processing undertaken by the publisher and that undertaken by the search engine, for example the publisher may be exempted by Article 9 of the Directive if it carries out the processing for purely journalistic purposes while the search engine may not benefit from that exemption.[154] Furthermore, the legitimate interest in justifying the processing and the consequences of that processing may be different from the points of view of the publisher and that of the search engine.[155]

The focal point of this dissertation revolves around the scope of the RTBF. Before going any further, it is important to clarify that the RTBF does not, in the present case, imply that the information in question is to be removed. What is at issue is that the link to the information is to be removed or that so called "delisting" should take place.

The question posed by the CJEU in this regard is as follows:

> "*must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the*

152 Par 82, 88 of the judgment in *Google SL*.
153 Par 84 *id*.
154 Par 85 *id*.
155 Par 86 *id*.

information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?"[156]

Google and others argued that this should not be the case due to Article 12(b) and 14(a) of the Directive conferring rights on data subjects only where the processing is incompatible with the Directive or compelling grounds exist, more than the mere wish for the data to be forgotten.[157] Mr. González and others argued that the data subject may oppose the activity engaged in by the search engine because the fundamental rights to the protection of data and privacy will encompass the RTBF and the data subject's rights will override the interests of the search engine as well as the general interest in the freedom of information.[158]

AG Jääskinen was of the opinion that the Directive does not provide for a general RTBF but that in the instances of processing of data without the data subject's consent, one must compare the purposes of the processing and the interests served by it to those of the data subject.[159] In AG Jääskinen's opinion the subjective preference of the data subject alone does not amount to a compelling and legitimate ground within the meaning of Article 14(a) of the Directive.[160] AG Jääskinen was further of the opinion that if a search engine is found to be the responsible controller for the personal data on third party's web pages, then the service provider would have to put itself in the shoes of the publisher of the source web page and verify that the processing of the personal data in question is legal and legitimate in terms of the Directive.[161]

AG Jääskinen opined that the issues concerning whether there is a RTBF will be determined by interpretation of the legislation in place, such as the Directive and the

156 Par 20 subpar 3 of the judgment in *Google SL*.
157 Par 90 *id*.
158 Par 91 *id*.
159 Par 108 of his opinion in *Google SL*.
160 *Ibid*.
161 Par 109 *id*.

Charter, and will involve an argument surrounding the competing rights of, *inter alia*, the data subject on the one hand and the search engine on the other.[162] AG Jääskinen pointed out that another question which arises is whether there is a positive obligation on the EU and Member States to enforce, as against search engines, which are private subjects, a RTBF.[163] AG Jääskinen placed a high value to the right to information and refers in this regard to the case of *Times Newspapers LTD (Nos.1 and 2) v The United Kingdom* wherein it was held that internet archives make a substantial contribution to preserving and making available important information which has educational, historical and research qualities which are easily accessible to the public at a nominal or no fee at all.[164] AG Jääskinen did, however, concede that when striking a balance between the competing rights involved, it will favour the data subject when the news events are past events and not current events, such as in the case of Mr. González.[165] With reference to the case of *Aleksey Ovchinnikov v Russia*, AG Jääskinen stated that in certain circumstances the restriction on the reproducing of information that is already in the public domain may be justified and therefore the protection of one's private life can be invoked, in principle, even if the information concerned is already in the public domain.[166]

AG Jääskinen was of the opinion that in our modern society the right to search information via search engines is one of the most important means of exercising one's right to freedom of information and that an internet user's right to information would be jeopardised if a search for information regarding an individual did not generate a search result which indicates a truthful reflection of the relevant web pages but merely an edited version of the truth.[167] AG Jääskinen rejected the notion that the Directive makes provision for a RTBF and felt it would burden search engines with an obligation whereby they are required to remove legitimate and legal information which has entered into the public sphere.[168] AG Jääskinen further pointed out that it is unfair and perhaps impractical to expect a search engine to handle each request made by a data subject on a case-by-case manner because the

162 Par 119 of his opinion in *Google SL*.
163 *Ibid*.
164 Par 123 *id*.
165 *Ibid*.
166 Par 127 *id*.
167 Par 131 *id*.
168 Par 133 *id*.

likely result of such a request will either lead to automatic withdrawal of links or to an unmanageable number of requests referred to the search engine.[169] A further effect which may follow is an interference with the freedom of expression of the publisher whereby the information on his/her web page would effectively be censured due to a dispute between the search engine and the data subject.[170]

Mr. González further relied on the wording of Article 12(b) of the Directive read together with Article 6(1) of the Directive in his argument that the information relating to him has now become inadequate, irrelevant or excessive in light of the purposes of the processing, even though it may initially have been lawful, the course of time has rendered it incompatible with the Directive.[171]

The CJEU pointed out that in each case the processing of personal data must be authorised in terms of the provisions of Article 7 of the Directive for the entire period for which it is carried out.[172] The CJEU reasoned that when considering such a request it should be examined whether the data subject has the right that his personal information should, at this point in time, no longer be linked to his name by a list of results displayed following a search of his name.[173] The CJEU held that it is not necessary to show prejudice to the data subject in this regard.[174]

