UNIVERSITY OF KWAZULU-NATAL

SCHOOL OF LAW, PIETERMARITZBURG

A critical analysis of the right to be forgotten in South African law in light of the rights of freedom of expression and privacy.

Helga Schultz

(203507808)

This thesis is submitted in fulfilment of the requirements for the degree of Doctor of Philosophy.

Supervisor: Prof DW Freedman

2024

DECLARATION

I, Helga Schultz, declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.

B. This dissertation has not been submitted for any degree or examination at any other university.

C. This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

D. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a. their words have been re-written, but the general information attributed to them has been referenced;

   b. where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

E. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

F. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the sources being detailed in the dissertation/thesis and in the References sections.

Signed:

Date: 15 March 2024

ABSTRACT

The Protection of Personal Information Act 4 of 2013 (POPI) was fully commenced on 1 July 2020. POPI was formed by the principles laid down in the European Union Data Protection Directive 95/46/EC, which has now been replaced by the Regulation (EU) 2016/679 (General Data Protection Regulation or GDPR). POPI is designed to regulate the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and freedoms of not only the data subject, but also of the general public. POPI provides, under certain circumstances, for the correction as well as deletion of personal information. In terms of digitally stored information, deletion includes the de-indexing/de-listing by search engines as well as the taking down and complete removal and destruction of information, not only from web pages by those that control and process such information, but also information held in storage by public and private authorities. This process is called the right to be forgotten.

Europe is one of the leading advocates of the right to be forgotten, with the Court of Justice of the European Union and European Court of Human Rights taking the lead in describing and outlining the scope of the right to be forgotten, especially since *Google Spain SL, Google Inc. v AEPD, v Mario Costeja González* EU:C:2014:317.

The main objective of this thesis is to critically analyse the right to be forgotten in the South African legal context, and investigate how the right is balanced in light of the traditional rights of freedom of expression and privacy, in the digital age. The research involves setting out, as it relates to the right to be forgotten, the various legal principles and relevant legislative instruments from both national and foreign jurisdictions, describing and analysing the arguments from the European Courts, and critically examining how these could be applied in the South African context.

ACKNOWLEDGEMENTS

I thank my Lord and Saviour, for being my light, salvation and strength (Psalm 27 v 1) from the beginning all the way to the end of this journey.

To Mama and Papa: DANKE! I am grateful for their love, encouragement and patience throughout the entire journey. Especially, Papa, for being prepared to read chapters and provide comments and corrections, and for being a sounding board for my ideas and thoughts. It has meant a lot that he shared a part of this journey with me.

I also thank Prof DW Freedman for his supervision, patience, comments and time. I have enjoyed the journey. Thanks too to Prof SV Hoctor for the initial guidance in finding a topic.

To my family and friends, thank you for the encouragement and understanding that the journey is long, and for the friendship and prayers along the way. It is truly appreciated.

To the Judge President, the Judiciary, and colleagues of the Division of the High Court, KwaZulu-Natal, thank you! A special mention and thank you is added for the Honourable Mr Justice Koen – it was one of his judgments that sparked the journey on this topic, and for reading and commenting, in between his busy schedule, on initial drafts of some of these chapters, it is appreciated.

TABLE OF CONTENTS

Declaration i
Abstract ii
Acknowledgements iii
Table of contents iv
List of abbreviations xiii
Citing international and foreign case law xv
CHAPTER 1 1
Introduction 1
I Privacy and the internet 1
II Artificial intelligence, algorithms, and other definitions 4
(a) Introduction 4
(b) Search engines 4
(c) Algorithms 5
(d) Artificial intelligence 7
(e) Cookies and other trackers 9
(f) Conclusion 11
III The right to be forgotten 11
(a) Introduction 11
(b) Maybe not that new 12
(c) What is the "right to be forgotten"? 13
(d) The legal framework 16
IV Information/data and protecting human rights 16
(a) Some general thoughts 16
(b) Cybercrime 19
(c) Another thing . . . "Big Brother is Watching You": Surveillance 22
(d) Doxing 27
(e) Personal information/data is needed for . . . daily life 28
V Research questions and a hypothesis 29
VI Rationale 31
VII Comparative study 32

VIII Limitations 35
IX Research methodology 35
X Conclusion 35
CHAPTER 2 37
Directive 95/46 and the GDPR 37
I Introduction 37
II Directive 95/46 42
(a) Introduction 42
(b) Objectives and scope 43
(c) Definitions 48
(d) The principles for the processing of personal data 52
(i) Legitimacy of processing 53
(ii) Purpose specification 54
(iii) Minimality 55
(iv) Information quality 55
(v) Retention of records 55
(vi) Confidentiality and security of processing 56
(vii) Accountability 57
(viii) The data subject's right to participate 57
(e) Conclusion 59
III The GDPR 61
(a) Introduction 61
(b) Objectives and scope 63
(c) Definitions 65
(d) Principles and the right to be forgotten 69
(i) Legitimacy of processing 70
(ii) Purpose specification 72
(iii) Minimality 73
(iv) Information quality 73
(v) Retention of records 74
(vi) Confidentiality and security of processing 74

(vii) Accountability 75
(viii) The data subject's right to participate 75
(e) The right to be forgotten 78
(f) Conclusion 83
IV Transition between Directive 95/46 and the GDPR 84
(a) Introduction 84
(b) Deutsche Post AG v Hauptzollamt Köln 85
(c) Data Protection Commission v Facebook Ireland & Schrems 88
(d) Conclusion 89
V Conclusion 89
CHAPTER 3 91
Google Spain and the Right to be Forgotten 91
I Introduction 91
II Google Spain and the right to be forgotten hitS the limelight 94
(a) Facts and issues raised 95
(b) Legal framework 98
(c) Jurisdiction and the responsibility of operators 100
(d) The scope of "the right to be forgotten" 101
(i) Generally forgetting information: Questions 2(c) and (d) 101
(ii) Can lawfully published information be forgotten? 104
III What the academics thought of Google Spain 107
IV Developing Google Spain's right to be forgotten through the case law 115
(a) Introduction 115
(b) Territorial jurisdiction 115
(i) Background and issue 116
(ii) The territorial extent of the right to be forgotten 117
(iii) Application 117
(iv) Conclusion 119
(c) The right to forget a crime and criminal trials 120
(i) Introduction 120
(ii) Forgetting expunged criminal convictions 122

(iii) Considerations of access to contemporary historical events in online archives 127
(iv) Family applying for the crime to be forgotten 132
(v) Conclusion..... 134
(d) Statements, interviews, etc, made in a professional capacity 135
(e) Processing special categories of data..... 139
(i) Introduction 139
(ii) Duties imposed on search engine operators and/or controllers..... 141
(iii) De-linking and exceptions..... 142
(iv) Operators of search engines to set out the current position..... 145
(v) Conclusion..... 147
(f) Anonymisation and deletion of archives, and the right to be forgotten..... 147
(i) Introduction 147
(ii) Anonymisation 148
(iii) Deletion 159
(g) Conclusion 163
V Conclusion..... 169
CHAPTER 4 170
South African Law: Privacy and Expression 170
I Introduction 170
II The right to privacy..... 172
(a) Introduction and historical context 172
(b) The scope of privacy in Bernstein v Bester and its application..... 175
(i) Legitimate expectation of privacy..... 175
(ii) Privacy exists along a continuum..... 176
(iii) The inner sanctum 185
(c) The States interests and privacy..... 189
(d) Conclusion 190
III Freedom of expression..... 191
(a) Introduction and historical context 191
(b) The importance of free expression..... 193
(c) Structure of section 16 196

(i) Introduction 196
(ii) Section 16(1): The meaning of expression 196
(iii) Section 16(2): Limits to freedom of expression 199
(iv) Conclusion 200
(d) Specific protections afforded by section 16(1) 201
(i) Press freedom 201
(ii) Convey and receive information 201
(e) Hate speech 202
(f) Conclusion 206
IV How the cases have balanced privacy and expression 207
(a) Introduction: general remarks 207
(b) Classified information 209
(c) Confidentiality and a free press 209
(d) Journalistic sources 213
(e) Public access to information in court files 213
(f) Defamation and technology 215
V Conclusion 219
CHAPTER 5 221
POPI and the Right to be Forgotten in SA 221
I Introduction 221
II POPI: An overview 224
(a) Introduction 224
(b) Definitions 225
(c) Conclusion 231
III Application, interpretation, and purpose 232
IV Processing of personal information 236
(a) General principles 236
(i) Condition one: Accountability 237
(ii) Condition two: Processing limitations 238
(iii) Condition three: Purpose specification 240
(iv) Condition four: Further processing limitation 242

(v) Condition five: Information quality 242
(vi) Condition six: Openness 243
(vii) Condition seven: Security safeguards 245
(viii) Condition eight: Data subject participation 247
(ix) Conclusion 248
(b) Processing of special personal information 249
(c) Processing of children's personal information 251
(d) Exemptions/exclusions/exceptions 253
(e) Direct marketing and the rights of data subjects 255
(f) Conclusion 256
V Supervision of POPI 257
VI Jurisdiction 258
VII The right to be forgotten and POPI 261
(a) Introduction 261
(b) POPI, privacy, expression, and forgetting 262
(c) Section 11 264
(i) Justifying the processing of personal information 264
(ii) The issue of consent 265
(iii) Objecting to the processing of personal information 268
(iv) Divine Inspiration Trading 205 (Pty) Ltd v Gordon 271
(aa) Facts and contentions 271
(bb) The court's findings and conclusions 272
(d) Section 24 274
(e) Defining the right to be forgotten in South Africa 275
(i) Introductory remarks 275
(ii) How Google Spain defined the right to be forgotten 277
(iii) Why is a right to be forgotten necessary? 280
(iv) What could a South African right to be forgotten look like? 284
(v) POPI 287
(vi) Remedies provided in POPI 292
(f) Conclusion 293