The CJEU therefore concluded that the fundamental rights under Articles 7 and 8 of the Charter override, as a rule, not only the economic interest of the operator of a search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name.[175] The CJEU however stated that it may not always be the case and that this will depend on the circumstances.[176] Circumstances the CJEU listed include the public role of the data subject or that the interference with the data subject's fundamental rights is justified on the grounds that

169 Par 133 of his opinion on *Google SL*.
170 Par 134 *id*.
171 Par 92, 93, 94 of the judgment in *Google SL.*
172 Par 95 *id*.
173 Par 96 *id*.
174 *Ibid.*
175 Par 97 *id*.
176 *Ibid.*

there is a preponderant interest of the public in having access to the information in question.[177]

The CJEU held that due to the fact that the information regarding the attachment proceedings for the recovery of social security debts being sensitive to the data subject's private life and furthermore the fact that the initial publication had taken place 16 years earlier, the data subject establishes a right that the information should no longer be linked to his name by means of such a list.[178] The CJEU found that there does not appear to be reasons substantiating a preponderant interest of the public in that information being displayed and therefore the data subject may, by virtue of Article 12(b) and 14(a) of the Directive, require those links to be removed from the list of results.[179]

IV. CONSEQUENCES AND CRITIQUE OF THE JUDGMENT

In an article published in *The Guardian*, Tippmann and Powles[180] quote some interesting statistics regarding the removal of links which are as a direct result of the judgment in *Google SL.* It is averred that less than 5% of the nearly 220 000 individual requests made to Google are to remove links related to information concerning criminals, politicians and high-profile figures.[181] It is furthermore averred that of the 218 320 requests to remove links between 29 May 2014 and 23 March 2015, 46% have been successfully delisted on individual name searches.[182]

The adoption and application of the RTBF is problematic in practice for many reasons, some of which are attributable to the ubiquitous nature of the internet and the ease at which information can be replicated.[183] Even if information is erased from one source, innumerable other websites, internet archives, cache copies and

177 Par 97 of the judgment in *Google SL*.
178 Par 98 *id*.
179 *Ibid*.
180 "Google accidentally reveals data on 'right to be forgotten' requests" dated the 14th of July 2015 and available at http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests (accessed 30 October 2015).
181 *Ibid.*
182 *Ibid.*
183 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 178.

abstracts produced by search engines still continue to provide the information in question.[184] It may even occur that, before a request for erasure has been made, the information in question has already been strewn all over the internet and may become nearly impossible to track down.[185] Another practical issue to consider is the "Streisand Effect" which denotes the phenomenon on the internet whereby an attempt to censor or remove information backfires, causing the information to be widely publicised.[186] This effect owes its name to Barbara Streisand's unsuccessful legal battle to censor publication of photos of her Malibu house, which only caused more internet publicity to be directed at her private life.[187] It appears that the fact that someone wants to remove information only means that people want to know about it even more.

A further phenomenon is occurring which follows, more or less, this scenario: a link to an online newspaper article is removed by Google due to a complaint by a data subject; Google informs the online newspaper of the link which is removed; the newspaper writes a new article which contains the information of the previous article but also about the fact that Google has removed the link to the previous article; this has the effect of drawing even more attention to the new article and thereby defeating the purpose of the removal in the first place.[188]

Cofone argues that the main problem with the judgment in *Google SL* is that the Court reasoned that the information indexed by Google was not relevant, which begs the question as to who decides what is relevant.[189] Cofone argues that if what is relevant is to be decided centrally by a Court then the rights to freedom of expression and access to information will suffer.[190] This is also because search

184 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 178.

185 *Ibid.*

186 Morozov E "Living with the Streisand Effect" dated 26 December 2008 *The New York Times* and available at http://www.nytimes.com/2008/12/26/opinion/26iht-edmorozov.1.18937733.html?_r=0 (accessed 30 October 2015).

187 *Ibid.*

188 Taibi C "How the EU's 'Right to be Forgotten' Rule is Backfiring Completely'" dated 22 July 2014 *The Huffington Post* and available at http://www.huffingtonpost.com/2014/07/22/right-to-be-forgotten-google-publishers-uk_n_5610803.html (accessed 30 October 2015).

189 Cofone I "Google v. Spain: A Right To Be Forgotten?" (2015) 15 *Chicago-Kent Journal of International and Comparative Law* 9.

190 Pg 9, 10 *id.*

engines function as intermediaries and it is ultimately the internet user who determines the results of a search and who then decides which web pages to read.[191] Ultimately if the information, say of Mr. González's past, appears at the top of a search result, it means that a large amount of internet users considered that information relevant.[192] Cofone further argues that it is not sound to reason on the one hand that the information should be kept online (due to the fact that it was legally published) but on the other hand reason that the information should be made inaccessible.[193]

Rosen is of the opinion that the RTBF constitutes the biggest threat to free speech on the internet in the coming decade.[194] Rosen argues that it is untenable to expect a data controller (like Facebook or Google) to engage in difficult line-drawing exercises previously performed by Courts.[195] Rosen reasons that the expected effect, in light of the extreme sanctions which may be levied against the data controller, is that the data controller may opt for deletion in ambiguous cases.[196] Ahmed is also of the opinion that it is impossible for Google (whose main function is not the adjudication of the RTBF requests) to neutrally and fairly adjudicate on the gargantuan amount of individual RTBF requests on the basis of the merits of each case.[197]

Ahmed identifies further stumbling blocks to the application of the RTBF in the form of the uncertainty prevailing around the definition of certain terms, such as when personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.[198] This is because there is not, according to Ahmed, a universal definition of "irrelevant" or "unnecessary data".[199] The same problem arises with the definition of in the "public interest", especially where the task

191 Cofone I "Google v. Spain: A Right To Be Forgotten?" (2015) 15 *Chicago-Kent Journal of International and Comparative Law* 10.
192 *Ibid*.
193 *Ibid.*
194 Rosen J "The Right to be Forgotten" (2012) 64 *Stanford Law Review Online* 88.
195 Pg 90 *id*.
196 Pg 90, 91 *id.*
197 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 180.
198 Pg 181 *id*.
199 *Ibid.*

of defining this is left to a private corporation.[200] Ahmed also points out that it is impossible to know, at the moment the link to the information is to be delisted or not, whether that information will be completely worthless and irrelevant in the future.[201]

Ahmed recommends that in order to ensure the proper implementation of the RTBF, a perfect balance must be struck between the individual's right to privacy (and the RTBF) and other fundamental rights (such as the right to freedom of expression and the public's right to know).[202] Ahmed further argues that a specialised neutral independent body should be established, empowered with the authority to regulate and monitor the implementation of the RTBF.[203] This independent body will be able to adjudicate on requests on their individual merits and take away the burden on the private data controllers (and not to mention provide greater legitimacy to the right by reducing the risk of censorship and exploitation of the RTBF).[204] Ahmed also suggests that three factors should be taken into account when considering a delisting and they are: the amount of time which has passed since publication; the impact of the public's ability to access the information on the data subject; and the relevance of the information to the public and the data subject.[205]

Gstrein is in favour of an approach whereby the RTBF is only a measure of last resort in cases where other less intrusive measures fail.[206] Gstrein proposes that there should be a change in the nature of some information networks from an open network to a closed one so that certain (more sensitive) information can be "closed up".[207] But as Gstrein himself points out, it may be difficult to determine which information systems should be designed to be open and which ones should be closed.[208]

---

200 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 182.

201 *Ibid.*

202 *Ibid*.

203 Pg 183 *id.*

204 *Ibid.*

205 *Ibid.*

206 Gstrein O "The Cascade of Decaying Information: Putting the 'Right to be Forgotten' in Perspective" (2015) 21(2) *Computer and Telecommunications Law Review* 44.

207 Pg 46, 46 *id*.

208 Pg 47 *id.*

Pursuant to the judgment in *Google SL*, Google invited independent experts to join an Advisory Council with the aim of providing advice to Google regarding the consequences of the *Google SL* judgment. The Advisory Council published a report called *The Advisory Council to Google on the Right to be Forgotten* (the Report).[209]

The experts were tasked to advise Google on performing the balancing act between an individual's right to privacy and the public's interest in access to information.[210] The Report points out that the effect of the judgment does not amount to a general RTBF but requires Google to remove links returned in search results based on an individual's name when those results are inadequate, irrelevant or no longer relevant, or excessive.[211] Google is not compelled to remove the results if there is an overriding public interest in them.[212] It is also pointed out that there are people who are able to perform more extensive searches who will still be able to find the information in question (since only the link to the information has been removed and not the information itself).[213]

The Report identifies four primary criteria which they advise Google to evaluate when considering delisting requests from data subjects.[214] The first criterion is the data subject's role in the public life;[215] the second criterion is the nature of the information involved;[216] the third criterion is the source of the information;[217] the fourth criterion is the time and how the effluxion of time relates to the information in question.[218] The Report goes further to explain procedural elements which will have to be in place in order to give effect to the judgment.[219] This involves the steps a data subject should take when requesting for the delisting of information[220] and the

209 Dated 6 February 2015 and available at https://www.google.com/advisorycouncil/ (accessed 30 October 2015).
210 Pg 1 of the Report.
211 Pg 3 *id*.
212 *Ibid.*
213 Pg 4 *id*.
214 Pg 7 *id*.
215 Pg 7, 8 *id*.
216 Pg 9 to 13 *id*.
217 Pg 13 *id*.
218 Pg 14 *id*.
219 Pg 15 *id*.
220 Pg 15, 16 *id*.

notifying of webmasters who published the information of a delisting.[221] Furthermore the Report suggests that procedures should be in place to challenge the decision to delist information[222] and that there should be an appropriate geographic scope for delisting.[223] The Report also suggests that Google should operate in a transparent manner when deciding whether or not to delist information.[224] Google has taken steps in order to attempt to give effect to the judgment.[225]

V. CONCLUSION

One has to sympathise to some extent with search engines, particularly Google, due to the immense consequences which the judgment in *Google SL* entails for them.

The criticism cited herein above against the judgment in *Google SL* pertaining to the RTBF is certainly not without merit. The CJEU and the AG assigned to the case could not even agree on the ambit of the RTBF. Even in light of all the criticism, should the CJEU have come to a different conclusion in light of the facts at hand and the provisions of the Directive? When a search was conducted on Mr. González's name the results were indeed, in the very least, no longer relevant and excessive. One of the problems therefore is that if the decision is applied on a large scale, the consequences are untenable and there simply is not a sound structure in place to ensure the proper implementation of the RTBF.