VIII Conclusion 293
CHAPTER 6 295
Forgetting: Lessons for South Africa 295
I Introduction 295
II Jurisdiction 298
(a) Introduction 298
(b) Summary of the CJEU case discussion and legal principles 300
(c) South Africa 301
(d) Comment 302
III The right to forget crimes and criminal trials 302
(a) Introduction 302
(b) Summary of the EU and national high court case discussion and legal principles 303
(c) South Africa 305
(d) Comment 307
IV Statements, etc. made in a professional capacity 308
(a) Introduction 308
(b) Summary of the German case discussion and legal principles 308
(c) South Africa 309
(d) Comment 312
V Processing special categories of data/information 313
(a) Introduction 313
(b) Summary of the CJEU case discussion and legal principles 313
(c) South Africa 316
(d) Comment 319
VI Anonymisation or deletion of archives 320
(a) Introduction 320
(b) Summary of the ECtHR case discussions and legal principles 320
(c) South Africa 323
(d) Comment 325
VII General remarks and further considerations 326
(a) Introduction 326

(b) Decommodification of personal data / combatting surveillance capitalism 327
(c) Eternal memory of and the ease of accessing data/information on the internet ... 331
(d) Anonymisation: Protecting vulnerable family members and innocent bystanders334
(e) The right to be forgotten and AI 337
(f) Conclusion 343
VIII Conclusion 344
(a) The aim of the thesis 344
(b) The first question 345
(c) The second question 346
(d) The third question 349
(e) The fourth question 350
IX In closing 353
BIBLIOGRAPHY 357
Books 357
Articles and blogs 358
Conference papers and conference proceedings 394
Dissertations/Thesis 395
Opinions 396
Online sources 397
Reports/Papers 398
TABLE OF CASES 401
Australia 401
Canada 401
Europe and the European Union 401
Germany 408
The Netherlands 409
Northern Ireland 409
South Africa 409
United Kingdom 416
United States 417
TABLE OF STATUTES 418

Canada 418
Europe and the European Union 418
Statutes/Regulations 418
Directives 419
Treaties/Conventions 420
Germany 420
South Africa 420
United Kingdom 422
United States 422

LIST OF ABBREVIATIONS

The following list is of the most often used abbreviations within the thesis – not all are listed here.

The necessary abbreviations were kept, as far as possible, to a minimum.

Abbreviation	Full Title
Article 29 WP	Article 29 Data Protection Working Party
Charter	Charter of Human Rights of the European Union (2012/C 326/02) OJ 2012, C 326/391, 26.10.2012
CJEU	Court of Justice of the European Union
Constitution	Constitution of the Republic of South Africa, 1996
Convention	Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, as amended by Protocols Nos. 11, 14 and 15, and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, 1981
Directive 95/46	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, No L 281 /31, 23. 11. 95
eCommerce Directive 2000/31	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ 2000, L 178, 17.7.2000
ECTA	Electronic Communications and Transactions Act 25 of 2002
ECtHR	European Court of Human Rights
EU	European Union
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ 2016, L 119/1, 4.5.2016 (the General Data Protection Regulation).
GG	Basic Law for the Federal Republic of Germany / Grundgesetz für die Bundesrepublik Deutschland
Google Spain	*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) EU:C:2014:317, [2014] EUECJ C-131/12
Interim Constitution	Constitution of the Republic of South Africa 200 of 1993
NCA	National Credit Act 34 of 2005
OECD	Organization for Economic Cooperation and Development
OECD Guidelines	Organization for Economic Cooperation and Development's *Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data*
PAIA	Promotion of Access to Information Act 2 of 2000
POPI	Protection of Personal Information Act 4 of 2013

RICA	Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002
SA	South Africa
SALRC	South African Law Reform Commission
TFEU	Treaty on the Functioning of the European Union (Consolidated 2016)
UK	United Kingdom
US	United States or United States of America

CITING INTERNATIONAL AND FOREIGN CASE LAW

In the thesis, and to remain as consistent as possible with all other sources quoted, some of the international / foreign judgements used will be cited as follows:

Regarding European Case Law

Specifically for European Union case law, ie that emanating from the Court of Justice of the European Union, the standard proposed is based on the European Case-Law Identifier or ECLI, and is written as follows: "Judgement of 13 May 2014, Case C-542/09 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317".

However, this is cumbersome hence the version proposed by OSCOLA, slightly modified to match South African citations will be followed, for footnotes, the reference, eg "*Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317", and in the Bibliography the citation will read: "*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C 131/12) EU:C:2014:317".[1]

If there is a Bailii.org (British and Irish Legal Information Institute) citation available, especially for the cases emanating from the European Court of Human Rights, this has been used, eg "*Times Newspapers Ltd v The United Kingdom (Nos. 1 & 2)* [2009] ECHR 451".[2] Alternatively, as provided or "unreported cases" in terms of the requisite guide, eg "*Times Newspapers Ltd v The United Kingdom (Nos. 1 & 2)* (European Court of Human Rights) application nos. 3002/03 and 23676/03 (10 March 2009)". This will mainly be used where the cases appear in French on Bailii.org.

Regarding German Case Law

It is worth noting that the German case law generally does not have a case name, ie the parties are anonymised and with the use of letters and numbers to provide the information regarding the citation of the case, and in some instances this will include the ECLI (European Case-Law Identifier).

There are a few exceptions regarding the non-use of case names: if one of the parties is a

[1] See S Meredith & D Nolan *The Oxford University Standard for Citation of Legal Authorities*, 4ed (2012) at 30ffg.
[2] Unless Bailii.org (British and Irish Legal Information Institute) carries the French text, which I am unable to read.

well-known person (ie actor, politician, etc.) or there is a company or similar entity involved, then this may be used as a "case name". In other instances, a descriptive title is given for the case, eg, "*Tonband*", which translates to cassette, as that matter was dealing with the use of cassette voice recordings or "*Recht auf Vergessen I*", which translates to "*Right to be forgotten I*", as this was the main legal aspect of the case. German cases will be cited along the following lines:

OLG Stuttgart, Urteil vom 08.10.2015 - 2 U 25/15;

BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 16/13; DE:BVerfG:2019:rs20191106.1bvr001613 – *Recht auf Vergessen I* (the date may read 06.11.2019 and the rest will remain the same); or,[3]

34 BVerfGE 238 – *Tonband* (where the reported book form is available).[4]

[3] The footnote will read: "BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 16/13 – *Recht auf Vergessen I*".

[4] The citations were guided by: 'Hinweise für Autoren' in *Neue Juristische Wochenschrift*, no. 12/2019, https://www.beck.de/rsw/upload/NJW/Autorenhinweise_2019.pdf (Accessed: 21 April 2021); Library of Congress, https://www.loc.gov/law/help/constitutional-court-cases/germany.php (Accessed: 21 April 2021); and *Journal of International Law and Politics Guide to Foreign and International Legal Citations* 2006 (New York University), https://www.law.nyu.edu/sites/default/files/upload _documents/Final_GFILC_pdf.pdf; accessed 17 November 2020.

CHAPTER 1

INTRODUCTION

I PRIVACY AND THE INTERNET

The internet never forgets. The internet's design promotes finding, sharing and receiving of information, often within seconds, if not "real-time". It is available, colloquially expressed, "24/7/365". These characteristics are reflected in the names describing the internet, ie the World Wide Web, cyberspace, information superhighway as well as "history's greatest tool for global access to information".[1] Searches for information or data are conducted with relative anonymity – especially where these functions are enabled on a search engine tool.[2]

The ability to obtain news and information with relative ease and at a very quick speed certainly gives the internet an attractive aura. Individuals are able to watch sporting events, concerts, etc. in "real-time", ie with no or an incredibly minimal delay,[3] for example, events are hosted on YouTube and other media or broadcast organisations' websites.

However, private bodies, individuals, and institutions are not the only ones found on the internet. Public bodies also have internet websites containing information about their functions, powers and procedures created for public use and knowledge.

The internet also acts as an open canvas that allows private bodies, individuals and

---

[1] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (6 April 2018) UN Doc. A/HRC/38/35 para 1. Note *L.B. v Hungary* [2021] ECHR 2 para 14, of the dissenting opinion by Ravarani and Schukking JJ, remarked how difficult it is to be forgotten on the internet. The ECtHR in *Editorial Board of Pravoye Delo and Shtekel v Ukraine* [2011] ECHR 748 para 63 stated

> "the Internet is an information and communication tool particularly distinct from the printed media, in particular as regards the capacity to store and transmit information. The electronic network serving billions of users worldwide is not and potentially cannot be subject to the same regulations and control. The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned."

See also A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 113.

[2] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) UN Doc. A/HRC/17/27 para 23. Alphabet's search engine tool, Google, has become synonymous with searching for information on the internet, ie it is often said that internet user's "google it" when they are unsure of topic or what the latest news is – see S van Deventer 'Problems relating to the formation of online contracts: A South African perspective' (2021) *South Africa Law Journal* 219 at 227, and E Mik 'Contracts governing the use of websites' (2016) *Singapore Journal of Legal Studies* 70 – 94.

[3] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) UN Doc. A/HRC/17/27 para 23. See also A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 129.

organisations, as well as public bodies and government institutions, to create content, ie information or data, either on, for example, the organisation's or company's website, in a personal blog or through a social media website. Relatively popular websites are those that belong to news agencies, for example News24, or encyclopaedic web pages, such as *Encyclopaedia Britannica* or *Wikipedia*. When private and public bodies create a social media account, it becomes a platform from which they may express themselves through written comments or post photographs and create new connections through these pages by adding new people to their "contacts" list. The more popular social media websites include Facebook, X (formerly Twitter), LinkedIn, Instagram and TikTok. Thus, freedom of expression – one of the traditional news media's most important rights – is given a greater audience and is well-catered by and suited to the design of the internet.

However, the internet is no longer confined to desk top computers and laptops. Mobile technology with internet capabilities allows for "on-the-go" access to the internet, anytime, anywhere, provided there is the necessary signal. Media houses, social media companies, banking institutions and various other public and private organisations have designed mobile versions, in the form of applications or simply "apps", of their website, making them suitable for smart phones and tablets. They carry, where necessary, the same login credentials as their web counterparts. The emergence of smart phone technology has certainly revolutionised how we interact with other human beings and the internet in our day-to-day lives.[4] Zunger, a physicist turned computer scientist, described this phenomenon as follows:[5]

> "[computers] have made having friends on the other side of the world as normal as having them next door, have put the sum of human knowledge in our pockets, and have made nearly every object we encounter more reliable and less expensive. Yet their failure, whether by accident or by unthinking design, can have catastrophic consequences for individuals and society alike."[6]

Through these digitised platforms, ie news sites and social media pages, individuals have the

[4] Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe*, dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019), and J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 56.

[5] Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe*, dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019), and J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 56.

[6] Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe*, dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019). See also E Stiakakis, CK Georgiadis & A Andronoudi 'Users' perceptions about mobile security breaches' (2016) 14 *Information Systems and e-Business Management* 857 at 858.

ability to express themselves and share ideas and opinions. Hence, freedom of expression is no longer the sole domain of the press and persons physically and openly airing their views in public places or printed newspapers. In today's modern society, individuals, using computers, cell phones, tablets and other similar devices, "post" information about themselves, as well as air their views on the aforementioned digitised platforms.[7]

The internet is one of the most disruptive, yet useful tools of our time, revolutionising the way in which individuals are able to obtain information.[8] However, Zunger's words, quoted above, allude to a more unsettling side of the internet. The information displayed on the internet, whether posted by oneself or another person, may affect the ability to find suitable employment. For example, the publication of a property sale due to insolvency[9] or attending an interview to defend company policies, even if the employee does not personally agree with them, can impact one's job prospects.[10] The reason for this is because the internet's design is predominantly public in nature; this includes traditional newspapers having an online presence, and social media websites, ie Facebook, which are "social".[11] The internet, significantly with the use of social media websites, allows persons to not only freely express themselves, but also find personal information on others. Celebrity status is no longer a criteria for an individual to be scrutinised and gossiped on by the public.[12] Cashmore in an article for CNN.com summed this up when he wrote "[privacy] is dead, and social media holds the smoking gun."[13] How can

[7] J Rosen 'The web means the end of forgetting' *New York Times Magazine*, dated 21 July 2010, *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022). See also J Rosen 'Free speech, privacy, and the web that never forgets' (2011) 9 *Journal on Telecommunications & High Technology Law* 345 – 356, and M Crockett 'The internet (never) forgets' (2017) 19 *SMU Science and Technology Law Review* 151 – 181. Rosen, in an article for the *New York Times Magazine*, vividly details the catastrophic impact that the internet has, especially when seeking employment opportunities and receiving rejection letters, based on old posts, created by oneself or another. The content of these posts may contain of a controversial cause, what was thought of as harmless at the time – a fun night out as a university student, a comment in support, a publication or dissertation that an individual no longer wants to be associated with. In other words, employers seek out the personal information created by prospective employees to evaluate whether these will fit into the company profile. Certainly, a frightening reality for many, making the idea of the right to be forgotten an irresistible prospect. See also J Spillane 'Google's "right to be forgotten" – A dream come true for job seekers?' *Business 2 Community*, dated 17 July 2014, *https://www.business2community.com/human-resources/googles-right-forgotten-dream-come-true-job-seekers-0946918* (Accessed 26 November 2022).

[8] See Article 19 'Digital Rights' available at *https://www.article19.org/issue/digital-rights/* (Accessed 15 April 2019).

[9] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[10] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*.

[11] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 14. See also See Article 19 'Digital Rights' available at *https://www.article19.org/issue/digital-rights/* (Accessed 15 April 2019).

[12] J Rosen 'The web means the end of forgetting' *New York Times Magazine*, dated 21 July 2010, *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022).

[13] P Cashmore 'Privacy is dead, and social media holds smoking gun' *CNN.com*, dated 28 October 2009. *https://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/* (Accessed: 3 December 2022). Compare with *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 145.

individuals claw back their privacy? How can individuals protect privacy on the internet? Everyone has information from their past that they do not want revealed. Where to from here? One of the ways in which people claw or claim back their privacy is through the right to be forgotten. However, before discussing what the right to be forgotten entails, it would be useful to define some concepts and set out their relationship with gathering information on the internet.

II ARTIFICIAL INTELLIGENCE, ALGORITHMS, AND OTHER DEFINITIONS

(a) Introduction

Certain technical words and phrases will be defined to provide some clarity. These are not the only technical terms, but certainly, some of the more important ones to note, as they have an effect on the right to privacy, ie the right to keep one's data private, processed fairly, and with the requisite consent.

The world of technology is changing at a very rapid pace; this does come with many benefits, but also with problems or challenges of its own. The various technological terms that will be referred to throughout this thesis include search engines, algorithms, artificial intelligence ('AI') as well as cookies. These terms are discussed below.

(b) Search engines

Starting with search engines, as this is the tool used to find information, including personal information, which is a key focus in this thesis. The two European Regional Courts, namely the Court of Justice of the European Union (the CJEU) and the European Court of Human Rights (the ECtHR), have both in broad terms, described the functions of "search engines", applying these descriptions to both the internet as well as website specific search tools.[14] The reason for looking at how the courts have understood what a search engine is relates to the cases and their focus on how search engines impact on the rights and freedoms of individual data subjects and internet users, within the definitions, functions and duties of all those involved in processing personal data.[15] The two courts have kept their definitions of search

[14] J Kerr 'What is a search engine? The simple question the Court of Justice of the European Union forgot to ask and what it means for the future of the right to be forgotten' (2016) 17(1) *Chicago Journal of International Law* 217 at 226 – 227.

[15] See generally *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *Google LLC v CNIL* EU:C:2019:772, *Data Protection Commission v Facebook Ireland and Maximillian Schrems* EU:C:2020:559, and *TU, RE v Google Spain LLC* EU:C:2022:96.

engines as wide as possible to allow for the comprehensive protection of the rights and freedoms of individual data subjects and internet users.[16] The ECtHR when describing a search engine has used phrases such as "automated sorting system . . . operating under human control, selected communications containing specific search terms or combinations thereof".[17] The CJEU described a search engine being a "tool that guides [internet] users to relevant webpages based on their search queries".[18]

Jääskinen, the advocate general in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (*Google Spain*),[19] in his opinion to the Grand Chamber, described the various functions of a search engine as including copying, analysing and indexing the "content on its own devices" that is contained on existing websites.[20] The indexed information, based on the keywords entered into the search tool, will appear on a results page in the form of hyperlinks or simply links, that when clicked on will lead the internet user to the relevant information on the website.[21] Kokott, in her opinion to the Grand Chamber in an "opinion procedure", described a website's internal search tool in similar terms to that of an internet search engine.[22] Search engines have become vital tools for searching for information on the internet.

(c) Algorithms

An algorithm is a set of commands that depict how a task is performed. In computer science algorithms will tell a computer how to perform through a specific sequence of instructions.[23] Algorithms form the basis of many computerised functions from simple tasks on a laptop to the integrated systems of smart devices designed to make one's daily life easier.[24] In internet

[16] J Kerr 'What is a search engine? The simple question the Court of Justice of the European Union forgot to ask and what it means for the future of the right to be forgotten' (2016) 17(1) *Chicago Journal of International Law* 217 at 226 – 227.
[17] *Liberty & others v United Kingdom* [2008] ECHR 568 para 43.
[18] *Google France SARL & Google Inc. v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA & Luteciel SARL; Google France SARL v CNRRH SARL, Pierre-Alexis Thonet, Bruno Raboin & Tiger* SARL EU:C:2010:159 para 22, and J Kerr 'What is a search engine? The simple question the Court of Justice of the European Union forgot to ask and what it means for the future of the right to be forgotten' (2016) 17(1) *Chicago Journal of International Law* 217 at 227.
[19] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[20] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2013:424, delivered on 25 June 2013 paras 33 – 35.
[21] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2013:424, delivered on 25 June 2013 para 33.
[22] Opinion of Advocate General Kokott in *Opinion procedure 2/13 initiated following a request made by the European Commission* EU:C:2014:2475, delivered on 13 June 2014 para 224 as a general reference that even internal search engines within websites provide a similar function as internet based search engines.
[23] S Papastefanou 'Smart grids and machine learning in Chinese and Western Intellectual Property Law' (2021) 52 *International Review of Intellectual Property and Competition Law* 989 at 993.
[24] L Ulbricht & K Yeung 'Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms' (2022) 16 *Regulation & Governance* 3 at 3.

searches the keywords forming the search will create the algorithm, where typed in the search tool, and once the search button or enter key are pressed, the results are displayed.[25] This is important to remember, as the CJEU targeted algorithms – although how they function, etc. was not explored in the judgment – as the tool to implement the right to be forgotten.[26]

There have been calls for algorithmic and data transparency, meaning that the data sets used to train and refine algorithms be exposed, which may lead to a compromise in the privacy of data subjects, but it also refers to making the source code publicly available.[27] However, this is beyond the scope of this thesis. The most important aspect of algorithms is not so much in the detail of how they are created or designed, trained or refined, etc. by those that create them, but rather in the fact that algorithms are the chosen tool of the CJEU to implement the internet based right to be forgotten.[28]

---

[25] L Ulbricht & K Yeung 'Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms' (2022) 16 *Regulation & Governance* 3 – 22. For a complete discussion on algorithms and how they work see P Bell 'Algorithms: The intellectual capital of the internet' (2001) July/August *Ivey Business Journal* 44 – 48. De Hert and Papakonstantinou point out that Google is the leader in search based algorithms, in terms of accuracy and indexing – see P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627.