There is also a profound irony present in the aftermath of Mr. González's legal battle, which is the fact that if someone were to type his name into the Google search engine, they will be immediately referred to the judgment in *Google SL* which exposes the elements of his past which he so desperately wanted to have consigned to oblivion. Mr. González's legal battle was therefore not in his own interest but in the interest of many others in his position.

---

221 Pg 17 of the Report.
222 Pg 18 *id*.
223 Pg 18, 19, 20 *id*.
224 Pg 21 *id*.
225 By visiting https://support.google.com/legal/answer/3110420?hl=en a data subject is guided through the delisting process.

With the *Google SL* judgment causing states, even outside the EU, to reconsider their policy with regard to the RTBF, it remains to be determined how the judgment will influence the data subject in South Africa.

CHAPTER 4

THE "RIGHT TO BE FORGOTTEN" IN SOUTH AFRICA

I. INTRODUCTION

The question of whether the RTBF will find application in our law will involve, *inter alia*, an investigation of our law of privacy and protection of personal information. In South African law the first port of call when discussing the right to privacy is Section 14 of the Constitution which states that:

> "*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.*"

The right to privacy is also found in our common law and there are several enactments of legislation which provide for data protection. These include the Regulation of Interception of Communications and Provision of Communication-Related Information Act,[226] the Electronic Communications and Transactions Act,[227] the Interception and Monitoring Act,[228] the Promotion of Access to Information Act[229] and, perhaps of most importance to this dissertation, the Protection of Personal Information Act[230] (the POPI).

There are, without a doubt, many instances in South Africa which are analogous to the case of *Google SL* where personal information is processed and forms part of a list of search results which a data subject does not wish the internet user to see.

---

226 Act 70 of 2002.
227 Act 25 of 2002.
228 Act 127 of 1992.
229 Act 2 of 2000.
230 Act 4 of 2013.

A brief investigation of the nature and scope of the right to privacy in South Africa is a logical point of departure.

II. THE RIGHT TO PRIVACY

Neethling, in his doctoral thesis,[231] defined privacy as "*an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined should be excluded from the knowledge of outsiders and in respect of which there is a will that they be kept private.*" This definition of privacy was accepted, *inter alia*, in the case of *National Media Ltd and Another v Jooste.*[232]

The case of *Bernstein and Others v Bester and Others NO*[233] (*Bernstein*), is instructive in an investigation of the nature and scope of the constitutional right to privacy. The Court acknowledged that at common law the test to determine whether an infringement of privacy has occurred would involve a single enquiry, including an assessment of the lawfulness of the infringement of privacy, and it follows that a ground of justification would exclude the wrongfulness of an invasion of privacy.[234] The right to privacy is recognised by our common law as an independent right of personality.[235] In contrast to the common law test, the Court in *Bernstein* states that the test in terms of the Constitution constitutes a two-stage approach.[236] This entails firstly an investigation into whether or not a right has been infringed and secondly if such infringement was justified.[237] Put another way, what is required is that a person has a subjective expectation of privacy that society has recognised as objectively reasonable.[238]

The constitutional right to privacy is not absolute and is subject to limitation in terms of our law of general application[239] and has to be weighed against the rights of others. The Court makes reference to Article 8 of the Convention by noting that it

231 *Die Reg op Privaatheid* (UNISA 1976) pg 287.
232 1996 (3) SA 262 (A) pg 271.
233 1996 (2) SA 751 (CC).
234 Par 71, pg 790 *id*.
235 *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 (4) SA 376 (T).
236 Par 71, pg 790 of the judgment in *Bernstein*.
237 Par 57 to 59, pg 785, 786 *id*.
238 Papadopoulos et al *Cyberlaw@SA III* 3rd edition (2012) 278.
239 Sec 36 of the Constitution.

provides that the right to privacy may be limited only in accordance with the law and must be necessary in a democratic society.[240]

The Court in *Bernstein* notes[241] the two stage test constructed in the American case of *Katz v United States*[242] which dealt with a governmental invasion of a person's privacy. The Court in *Katz v United States* stated as follows: "*My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." "* The Court in *Bernstein* held that a sensible approach to the scope of a person's privacy would be to extend it only to those aspects in regard to which a legitimate expectation of privacy can be harboured.[243]

The Court in *Bernstein* further states that the nature of privacy relates only to the most personal aspects of a person's existence and must be viewed in relation to the rights of others.[244] This sentiment echoes the clash of rights at play in *Google SL*, being the rights of the data subject as opposed to, *inter alia*, the interest of the public in accessing the information as well as the interests of the publisher. It can therefore be said that the right to privacy lies along a continuum in which the more a person interacts with the world, the more the right to privacy becomes diluted.[245] Unfortunately in the modern age most individuals should realise that millions of little pieces of personal information concerning them are out there being processed by often nameless and faceless people intent on using such information for unknown purposes.[246]

Suppose a similar set of facts as that in *Google SL* take place in South Africa. By application of Neethling's definition, the data subject in question would argue that his/her personal information which has become public should be excluded from the

240 Par 72, pg 790 of the judgment in *Bernstein.*
241 Par 75, pg 792 *id*.
242 389 US 347 (1967) pg 361.
243 Par 75, pg 792 of the judgment in *Bernstein*.
244 Par 79, pg 795 *id*.
245 Papadopoulos S "Revisiting the Public Disclosure of Private Facts in Cyberworld" (2009) *Obiter* 37.
246 Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position" (2007) *SALJ* 401.

knowledge of outsiders and he/she has a will that the information should be kept private. The reason for this will of the data subject is however not because the initial publication was unlawful but that the data subject has the right to have such personal information to be consigned to oblivion.

The interpretation and application of the POPI will play a crucial role when considering RTBF from a South African context. Some of the relevant provisions of the POPI are now investigated.

III. THE PROTECTION OF PERSONAL INFORMATION ACT (THE POPI)

The South African Law Reform Commission[247] (the SALRC) identified a clear problem in our law regarding the lack of proper protection of the personality of the data subject by processing of personal information.[248] The SALRC identified the Directive as an instrument which was born from essentially the same problems faced by the Member States of the EU and relies on it in its argument for the implementation of a similar law in South Africa.[249] There was also an argument in favour of legislative reform due to the protection of personal information not being nearly sufficient, at that stage, when measured against international norms and standards.[250] It is clear that South African law borrowed quite liberally from the EU when drafting the POPI.

The POPI was assented to on the 19th of November 2013 and, in brief terms, the POPI exists in order to promote the protection of personal information and to introduce minimum requirements for the processing of personal information. The preamble of the POPI reiterates some of the findings of the SALRC and states that the right to privacy includes the right to protection against unlawful collection, retention, dissemination and use of personal information. Furthermore, the preamble notes that there is a need for the removal of unnecessary impediments to the free flow of information. The preamble further states that the POPI is necessary in order

247 SALRC Discussion paper 109, Project 124, October 2005.

248 Page 2, Chapter 1 *id*.

249 Pg 6, 7, 8, Chapter 1 and in particular par 1.2.22 *id*.

250 Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position" (2007) *SALJ* 433.

to regulate, in harmony with international standards, the processing of personal information in a manner that gives effect to the right to privacy subject to justifiable limitations imposed by competing rights.

The internet operates on the basis that information should be able to flow un-impeded over national borders and therefore the standards for the protection of personal information should be equivalent in all countries connected to the internet.[251] It appears that the South African legislature has taken cognisance of this and therefore attempts to align the provisions of the POPI to that which is internationally acceptable.

The purpose of the POPI is, *inter alia*, to give effect to the constitutional right to privacy by providing protection to personal information which is processed by a responsible party subject to ensuring that a balance is achieved between the right to privacy and the rights of others (specifically the right to access to information).[252] The POPI also serves to lay down minimum requirements for processing of personal information by establishing conditions which are in harmony with international standards.[253] It provides persons with rights and remedies to protect their personal information from wrongful processing[254] and establishes voluntary and compulsory measures to ensure compliance.[255] The POPI must be interpreted in a manner which gives effect to this purpose.[256]

In short the POPI applies to the processing of personal information which is entered into a record by or for a responsible party[257] where the responsible party is either domiciled in the Republic or makes use of automated or non-automated means within the Republic (unless those means are used only to forward personal

251 Van der Merwe et al *Information and Communications Technology Law* (2008) 320.
252 Sec 2(a).
253 Sec 2(b).
254 Sec 2(c).
255 Sec 2(d).
256 Sec 3(3)(a).
257 Sec 3(1)(a).

information through the Republic).[258] The POPI applies to the exclusion of other legislation which is inconsistent with it,[259] unless other legislation would provide more extensive rights.[260]

The purpose, application and interpretation of the POPI resemble many of the core elements and ideals that are encompassed in the Directive. This similarity, and other similarities which are discussed herein below, are of crucial importance when investigating the RTBF in a South African context. It is therefore necessary to critically investigate some of the definitions contained in the POPI.

A data subject "*means the person to whom personal information relates*."[261]

Personal information "*means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to…"*[262]

This definition is similar to the definition of "personal data" in the Directive and both definitions are broad in its scope.[263] The POPI however goes so far that it appears that almost all information could be construed to be personal information and the definition is not a closed list.

Processing "*means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –*

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

---

258 Sec 3(1)(b).
259 Sec 3(2)(a).
260 Sec 3(2)(b).
261 Sec 1.
262 Sec 1.
263 Although the definition of "personal data" in the Directive does not include juristic persons.

(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;"[264]

Once again there is a stark resemblance between this definition and that of "processing of personal data or processing" in terms of the Directive. This definition in terms of the POPI is once again wide in scope.

The responsible party "*means 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.*"[265]

This definition is similar to that of the definition of a "controller" in terms of the Directive.