[26] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See R Seyfert 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1550 – 1552: Algorithms are the tool used for implementing the right to be forgotten. In terms of the GDPR, it is likely that algorithms based what is termed the essentialist definition ie the core code contains the nature and essence of what the algorithm is required to do to produce a specific result (intention or strategy). In this instance, the code must be programmed to produce the intention that the information is no longer linked to the data subject's name, when a search is carried out, using the data subject's name as the search terms in the internet or internal website's search tool. Alternatively, the information linked to the data subject's name must be reflected in chronological order, with the latest information appearing first or towards the top on the results page. N Gumzej 'Technical Solutions Supporting the Online RTBF in the CJEU and ECHR Jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 – 1473 discusses some of the other technical measures available to implement the right to be forgotten requests. Important to note is that even though algorithms are the suggested solution for the implementation of the right to be forgotten from the CJEU, but those coding the algorithms must still act responsibly and be accountable to the person harmed thereby, see J Metcalf, R Singh, E Moss, E Tafesse & EA Watkins 'Taking algorithms to courts: A relational approach to algorithmic accountability' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 1450 – 1462.

[27] S Abiteboul & J Stoyanovich 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation' (2019) 11(3) *Journal of Data and Information Quality* 1 at 4. Note the following from R Seyfert 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1542 – 1558: with regards to regulating the trade of algorithms, algorithms will either be classified as first, essentialist and intentionalist, ie an algorithm is defined by its core (or code) or intention (or strategy), ie the sequence of instructions would amount to the core/code, and what is the aim of the algorithm, or the result that it is expected to generate, amounts to its intention/strategy. The second definition, behaviouristic classification, focuses on the behaviour or conduct of the algorithm, and how this behaviour impacts on the environment in which the algorithm is used.

[28] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See also P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627, and S Abiteboul & J Stoyanovich 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation' (2019) 11(3) *Journal of Data and Information Quality* 1 at 2 – 3.

(d) Artificial intelligence

One of the areas where we have seen the most rapid development is AI. AI is reliant on algorithms that form a type of "neural network" as the base from which it performs the functions for which that specific AI application was created.[29] AI encompasses a range of technological advancements, including autonomous and connected objects, machine and deep learning. AI and the applications from which it functions have started to seamlessly become a part of everyday life, one application on smart phone technology, for example, which is useful, as much as it may frustrate, is predictive text, this is an example of AI or machine-based learning technology.[30] Other examples include (but are certainly not limited to) tailoring social media feeds and controlling traffic flow in city streets. AI is used in autonomous vehicles and in consumer devices such as smart assistant applications, spam filters, voice recognition, search engines, and even in the medical field to assist health care practitioners to better diagnose, predict, prevent and treat diseases or illnesses.[31]

AI has the "potential to revolutionise societies in positive ways" but as is the case with most technological advances, it may "have a negative impact on human rights" if it is abused by corporate and State parties.[32] In particular, machine learning is able to draw inferences, and make predictions as well as decisions regarding individuals. In terms of data protection laws, this is problematic, as these decisions may lead to discrimination and further human rights violations.[33] AI uses various algorithms in order to perform a specific function but so does the

[29] Access Now *Human Rights in the Age of Artificial Intelligence* (November 2018) at 10, Privacy International and Article 19 *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (April 2018) at 6, S Papastefanou 'Smart grids and machine learning in Chinese and Western Intellectual Property Law' (2021) 52 *International Review of Intellectual Property and Competition Law* 989 at 993, and MT Baldassarre, D Caivano, B Fernandez Nieto, D Gigante & A Ragone 'The social impact of generative AI: An analysis on ChatGPT' In *Proceedings of the 2023 ACM Conference on Information Technology for Social Good (GoodIT '23)* (6 – 8 September 2023, Lisbon, Portugal) 363 at 363.

[30] Privacy International and Article 19 *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (April 2018) at 6 & 18, SAD Popenici & S Kerr 'Exploring the impact of artificial intelligence on teaching and learning in higher education' (2017) 12(22) *Research and Practice in Technology Enhanced Learning* 1 at 5, and generally C Janiesch, P Zschech & K Heinrich 'Machine learning and deep learning' (2021) 31 *Electronic Markets* 685 – 695.

[31] Privacy International and Article 19 *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (April 2018) at 4, and see generally D Donnelly 'First do no harm: Legal principles regulating the future of artificial intelligence in health care in South Africa' (2022) 25 *Potchefstroom Electronic Law Journal* 1.

[32] Privacy International and Article 19 *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (April 2018) at 2 & 4, see also N Mashinini 'The impact of deepfakes on the right to identity: A South African perspective' (2020) 32(5) *SA Mercantile Law Journal* 407 – 436 as an example of a more sinister side to AI.

[33] R Allen & D Masters 'Artificial Intelligence: The right to protection from discrimination caused by algorithms, machine learning and automated decision-making' (2020) 20 *ERA Forum* 585 – 598, and E Bayamlıoğlu 'The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"' (2022) 16 *Regulation & Governance* 1058 – 1078. Note also Recitals 71 and 75 of the Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation or GDPR) which provide that natural persons should have the right to object to automated decision

internet. Legal questions have started to emerge in respect of an individual's liability in delict where AI has been proven to have caused the damage.[34]

One of the most radical developments in AI is the introduction of OpenAI's ChatGPT.[35] ChatGPT is a so-called chatbot, an AI program that mimics human conversation.[36] A lot of ethical questions have arisen around the use of ChatGPT, mainly due to the realistic nature of the responses that it can produce.[37] One of the issues that still needs to be explored with regard to ChatGPT is the ability it has to infringe on human rights and freedoms.[38] One of the main

---

making (recital 71), and the processing of personal data should not negatively impact on their rights and freedoms, thereby leading to discrimination, identity theft and any other harm that may result against a natural person (recital 75).

[34] See generally, P Čerka, J Grigienė & G Sirbikytė 'Liability for damages caused by artificial intelligence' (2015) 31 *Computer Law & Security Review* 376 – 389, W Erlank & L Ramokanate 'Allocating the risk of software failures in automated message systems (autonomous electronic agents)' (2016) 28(2) *South African Mercantile Law Journal* 201 – 237, W Barfield 'Liability for autonomous and artificially intelligent robots' (2018) 9 *Paladyn, Journal of Behavioral Robotics* 193 – 203, M Busuioc 'Accountable Artificial Intelligence: Holding Algorithms to account' (2021) 81 *Public Administration Review* 825 – 836.and K Stuurman & E Lachaud 'Regulating AI. A label to complete the proposed Act on Artificial Intelligence' (2022) 44 *Computer Law & Security Review* 105657.

[35] The 'GPT' in ChatGPT means 'Generative Pre-training Transformer', see E Gregersen 'ChatGPT' *Encyclopedia Britannica,* 30 June 2023, *https://www.britannica.com/technology/ChatGPT* (Accessed: 12 July 2023).

[36] M Dahiya 'A tool of conversation: Chatbot' (2017) 5(5) *International Journal of Computer Sciences and Engineering* 158 – 161, and E Gregersen 'ChatGPT' *Encyclopedia Britannica,* 30 June 2023, *https://www.britannica.com/technology/ChatGPT* (Accessed: 12 July 2023).

[37] MR King 'A conversation on artificial intelligence, chatbots, and plagiarism in higher education' (2023) 16(1) *Cellular and Molecular Bioengineering* 1 – 2, J Euchner 'Almost human' (2023) 66(2) *Research-Technology Management* 10 – 11, and C Krönke 'Attention is all you need: ChatGPT und die DSGVO' *VerfBlog,* 14 April 2023.