The POPI furthermore lays down certain requirements for the lawful processing of personal information by a responsible party[266] and also requires there to be a specific and lawful purpose for the collection of personal information.[267] The POPI requires the responsible party to ensure that the requirements of the POPI are met[268] and that processing of personal information is done lawfully.[269] Furthermore, the processing of information must be done in a reasonable manner that does not infringe the privacy of the data subject[270] and the processing must be adequate, relevant and not excessive (the minimality principle).[271] The minimality principle is also to be found, in a similar form, in the Directive in Article 6(1). This strengthens

264 Sec 1.
265 Sec 1.
266 Sec 4.
267 Sec 13(1).
268 Sec 8.
269 Sec 9(a).
270 Sec 9(b).
271 Sec 10.

the argument in favour of the existence of the RTBF in South Africa due to the Court in *Google SL* relying in part on Article 6(1) when coming to its conclusion.

A search engine, like Google, falls within the ambit of the POPI in that they process personal information which is necessary for the pursuance of the legitimate interests of the responsible party or of a third party to whom the information is supplied (for example the internet user).[272]

What may also be a possible ground for arguing the existence of the RTBF in South Africa is that, in terms of Section 14(1) of the POPI, records of personal information may only be retained for a period necessary for achieving the purpose for which the information was collected unless certain exceptions apply.[273] The POPI further provides that a responsible party must take steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.[274] This is also relevant to the RTBF in South Africa.

Specific provisions apply to special personal information which would include information concerning, *inter alia,* religious beliefs, race or health.[275] It is possible for the Regulator to grant exemption to a responsible party in breach of a condition for the processing of the information in certain circumstances.[276] The POPI then also sets out the procedure regarding complaints to the Regulator, the action which must be taken upon receipt of such complaints as well as the powers of the Regulator.[277] Furthermore the POPI provides civil remedies which may be available against a responsible party[278] and also sets out an array of offences, penalties and administrative fines which may be levied in some instances.[279] These provisions will

272 Sec 11(1)(f).
273 As are listed in Sec 14(1)(a) to (d).
274 Sec 16(1).
275 Sec 26 to 35.
276 Sec 37(1).
277 Sec 74 to 82.
278 Sec 99.
279 Sec 100 to 109.

have to be analysed carefully when a data subject wishes to submit a complaint against a responsible party.

The POPI does not apply to the processing of information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.[280] In this regard it is noteworthy to mention that in *Google SL* the CJEU held that there may be a difference between a publisher and a search engine in that a search engine may not benefit from the protection afforded by the analogous provision in terms of Article 9 of the Directive and the reasons for processing can be regarded as somewhat different from the perspective of a publisher and that of a search engine.

The basis upon which the CJEU in *Google SL* held that a data subject may have the RTBF in some instances is essentially based on Article 12(b) and 14(a) of the Directive. In short Article 12(b) gives a data subject the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive. Article 14(a) grants a data subject the right in some instances to object on compelling legitimate grounds relating to his situation to the processing of data relating to him. With this in mind it is apt to look at the rights afforded to a data subject in terms of the POPI.

The POPI states that: "*A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right… – (c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24; (d) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a);…*"[281]

280 Sec 7(1).
281 Sec 5.

In terms of Section 11(3)(a) of the POPI "*A data subject may object, at any time, to the processing of personal information – (a) in terms of subsection 1(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing;*" There is a marked similarity in this Section to that of Article 14(a) of the Directive which provides weight to an argument that the RTBF should be recognised in South Africa.

Section 11(4) provides that, if a data subject has objected to the processing of personal information in terms of Section 11(3), then the responsible party may no longer process that personal information.

In terms of Section 24(1) of the POPI "*A data subject may, in the prescribed manner, request a responsible party 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…*" There is once again a marked similarity here to the provisions of the Directive, in particular Article 12(b), which the CJEU in *Google SL* also relied on in coming to the conclusion that there is a RTBF.

Section 24(2) of the POPI then provides for the process a responsible party must follow as soon as they receive notice in terms of Section 24(1). The responsible party would have to correct the information,[282] destroy or delete it,[283] provide the data subject with credible evidence in support of the information[284] or where no agreement can be reached between data subject and responsible party, steps can be taken to attach information that is to be read with the disputed information.[285]

---

282 Sec 24(2)(a).
283 Sec 24(2)(b).
284 Sec 24(2)(c).
285 Sec 24(2)(d).

It is evident that our law may lean in favour of the recognition of the RTBF. If the CJEU on the strength of Articles 12(b) and 14(a) of the Directive found in favour of the RTBF it can surely be argued that our Courts should also find so due to the patent similarity between the aforementioned Articles and Sections 24(1) and 11(3)(a) of the POPI.

Complaints in terms of the provisions of the POPI are to be handled by the Regulator.[286] The Regulator must have regard for the protection of all human rights and social interests that compete with privacy[287] and must also consider developing general international guidelines relevant to the better protection of individual privacy.[288]

In an article in the *BusinessReport* Kirby[289] submitted that South African law is aligned to the European position as set out in *Google SL* in that Section 24 of the POPI affords a data subject certain rights regarding the correction of personal information. Kirby states that the RTBF in South Africa would only apply to personal information which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or which has been obtained unlawfully.[290]

In an article on *Webber Wentzel Blogs,* Milo[291] notes that Google has reportedly received a flood of requests from various persons, including politicians and persons with criminal records, for their information to be removed and that Google itself has also taken steps to implement the decision. Milo states that the decision in *Google SL* will be of persuasive authority in South Africa due to the similar provisions

286 Sec 40(1)(d).
287 Sec 44(1)(b).
288 Sec 44(1)(d).
289 "What SA law says about the right to be forgotten" dated 13 June 2014 and available at http://www.iol.co.za/business/opinion/what-sa-law-says-about-the-right-to-be-forgotten-1.1702860#.VdLApPmqqko (accessed 30 October 2015).
290 *Ibid.*
291 "Is there room for a 'right to be forgotten' in South Africa" dated 6 June 2014 and available at http://blogs.webberwentzel.com/2014/06/is-there-room-for-a-right-to-be-forgotten-in-south-africa/ (accessed 30 October 2015).

contained in the POPI.[292] It is furthermore argued that the findings of the Court in *Google SL* regarding the fact that the Spanish Court does have jurisdiction (despite Google Inc. being located outside Europe) and that Google was the "controller" in terms of the Directive will likely influence regulators even outside Europe.[293] Milo points out that there are similarities between the Directive and the POPI (in particular with regard to the principle of minimality, quality of information and correction of personal information).[294] Milo advocates for the media codes of ethics to be updated to provide for adequate safeguards for the protection of personal information.[295]

IV. CONCLUSION

The South African law pertaining to data protection is, as has perhaps been pointed out herein repeatedly, markedly similar to that in the EU.

It is however important to emphasise these similarities in a comparative study where there has been no direct pronouncement on the RTBF in South Africa. It appears that there is authority amongst South African lawyers which suggest that the RTBF applies in South Africa.

It may be premature to state outright that the RTBF does exist in South Africa, because this question will have to be addressed by the legislator or our Courts in future.

What can be said with some degree of confidence however is that there are good prospects for enforcing the RTBF in South Africa.

---

292 "Is there room for a 'right to be forgotten' in South Africa" dated 6 June 2014 and available at http://blogs.webberwentzel.com/2014/06/is-there-room-for-a-right-to-be-forgotten-in-south-africa/ (accessed 30 October 2015).

293 *Ibid.*

294 *Ibid.*

295 *Ibid.*

CHAPTER 5

CONCLUSION

Although it may seem strange, the ability which the human mind has to forget is, in some instances, a gift. This gift is not shared by computers, who have almost near perfect memory. The inability to forget hinders the ability of individuals to improve their present and their future as their past mistakes continuously haunt them.[296]

It may sound rather sensationalist but the judgment in *Google SL* has truly had an effect world-wide. Search engines are, for most internet users, their window into the information contained on the internet and the removal of links can amount to censorship of information. Of course the RTBF is not absolute but the stress which is now placed on the data controller to adjudicate on the crippling mass of requests may cause legitimate links to be delisted for fear of the drastic sanctions which may be imposed on it.[297]

The glasses through which we view the internet may become increasingly tainted because search results are not necessarily delivering a true reflection of the information which is out there. Most of us do not possess the ability to circumvent delisting and therefore there exists a legitimate concern for the rights of the internet user.

The EU has already started down the path for the codification of the RTBF[298] even in light of all the criticism which may be levelled at the recognition and application of the RTBF.[299] The internet however remains a tricky domain to regulate and may even in some instances have the opposite effect of what was intended by the regulator. An

296 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 176.
297 Rosen J "The Right to be Forgotten" (2012) 64 *Stanford Law Review Online* 90, 91.
298 GDPR pg 100, 101, 102.
299 *Supra* at Chapter 3.

excellent example of this is the "Streisand Effect" which causes even more interest in information people want to hide.[300]

The problems faced abroad regarding the RTBF will most certainly also be faced in South Africa at one point in time or another. The stark resemblance between the Directive and the POPI gives credence to the existence of the RTBF in South Africa.

The abundance of issues which surround the RTBF will also have to be addressed in a South African context. As Ahmed points out, it may be necessary for the establishment of an independent body to ensure legitimate compliance with the RTBF.[301] This may still not prove to be a solution because striking the perfect balance between the right of the data subject and the internet user will always be a complicated task. South Africans will also ask who will pay for such a body.

There is no quick solution to this problem. It is however suggested that, despite all the pitfalls, that the ambit and scope of the RTBF should be provided for in legislation similar to the GDPR proposed in the EU.

300 Morozov E "Living with the Streisand Effect" dated 26 December 2008 *The New York Times* and available at http://www.nytimes.com/2008/12/26/opinion/26iht-edmorozov.1.18937733.html?_r=0 (accessed 30 October 2015).

301 Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 183.

Word Count:

Inclusive of footnotes but excluding:

the table of contents; the title page; the declaration forms and the bibliography.

14 996 words.