[38] L Illia, E Colleoni, & S Zyglidopoulos 'Ethical implications of text generation in the age of artificial intelligence' (2023) 32(1) *Business Ethics, the Environment & Responsibility* 201 at 203, and JS Gordon 'AI and law: Ethical, legal, and socio-political implications' (2021) 36 *AI & Society* 403 – 404. OpenAI, the creators of ChatGPT, are currently being sued in a class action law suit in a district court in the Northern District of California in the US, amongst others claims, OpenAI has been accused of collecting and using personal data, obtained from the internet, books, articles etc. without the requisite consent, see the plaintiff's papers in the class action complaint in *PM & others v OpenAI LP & others* Case no 3:23-CV-03199, United States District Court, Northern District of California (filed on 28 June 2023), and K Jukam 'OpenAI sued over data collection practices' *Courthouse News Service,* dated 28 June 2023. *https://www.courthousenews.com/openai-sued-over-data-collection-practices/* (Accessed: 3 July 2023), and C Thorbecke 'OpenAI, maker of ChatGPT, hit with proposed class action lawsuit alleging it stole people's data' *CNN Business,* dated 28 June 2023. *https://edition.cnn.com/2023/06/28/tech/openai-chatgpt-microsoft-data-sued/index.html* (Accessed: 29 June 2023). A further two lawsuits have been filed against OpenAI for copyright infringement, see the plaintiffs' papers in *Tremblay & Awad v OpenAI Inc & others* Case no 4:23-CV-03223-KAW, United States District Court, Northern District of California, San Francisco Division (filed on 28 June 2023), *Silverman & others v OpenAI Inc. & others* Case no 3:23-cv-03416, United States District Court, Northern District of California, San Francisco Division (filed on 7 July 2023), and B Brittain 'Lawsuit says OpenAI violated US authors, copyrights to train AI chatbot' *Reuters,* dated 29 June 2023. *https://www.reuters.com/legal/lawsuit-says-openai-violated-us-authors-copyrights-train-ai-chatbot-2023-06-29/* (Accessed: 3 July 2023). See also the decisions in *Parker v Forsyth NO and others* (Regional Court, Johannesburg, Gauteng) unreported case no 1585/20 (29 June 2023) and *Mata v Avianca Inc.,* Case no 22-cv-1461 (PKC) (S.D.N.Y. 22 June 2023) where in both matters ChatGPT was used to draft either heads of argument. The cases cited in these court documents to substantiate certain points of law were fictitious. To one of the court documents was attached to a copy of the bogus or fictitious case. In both instances the court went to lengths in discussing the dangers of using ChatGPT without verifying the correctness of the allegations and cited material. *Mata v Avianca Inc*. illustrates these dangers as follows:

"Many harms flow from the submission of fake opinions. The opposing party wastes time and money in

issues so far identified is that a chatbot has the ability to exploit and further commodify data, including personal data.[39]

Although briefly mentioned here, AI (including ChaptGPT) will only be discussed where this has reference to the topic of the thesis. It should be remembered that algorithms are used in many applications, not just AI.

(e) Cookies and other trackers

Internet searches made using a search engine, eg Google or Yahoo, will inevitably leave traces called cookies, these are not the biscuits that one can snack on. Cookies are "small text files stored in the user's [ie the individual's] browser".[40] These text files provide information on how the individual came to the website, ie did they click on an advert displayed on another website, as well as how often the individual visits the site and their browsing behaviour.[41] An important function of cookies is to assist in displaying the contents of an internet website correctly, on the device accessing the website – hence, not all cookies should be distrusted.[42] Cookies are part of a group of programmes called trackers – and their function is to track individuals, ie internet users, across the internet by collecting and analysing an individual's browsing behaviour.[43] Trackers collect and process personal information or data without the

---

> exposing the deception. The Court's time is taken from other important endeavors. The client may be deprived of arguments based on authentic judicial precedents. There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity." (footnote omitted)

With regards to being liable to individuals where AI has infringed on their rights, see P Hacker, A Engel, & M Mauer 'Regulating ChatGPT and other large generative AI models' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago Illinois, United Stated of America) 1112 – 1123, J Metcalf, R Singh, E Moss, E Tafesse & EA Watkins 'Taking algorithms to courts: A relational approach to algorithmic accountability' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 1450 – 1462.

[39] L Illia, E Colleoni, & S Zyglidopoulos 'Ethical implications of text generation in the age of artificial intelligence' (2023) 32(1) *Business Ethics, the Environment & Responsibility* 201 at 203.

[40] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74, Opinion of Adovocate General Szpunar, in *Planet 49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* EU:C:2019:246, delivered 21 March 2019 para 78 – 91, and W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroom Electronic Law Journal* 1 at 2 – 5.

[41] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74, and K Mellet & T Beauvisage 'Cookie monsters. Anatomy of a digital market infrastructure' (2020) 23(2) *Consumption Markets & Culture* 110 – 129.

[42] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74.

[43] See generally C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) 74 – 80, and W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal

requisite consent of the internet user or individual. This may lead to a flood of adverts on social media feeds or other websites that are tailor-made for the individual, based on the analysis of their browsing behaviour.[44] These trackers are referred to as social plugins, as they appear on the website page in the form of a social media website "like" button, and work together with cookies.[45] They collect, process and store the data of individuals, ie internet users, irrespective of whether they have a social media account with a social media website, eg Facebook. Social plugins, often work in conjunction with cookies. Facebook is the biggest social media website that uses trackers.[46] The process of collecting the information is automatic,[47] and uses the unique Internet Protocol address, or IP address,[48] assigned to an internet-compatible device, first, to obtain the information of the individual, second, to process the personal information of the individual, and third, to track the individual.[49] Hence, cookies have become integral to the memory function of the internet.

Cookies are used in surveillance strategies, which are discussed later in this chapter. By collecting browsing behaviour or data, cookies can "remember" an individual's preferences and generate and target them with specific adverts.[50] The CJEU has recently ruled that users

implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroom Electronic Law Journal* 1 at 2 – 5.

[44] MJ Kelly 'What is a web tracker?' *The Mozilla Blog* (22 October 2019) *https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/* (Accessed: 16 November 2022). See also E Larson 'Tracking criminals with internet protocol addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 – 358 for the possible use of trackers in criminal investigations.

[45] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74. For a detailed discussion on the implications of social plugins in light of data protection legislation, see *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629, and W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroom Electronic Law Journal* 1 at 3 – 5.

[46] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629, and W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroom Electronic Law Journal* 1 at 4 – 5.

[47] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 133 – 135: function of automatically processing data by search engines on third-party websites is carried out by so-called web crawlers, these are programmes created by search engines to automatically search and browse the internet in order to collect, index and store information, irrespective of whether the information is personal information/data or not.

[48] An Internet Protocol address or IP address is a unique identifier which is assigned to each internet compatible device, whether mobile, laptop or computer. See *Breyer v Bundesrepublik Deutschland* EU:C:2016:779 para 15, and E Larson 'Tracking criminals with internet protocol addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 at 317 – 321.

[49] C Röttgen, 'Like or Dislike—Web Tracking' in T Hoeren, & B Kolany-Raiser (eds) *Big Data in Context* (2018) at 74, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629, W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroom Electronic Law Journal* 1 at 3 – 5.

[50] Opinion of Advocate General Szpunar, in *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* EU:C:2019:246, delivered 21 March 2019 paras

must be actively warned of the use of cookies and a pre-check tick box is therefore insufficient.[51]

(f) Conclusion

The main definitions or issues dealt with here all directly impact the right to privacy and the protection of personal information. Algorithms will feature more often in this thesis than the other definitions discussed above because the leading judgment that brought about the right to be forgotten relied on algorithms to practically implement the right to be forgotten.[52] The next section briefly describes the concept of the right to be forgotten.

III THE RIGHT TO BE FORGOTTEN

(a) Introduction

Data/information is collected for a myriad of reasons, how the data/information is collected, or and further related terms will be discussed later within this chapter. The focus of this part is to explain the main concept that this thesis will focus on, namely the right to be forgotten. The right to be forgotten has been put forward as a possible solution that individuals can use in protecting their privacy. Further solutions include (but this is not a complete list, as these concepts are not the focus of the thesis, but will be mentioned and discussed in light of the main topic): completely removing the information and ordering its destruction, or installing a paywall,[53] to limit the access thereof. Briefly, the right to be forgotten is somewhat of a misnomer, because the information is still available on the internet, but it is disconnected from the most popular search term that may be used to find, ie the person's name. But this will be explained more fully hereunder.

Unfortunately, as will be described later in this chapter, with cybercrime, once personal information is found on the Dark Web, there is very little that one can do to have that personal information removed. However, there is still hope, most information that individuals look for about others is generally available on the "normal" internet, and can be accessed through a

36 – 40, the paraphrase is specifically from paras 36, 37 and 39. *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C:2019:801,

[51] *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C:2019:801.

[52] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[53] The editors of the *Merriam-Webster.com dictionary* define a "paywall" as "a system that prevents Internet users from accessing certain Web content without a paid subscription". Merriam-Webster 'Paywall' *Merriam-Webster.com dictionary*. *https://www.merriam-webster.com/dictionary/paywall* (Accessed: 25 November 2023).

search engine such as Google, Yahoo, Bing, Firefox, etc. The former Canadian Privacy Commissioner, Daniel Therrien,[54] has opined on the ease with which one can obtain information, via the internet, with the use of search engines. With the same amount of ease, the information, even if out of context due to inaccuracies, can be reproduced and stored across multiple servers, making it difficult to delete.[55]

Where data subjects themselves are the authors of the information, the best solution is to "think before you post". However, as not all information is authored or posted by a data subject, the right to be forgotten has been praised as a solution to solve the perpetual memory of the internet.[56] However, as will be described later in the chapter, not all information that is placed on the internet about an individual is actually created by the individual that is the subject of that information.