BIBLIOGRAPHY:

European Union Legislation:

The Charter of Fundamental Rights of the European Union 2000/C 346/01

The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on The Protection of Individuals With Regard to The Processing of Personal Data and on The Free Movement of Such Data OJ 1995 L 281, p.31

The European Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950 (Signed in Rome on 4 November 1950)

Judgments of the Court of Justice of the European Union:

ASNEF & FECEMD v Administración del Estado (Cases C-468/10 and C-469/10) Judgment of the CJEU (Third Chamber) of 24 November 2011

Bodil Lindqvist (Case C-101/01) Judgment of the CJEU (Grand Chamber) of 6 November 2003

Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González (Case C-131/12) Judgment of the CJEU (Grand Chamber) of 13 May 2014

L'Oréal SA & 3 Others v eBay International AG & 9 Others (Case C-324/09) Judgment of the CJEU (Grand Chamber) of 12 July 2011

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy (Case C-73/07) Judgment of the CJEU (Grand Chamber) of 16 December 2008

Judgments of the European Court of Human Rights:

Aleksey Ovchinnikov v Russia (Application Number 24061/04) Judgment of the ECHR (First Section) of 16 December 2010

Times Newspapers LTD (Nos.1 and 2) v The United Kingdom (Application Numbers 3002/03 and 23676/03) Judgment of the ECHR (Fourth Section) of 10 March 2009

Opinions of the Advocate General in matters before the Court of Justice of the European Union:

AG Jääskinen's opinion delivered on 25 June 2013 in the case of *Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) & Mario Costeja González* (Case C-131/12) Judgment of the CJEU (Grand Chamber) of 13 May 2014

AG Jääskinen's opinion delivered on 9 December 2010 in the case *L'Oréal SA & 3 Others v eBay International AG & 9 Others* (Case C-324/09) Judgment of the CJEU (Grand Chamber) of 12 July 2011

AG Kokott's opinion delivered on 8 May 2008 in the case *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy & Satamedia Oy* (Case C-73/07) Judgment of the CJEU (Grand Chamber) of 16 December 2008

South African Legislation:

The Constitution of the Republic of South Africa, Act 108 of 1996

The Electronic Communications and Transactions Act, Act 25 of 2002

The Interception and Monitoring Act, Act 127 of 1992

The Promotion of Access to Information Act, Act 2 of 2000

The Protection of Personal Information Act, Act 4 of 2013

The Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act 70 of 2002

South African Case Law:

Bernstein and Others v Bester and Others NO 1996 (2) SA 751 (CC)

National Media Ltd and Another v Jooste 1996 (3) SA 262 (A)

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 (T)

Books:

Papadopoulos et al *Cyberlaw@SA III* 3rd edition (2012) Van Schaik Publishers

van der Merwe et al *Information and Communications Technology Law* (2008) LexisNexis

Journal Articles:

Ahmed F "Right to be forgotten: a critique of the post-Costeja Gonzalez paradigm" (2015) 21(6) *Computer and Telecommunications Law Review* 175

Cofone I "Google v. Spain: A Right To Be Forgotten?" (2015) 15 *Chicago-Kent Journal of International and Comparative Law* 1

Gstrein O "The Cascade of Decaying Information: Putting the 'Right to be Forgotten' in Perspective" (2015) 21(2) *Computer and Telecommunications Law Review* 40

Papadopoulos S "Revisiting the Public Disclosure of Private Facts in Cyberworld" (2009) *Obiter* 30

Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position" (2007) *SALJ* 400

Rosen J "The Right to be Forgotten" (2012) 64 *Stanford Law Review Online* 88

Internet Articles:

Kirby "What SA law says about the right to be forgotten" *BusinessReport* dated 13 June 2014 and available at http://www.iol.co.za/business/opinion/what-sa-law-says-about-the-right-to-be-forgotten-1.1702860#.VdLApPmqqko (accessed 18 August 2015)

Milo "Is there room for a 'right to be forgotten' in South Africa" *Webber Wentzel Blogs* dated 6 June 2014 and available at http://blogs.webberwentzel.com/2014/06/is-there-room-for-a-right-to-be-forgotten-in-south-africa/ (accessed 18 August 2015)

Morozov E "Living with the Streisand Effect" dated 26 December 2008 *The New York Times* and available at http://www.nytimes.com/2008/12/26/opinion/26iht-edmorozov.1.18937733.html?_r=0 (accessed 25 September 2015).

Taibi C "How the EU's 'Right to be Forgotten' Rule is Backfiring Completely'" dated 22 July 2014 *The Huffington Post* and available at http://www.huffingtonpost.com/2014/07/22/right-to-be-forgotten-google-publishers-uk_n_5610803.html (accessed 25 September 2015).

The Advisory Council to Google on the Right to be Forgotten Dated 6 February 2015 and available at https://www.google.com/advisorycouncil/ (accessed 18 August 2015)

Tippmann and Powles "Google accidentally reveals data on 'right to be forgotten' requests" *The Guardian* dated the 14th of July 2015 and available at http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests (accessed 18 August 2015)

Websites:

Composition of the CJEU available at: http://curia.europa.eu/jcms/jcms/Jo2_7024/ (accessed 25 September 2015)

Delisting Process: https://support.google.com/legal/answer/3110420?hl=en (accessed 25 September 2015)

Judgments of the CJEU and opinions of the Attorney Generals freely available at: www.curia.europa.eu (accessed 25 September 2015)

Judgments of the European Court of Human Rights freely available at: www.hudoc.echr.coe.int/eng (accessed 25 September 2015)

Foreign Case Law:

Katz v United States 389 US 347 (1967)

Proposals for a Regulation in the European Union:

Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) 2012/001 (COD) 9565/15 of 11 June 2015 pg 1, 2

Doctoral Thesis:

Neethling J *Die Reg op Privaatheid* (UNISA 1976)

Discussion Papers:

The South African Law Reform Commission Discussion paper 109, Project 124, October 2005