The right to be forgotten in essence requires a search engine (the request is generally aimed at search engines, as will be discussed later in the thesis) to de-linking or de-indexing the information where the search term used is the person's name. A further concept to keep in mind, because it is closely linked to the right to be forgotten is the "notice and take down", as this request (often made to publishers and operators of websites) requires that information be completely removed or "taken down".[57]

(b) Maybe not that new

The right to be forgotten has been seen, in recent times, as "the new kid right on the block", especially in light of the explosion of information that is now available on the internet – whether it be news platforms, or social media web pages. However, the right to be forgotten is not necessarily a "new right" *per se* as it has been a part of society's fabric in other forms.[58] These include the automatic expungement of criminal records after an effluxion of time (this could be a specified amount, or a reasonably long enough period), allowing convicted persons to

[54] Danie Therrien was the Canadian Privacy Commissioner 5 June 2014 – 3 June 2022, the current Privacy Commissioner is Philippe Dufresne, see 'Privacy Commissioners'. *https://lop.parl.ca/sites/ParlInfo/default/en_CA/People/OfficersParliament/privacyCommissioner* (Accessed: 27 April 2024).
[55] Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018).
[56] JS Van Oyen, M Lange & S Kreinsen, 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 at 307. See also *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 145.
[57] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 48, 59-60. See *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317 regarding the "right to be forgotten" and *Biancardi v Italy* [2021] ECHR 972 which required that the information be completely removed from the website.
[58] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015).

integrate and be rehabilitated fully into society, without a criminal misdemeanour still being held against them, especially where they have lived crime free for a number of years.[59] News is seen as a "perishable commodity" – what may be the main headlines this week will no longer captivate the interests of society the next day or the next week or the next month. As such the headlines and those individuals that have made the headlines, unless it is a public person, such as an actor or actress or singer, etc., or the event has left an indelible mark in human history, will most likely not be pertinently remembered.[60]

(c) What is the "right to be forgotten"?

Briefly explained, the right to be forgotten is a response to[61]

> "the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person [making] access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's [i.e. the individual's] fundamental right to privacy than the publication on the web page."

In the strictest sense, the right to be forgotten, which is a romantic form of the name, is strictly a request that information pertaining to, and displayed on a results page, on a search done using an individual's name, be de-listed or de-indexed. This is the narrow interpretation of the right.[62] Practically, this is achieved with the programming of algorithms. These algorithms are then designed or programmed to avoid displaying the unwanted information about a person on the results page, where the person's name is used as the search term.[63] The result of such de-listing

---

[59] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 4; Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018). With regards to South African law, this procedure is governed by sections 271A – 271D of the Criminal Procedure Act 51 of 1977.

[60] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 4 – 5.

[61] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 87, Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 59, and T Bertram, E Bursztein, S Caro *et al* 'Five years of the right to be forgotten' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*) (11 – 15 November 2019, London, United Kingdom) 959 at 959.

[62] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 1 and 32; Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 59; *GC & others and Commission nationale de l'informatique et des libertés (CNIL)* (Case C-136/17) EU:C:2019:773 para 46.

[63] B Malle, P Kiesberg, E Weippl & A Holzinger 'The Right to be Forgotten: Towards Machine Learning on Perturbed Knowledge Bases'. *https://www.researchgate.net/publication/306386339_The_Right_to_Be_Forgotten_Towards_Machine_Learning_on_Perturbed_Knowledge_Bases/link/5b387ac1a6fdcc8506e3cb73/download*; accessed 11 July 2019. See *GC & others v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773 para 78.

or de-indexing will make the information more difficult to find, especially where the easiest form of searching for such information may be using the individual's name.[64] The right to be forgotten has been referred to as the right to erasure,[65] as well as the right to oblivion.[66] There will be instances where the de-linking or de-indexing will be enough, but due to the nature of the information or the mere fact that the information displayed is incorrect or inaccurate, a further step may be required. In such instances, the appropriate remedy is to completely remove and destroy the information.[67]

The right to be forgotten gained prominence due to the 2014 CJEU's Grand Chamber decision in *Google Spain*.[68] The court placed the right to be forgotten within the purview of privacy law. However, the right to be forgotten is not an absolute right in terms of the EU Data Protection Directive 95/46/EC,[69] and must be balanced against all the relevant rights and freedoms of those involved in the litigation, including the rights and freedoms of the general public to impart and receive information.[70] The approach has been endorsed by the Queen's Bench in *NT1 & another v Google LLC & another*,[71] where various key features of the right to be forgotten were clarified and applied, including the grounding of the right to be forgotten in privacy law.[72] The CJEU has expanded on its approach in *GC & others and Commission nationale de l'informatique et des libertés (CNIL)*[73] and *Google LLC and Commission nationale de l'informatique et des libertés (CNIL)*.[74]

---

[64] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 17; Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018). See also *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 87; *NT1 & another v Google LLC &another* [2018] EWHC 799 (QB) para 32; Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 59.

[65] Article 17 of the General Data Protection Regulation, and Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 59.

[66] NN Gomes de Andrade 'Oblivion: The Right to be Different … from Oneself: Reproposing the Right to be Forgotten' (February 2012) 13 *IDP* 122 at 123, the right to forgotten / oblivion is translated as *droit à l'oubli* (French) or *diritto al'oblio* (Italian), and PA Bernal 'A Right to Delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 2.

[67] Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018); Article 17 of the General Data Protection Regulation (EU) 2016/679 (the GDPR).

[68] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. Also discussed in *GC & others v Commission nationale de l'informatique et des libertés (CNIL)* (Case C-136/17) EU:C:2019:773 and *Google LLC and Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.

[69] 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 (Directive 95/46).

[70] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 13.

[71] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB).

[72] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 13.

[73] *GC & others v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773.

[74] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.

The CJEU found in *Google Spain*, with regards to the use and application of the right to be forgotten and in light of the facts, that it is certainly easier to obtain information concerning an individual based on a search using their name as the search term.[75] Furthermore, that search engine operators will still be obliged, even where the information is not removed from the website of the third-party publisher, to remove the unwanted links on results pages where the search term used is the name of the data subject.[76] The essence of the request, according to the CJEU is that persons do not ask that the information, that is strictly speaking accurate, be completely removed, but merely that where a search is done using the individual's name as the search terms, that the undesired or unwanted information no longer displays in the search results page – this has been described as being "forgotten" in the "narrow sense". The individual is not asking the media or those that have published the accurate information to remove the information from their website, only that the information is no longer displayed on the results page of the internet search engine (eg Google, Yahoo, etc.).[77]

Put differently, individuals are asking that search results display the current legal position and not a historical version of themselves. In some instances, it will suffice for the search engine to adjust the search results to display the information in chronological order, with the most current information at the top of the list.[78]

There are a number of clear positions when it comes to the right to be forgotten, ie, the right to be de-listed or de-indexed in regards to information found on the internet, when a search is done on an individual's name.[79] The "so-called right" allows for information to be removed that no longer serves a legitimate purpose or where the retention of such information may cause harm to the individual. However, the right to be forgotten is not found in traditional human rights instruments, although the aim of the right is to protect privacy, and in certain instances, reputation or dignity.[80]

---

[75] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 87. See also I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) 302 – 304.
[76] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88.
[77] *NT1 and another v Google LLC and another* [2018] 3 All ER 581 para 38.
[78] *GC & others and Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773 para 78, see also para 52. T Bertram, E Bursztein, S Caro *et al* 'Five years of the right to be forgotten' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*) (11 – 15 November 2019, London, United Kingdom) 959 at 595, where the authors that data subject de-listing/de-referencing requests are mainly in relation to personal information found on the following websites: social media, directory services, news outlets and government websites. For an in-depth breakdown of what is de-listed, see Bertram *et al* from page 963 onwards.
[79] In terms of data protection laws, an individual is known as a "data subject".
[80] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 4; J Auloos 'The 'Right to be Forgotten' – Worth remembering?' (2012) 28 *Computer Law & Security Review* 143

(d) The legal framework

The right to be forgotten was formulated in *Google Spain*[81] using Articles 12*(b)* and 14*(a)* of Directive 95/46. Since 25 May 2018, Directive 95/46 has been replaced with General Data Protection Regulation (EU) 2016/679 (the GDPR). Article 17 within the GDPR provides for the right to be forgotten.

In accordance with *Google Spain*[82] the CJEU recognised that a right to be forgotten did exist in terms of Directive 95/46. This right to be forgotten has not been fully codified in the GDPR.[83] The right to have information erased due to inconsistencies or falsity, etc. appears in both Directive 95/46 and the GDPR. At first blush, both legislative instruments provide clear provisions for individuals, referred to as data subjects, to have information completely deleted or taken down – depending on the circumstances in terms of the request. Certainly, what can be pointed out at this stage is that the new Article 17 of the GDPR is far more clearly articulated than its predecessor. This will be fully explored in the thesis.

This raises the question: how much data is being collected, retained and then distributed or uploaded on to the internet or used with or without the consent of individuals? The reason for this is that the right to the protection of personal data or information forms a part of the right to privacy. The right to be forgotten is a remedy that assists in the protection of privacy, specifically the protection of personal data or information. To provide some background on where the right to be forgotten, as a remedy in the protection of personal data or information, fits in the following describes and explains some instances (is not a closed list) where data is collected, and uploaded onto the internet.

IV INFORMATION/DATA AND PROTECTING HUMAN RIGHTS

(a) Some general thoughts

Illicit data gathering compounds the problem mentioned in the question above. The internet has certainly complicated the protection of human rights in the digital age.[84] Social media

at 144-146.

[81] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[82] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[83] 'GDPR: Right to be Forgotten', available at *https://gdpr-info.eu/issues/right-to-be-forgotten/*; accessed 25 March 2019.

[84] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (6 April 2018) UN Doc. A/HRC/38/35 para 44ffg, and D Ayala 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 212.

websites and technological devices, with the combined use of data gathering, storage and analysing services, have affected the rights to privacy and freedom of expression.[85] Individuals may not intend for shared information to be made public. The shared information may be aimed only at a limited number of people or only at one person and any unauthorised distribution or use of such information may infringe various human rights, not merely the rights of freedom of expression and privacy.[86]

By way of example, but not the focus of the thesis, Zunger's words, quoted above, were a direct reflection of how easy it was for Facebook, Cambridge Analytica and their clients, without the necessary consent, to collect and subsequently use the data of a large number of Facebook users (anywhere in the range of 50 to 87 million users). The data was "surreptitiously" gathered (referred to as "harvested"), with the intention to analyse and thereby sway opinion in the presidential elections in the United States of America.[87] In their defence, it was stated that the data used was collected from those who had taken part in a voluntary survey. However, data or information was also "gathered" from those who had declined to answer the questions.[88] Perhaps the most sinister part of this campaign was that even those individuals who did not have a Facebook account were not "protected" or "immune" from the Cambridge Analytica/Facebook scandal.[89] Facebook tracked non-Facebook users through cookies that were hidden in beacons across websites. With the assistance of algorithms created by Cambridge Analytica, Facebook, or their clients, used "real-time monitoring" and tracked which services individuals clicked on, whether it was a link from Facebook or one of its partner

[85] J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and $$ (2018) August *Computer* 56 -57. See also *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791 para 120 – 122, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258 para 48.

[86] The extensive arguments in *NM & others v Smith & others* 2007 (5) SA 250 (CC), focused on that persons may impart information for a specific reason, ie the freedom to impart with that information on terms or in a situation or circumstance as they may decide and not for the free distribution thereof – hence the element of privacy that is still involved.

[87] Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe*, dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019), see also the general comments made in UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (11 May 2016) UN Doc. A/HRC/32/38 paras 25 – 26. See also the following enlightening discussion: P Bernal 'Facebook: Why Facebook makes the fake news problem inevitable' (2018) 69 *Northern Ireland Legal Quarterly* 513 – 530.

[88] J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 56.

[89] J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 58, and D Ayala 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 213. See also P Bernal 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1(2) *Journal of Cyber Policy* 243 at 246 – 252.

companies or subsidiaries, on which a Facebook logo appeared.[90] Brown points out that Facebook cooperated with Cambridge Analytica.[91] Bernal, with a focus on Facebook, explained by invading individual privacy, and also analysing the data/information provided on its site by various individuals and groups, was able to curate information or "news" that was used to target individuals in the form of personalised messages or content (a mixture of real news and misinformation). The curated "news" was designed around an individual's preferences and fears.[92] This certainly places a new perspective on the need to protect the rights of freedom of expression, privacy and dignity, and places a new light on the ideas surrounding the right to be forgotten.[93]

In a 2011 Report on the Promotion and Protection of the Right to Opinion and Freedom of Expression, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression expressed concern over the growing use of cookies and internet trackers which adversely impact human rights, especially with respect to the right to privacy:

> "The Special Rapporteur is concerned that, while users can enjoy relative anonymity on the Internet, States and private actors have access to technology to monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of Internet users' right to privacy, and undermine people's confidence and security on the Internet, thus impeding the free flow of information and ideas online."[94]

Furthermore, the Special Rapporteur emphasised that "[the] United Nations, regional organizations and treaty bodies have affirmed that offline rights apply equally online".[95] The problem lies in the nature of the internet and the fact that private companies control many of

[90] J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 56 and 58, and Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe,* dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019).
[91] AJ Brown '"Should I stay or should I leave?": Exploring (dis)continued Facebook use after the Cambridge Analytica scandal' (2020) 6(1) *Social Media + Society* 1 at 1, see also J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at at 57.
[92] P Bernal 'Facebook: Why Facebook makes the fake news problem inevitable' (2018) 69 *Northern Ireland Legal Quarterly* 513 – 530.
[93] J Isaak and MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) August *Computer* 56 at 56 and 58, and Y Zunger 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe,* dated 22 March 2018, *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019).
[94] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (16 May 2011) UN Doc. A/HRC/17/27 para 82.
[95] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (6 April 2018) UN Doc. A/HRC/38/35 para 1, and Access Now *Human rights impact assessments for AI: analysis and recommendations* (October 2022) at 5 – 6.

the platforms, search engines and websites used by individuals. Furthermore, States are not creating enough legal incentives for private companies to protect human rights.[96]

There are instances where States have begun to adopt laws that protect human rights, especially privacy on the internet, seeking to contain the damage that leaking sensitive information or data would cause. However, some non-governmental or human rights organisations have now begun to refer specifically to "digital human rights" as a category of rights that are of specific importance in respect of the internet. With respect to digital human rights, the technology that makes the internet key to the free flow of information is the same technology that may be used to stifle and restrict freedom of expression in favour of privacy.[97] These organisations bemoan the fact that the technology used to facilitate the free flow of information across the internet is the same technology used to restrict the flow of information. The technology referred to is the use of algorithms.[98]

(b) Cybercrime

It is worth noting the following at this stage in terms of cybercrime or hacking. Hacking is not merely the act of breaking into the system of a person, company, or government department and removing personal information, but it is also possible to install malware that destroys databases, or spyware to run in the background, ie without the knowledge of the user.[99] Hacking severely intrudes on the right to privacy and becomes a general security risk for the individual, especially with regard to sensitive information, such as banking details, email communications and other documents.[100] In some instances, criminals may hack and install ransomware in a

[96] UNHCR, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (6 April 2018) UN Doc. A/HRC/38/35 para 1. See also the report by Access Now *Human rights impact assessments for AI: analysis and recommendations* (October 2022). A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 – 133, the article outlines some of the main rights, many of which feature in this thesis and how these are affected by the internet and what mechanisms may be considered to protect them.

[97] See 'Digital Rights' available at *https://www.article19.org/issue/digital-rights/* (Accessed 15 April 2019).

[98] See 'Digital Rights' available at *https://www.article19.org/issue/digital-rights/* (Accessed 15 April 2019). E Esposito 'Algorithmic memory and the right to be forgotten on the web' (2017) April 4(1) *Big Data & Society* 1 – 11 – the author, not only describes how algorithms are used in their function of retrieving and remembering, but also, the law makers are trying to, through the use of technology, such as algorithms, to encourage the internet's ability to forget (see at 5).

[99] MA Dennis 'cybercrime' *Encyclopedia Britannica*, 25 August 2022, *https://www.britannica.com/topic/cybercrime* (Accessed: 7 December 2022). Malware is derived from 'malicious software', which includes 'viruses, trojans, spyware, and worms.' See WL Hosch 'malware' *Encyclopedia Britannica*, 30 Sep. 2022, *https://www.britannica.com/technology/malware* (Accessed: 8 December 2022). For further definitions, see generally *Encyclopedia Britannica*. See as an example of an active hacking group that acts as a "Robin Hood" between governments and their citizens: S Alexopoulou & A Pavli '"Beneath this mask there is more than flesh, beneath this mask there is an idea": Anonymous as the (super)heroes of the internet?' (2021) 34 *International Journal for the Semiotics of Law* 237 – 264.

[100] D Kahvedžić 'Cybercrime investigations of mobile phone devices and the cloud in the light of EU safe harbour

computer network system. The ransomware encrypts the documents and network users are then unable to access their encrypted records and files and data. The criminals demand ransom money (often in the form of a cryptocurrency, ie, Bitcoin, to make it difficult to trace into which accounts the money is transferred) to unlock and restore the system.[101] Alternatively, the ransom money is demanded, otherwise the personal data/information will be released on the Dark Web, making it available to all who use the Dark Web.[102] This creates havoc, especially in light of the reported instances committed against hospitals in England and companies and organisations in other parts of the world, such as Spain, Russia, Taiwan, Ukraine and India, and later affecting Germany, Japan and China.[103]

It goes without saying that cybercrimes are able to infringe on the rights and freedoms of all individuals.

South Africa (SA), in order to protect rights and freedoms against cybercrime,[104] has partially enacted the Cybercrimes Act 19 of 2020 on 1 December 2021.[105] The Cybercrimes Act has a wide jurisdiction to aid in investigating and prosecuting cybercrimes that are committed inside and outside of SA's borders against SA citizens, private and state-owned organisations or companies.[106] The Cybercrimes Act provides for cyber-related crimes that

---

rulings' (2016) 17 *ERA Forum* 355 at 365, LM Tanczer '50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers' (2020) 41(1) *Contemporary Security Policy* 108 at 111, and MA Dennis 'cybercrime' *Encyclopedia Britannica*, 25 August 2022, *https://www.britannica.com/topic/cybercrime* (Accessed: 7 December 2022).

[101] T Jordan 'A genealogy of hacking' (2017) 23(5) *Convergence: The International Journal of Research into New Media Technologies* 528 at 536 – 537, and MA Dennis 'cybercrime' *Encyclopedia Britannica*, 25 August 2022, *https://www.britannica.com/topic/ cybercrime* (Accessed: 7 December 2022).

[102] E Reddy 'Policing the Onion Router (Tor) crypto-markets on the dark web: An analysis of South African investigatory powers' (2023) 36(3) *South African Journal of Criminal Justice* 406 – 433 in light of the relevant browser or router as well as how the Dark Web operates, with specific references to hacking and police surveillance and crime fighting methods.

[103] A Griffin 'NHS Hack: Cyber attack takes 16 hospitals offline as patients are turned away', *Independent*, dated 12 May 2017, *https://www.independent.co.uk* (Accessed: 14 June 2019), C Graham 'NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history', *The Telegraph*, dated 20 May 2017. *https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransom ware-offensive/* (Accessed: 14 June 2019). See also MS Karim 'Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?' (2022) 143 *Marine Policy* 105138 on how cybersecurity breaches may affect an entire industry.

[104] See the preamble to the Cybercrimes Act 19 of 2020. For a discussion of the Cybercrimes Act see SS Ka Mtuze 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43(3) *Obiter* 536 at 568 – 569.

[105] Proc R42 in *GG* 45562 of 30 November 2021.

[106] Section 23 of the Cybercrimes Act 19 of 2020. Regarding the challenges of monitoring, investigating and later prosecuting in terms of such a wide jurisdiction, see S Dlamini & C Mbambo 'Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses' (2019) 5(1) *Cogent Social Sciences* 1675404. For a discussion of how AI is increasingly used in cybercrime related offences, see H Chitimira and P Ncube 'The regulation and use of Artificial Intelligence and 5G technology to combat cybercrime and financial crime in South African Banks' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 34.

include hacking (although not directly mentioned in the Cybercrimes Act) and for various related offences, including cyber-forgery, fraud and extortion. It also includes the sending of intimate malicious data communications or messages, which may contain a threat to commit violence or damage to property. The Cybercrimes Act also provides for protection orders in relation to the last-mentioned crimes.[107] The Cybercrimes Act works with the Protection of Personal Information Act 4 of 2013 (POPI) to strengthen compliance with the protection of personal information as stipulated within POPI and strengthen the enforcement mechanisms within POPI. The Cybercrime Act creates criminal penalties, whereas POPI provides civil remedies, for similar data breaches.[108]

To round off hacking, it is interesting to note that there are hackers that hack with the intention of exposing possible data breaches, thereby forcing governments and companies to take the protection of personal as well as other sensitive information seriously.[109] Not all hackers are out there to disrupt and destroy, some are, on their own account, wanting to assist.[110]

However, there are legal means to obtain information, including personal information. The ability to obtain information that is public, and/or private, is often as simple as using an internet search engine, such as Google, Yahoo, Bing, or Duck Duck Go. One of the most common phrases that people say is that if they don't know something, they simply "Google it" or "ask Uncle Google" to find the answer.

Cybercrime will not be discussed any further in this thesis, unless it relates to the topic of the right to be forgotten, data protection, and privacy or any of the main themes covered in

---

[107] See Chapter 2 of the Cybercrimes Act 19 of 2020, and L Astfalck, N Britton, C MacRoberts & E Van Der Vyver 'Cybercrimes Act: Cybercrimes are enforceable criminal offences in South Africa with effect from 1 December 2021' *Lexology*, 2 December 2021. *https://www.lexology.com/library/detail.aspx?g=d1d7d561-0687-416c-b3a3-fb2f0bfe16cc* (Accessed: 4 March 2023).

[108] SS Ka Mtuze 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43(3) *Obiter* 536 at 568 – 569 and R Byleveld 'A brief overview of the Cybercrimes Act 19 of 2020' FluidRock Governance Group, 15 February 2022. *https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/* (Accessed 4 March 2023).

[109] SH Chana & S Janjarasjitb 'Insight into hackers' reaction toward information security breach' (2019) 49 *International Journal of Information Management* 388 – 396, and LM Tanczer '50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers' (2020) 41(1) *Contemporary Security Policy* 108 – 128.

[110] LM Tanczer '50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers' (2020) 41(1) *Contemporary Security Policy* 108 – 128, and see D Cohen, A Elalouf & R Zeev 'Collaboration or separation maximizing the partnership between a "Gray hat" hacker and an organization in a two-stage cybersecurity game' (2022) 2 *International Journal of Information Management Data Insights* 100073 – the authors explain the different types of hackers, their aims and the reactions of organisations to how these hackers operate, especially with regards to the so-called grey hat hackers.

the thesis.

(c) Another thing . . . "Big Brother is Watching You": Surveillance

However, unknown to many, emails, social media posts, even phone calls and SMSs or WhatsApp, are not the only forms of data generated by individuals daily. Any individual with a cell phone has the ability to create data simply by moving from one cell phone tower to the next. This movement of the cell phone "logging" into different towers is a form of data known as metadata.[111] Metadata also includes IP addresses with respect to email connections. These IP addresses are used to track which computer an email was sent from.[112] Metadata is generally used to create a movement profile of an individual and is often most used in criminal investigations.[113] The fact that this data is created without much input from the individual or that it is a "by-product" of the main communication, has the benefit that criminals may be detected or successfully prosecuted, but this is a form of mass surveillance, and it affects the right to privacy of individuals, amongst other rights.[114] The National Security Agency in the United States vividly illustrated that based on the associations and the profiles created with the use of metadata, they can stop criminals before they can act. Alternatively, they are able to track them down with relative ease.[115] Other security agencies, including the United Kingdom, Canada and many other European countries, are increasingly using this form of data.[116]

---

[111] On the creation and concerns surrounding mobile location data see, D Franzen *et al* 'Am I private and if so, how many? Communicating privacy guarantees of differential privacy with risk communication' In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '22)* 7 – 11 November 2022, Los Angelse, California, United States of America) 1125–1139. See also D Bilchitz 'Privacy, surveillance and the duties of corporations' (2016) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 45 – 67 for the comprehensive discussion on the South African law, and for a specific discussion of surveillance in relation to the Protection of Personal Information Act 4 of 2013, see N Ismail 'Private closed-circuit television surveillance under the Protection of Personal Information Act 4 of 2013' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 20 – 37.

[112] Criminal investigations often include the use of metadata to track the perpetrators steps in the commission of the crimes, in other words, to place them either at the scene of the crime, but also to demonstrate if there was any prior preparation to commit the crime. See E Larson 'Tracking criminals with internet protocol addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 at 317 – 321, and M Zilka, R Fogliato, J Hron, B Butcher, C Ashurst & A Weller 'The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 1553 – 1569.

[113] *Shange & others v The State* [2017] 3 All SA 289 (KZP), see also Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 23 – 26, and E Larson 'Tracking criminals with internet protocol addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 at 317 – 321.

[114] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 23 – 26 and E Kosta 'Algorithmic state surveillance: Challenging the notion of agency in human rights' (2022) 16 *Regulation & Governance* 212 at 215. See also Y Jooste 'Surveillance capitalism as white world-making' (2021) 53 (1) *Acta Academica* 44 – 67.

[115] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 24 – General Counsel Stewart Baker's statement is 'we kill people based on metadata'.

[116] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the*

Furthermore, messaging services that offer end-to-end encryption for messages sent using the service, eg WhatsApp, are being placed under pressure by the so-called "Five Eyes" nations, ie the United States, the United Kingdom, Canada, Australia and New Zealand. The "Five Eyes" want the services to drop their guarantee of end-to-end encryption and allow the respective government security agencies to infiltrate private conversations in surveillance operations.[117] Jooste[118] and Bernal[119] both point out that surveillance has the potential to undermine democracy, as well as various human rights such as dignity, freedom of expression, and privacy, where there are no proper safeguards for the protection of rights in place.

The Global Positioning System or GPS, is not just a useful tool for travelling to new places but may also be used when tracking suspects of serious crimes.[120] In this instance, a transmitter is positioned, often on the vehicle of a suspect or another person linked to the suspect under investigation. The ECtHR has held that tracking with the use of GPS in creating a movement profile of the person under investigation does not infringe on the right to privacy, provided the investigators have obtained a court order to permit the use of GPS tracking, and is ultimately in proportion to the committed crime.[121]

Some countries have a mandatory data retention requirement, which means that any data collected, including metadata, must be retained for a certain period of time.[122] In some countries, this mass retention of data has been thwarted by public as well as judicial

Digital Age, (May 2016) at 24.

[117] IA Hamilton 'WhatsApp faces international pressure to hand over access to encrypted *chats' Business Insider South Africa*, 31 July 2019. *https://www.businessinsider.co.za/ encrypted-messaging-under-pressure-from-five-eyes-nations-2019-7* (Accessed: 5 August 2019). Note also R Perper 'Chinese citizens will soon need to scan their face before they can access internet services or get a new phone number' *Business Insider South Africa*, 10 October 2019. *https://www.businessinsider.co.za/china-to-require-facial-id-for-internet-and-mobile-services-2019-10* (Accessed: 11 October 2019).

[118] Y Jooste 'Surveillance capitalism as white world-making' (2021) 53 (1) *Acta Academica* 44 – 67, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 462, and 473 – 482.

[119] P Bernal 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1(2) *Journal of Cyber Policy* 243 at 245.

[120] *Uzun v Germany* [2010] ECHR 2263. For a summary on the international as well as South African perspectives in light of GPS and it's use in health care, see M Botes 'The use of geospatial surveillance data for public-health emergency and disaster management in South Africa: A review with legal recommendations' (2021) 3 *Tydskrif vir die Suid-Afrikaanse Reg* 474 – 503.

[121] *Uzun v Germany* [2010] ECHR 2263. See the discussion on closed circuit television cameras below, as well as the Chapter 4 on the South African law relating to surveillance of an individual during crime investigations. Compare with *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* (European Court of Human Rights) application no. 26968/16 (13 December 2022). See also MM Mswela 'Tagging and tracking of persons with albinism: A reflection of some critical human rights and ethical issues arising from the use of the global positioning system (GPS) as part of a solution to cracking down on violent crimes against persons with albinism' (2019) 22 *Potchefstroom Electronic Law Journal* 1 – 28 as an example where this is not solely used in criminal investigations, but for more controversial means.

[122] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age,* (May 2016) at 23- 24, these include the United States, the European Union, Australia.

opposition.[123] The use of mass surveillance was propelled into the headlines after Edward Snowden revealed the widespread use thereof by the intelligence agencies of the United States and the United Kingdom.[124]

In SA, this form of data must be retained for up to five years in terms of section 30(1)*(b)* of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (also referred to as "RICA").[125] By comparison, the CJEU ruled that Member States may not generally and indiscriminately retain metadata in the form of traffic and location data.[126] However, the CJEU provided that the traffic and location data may be retained for

[123] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 24, these include the Philippines and Paraguay.

[124] See *Big Brother Watch & others v The United Kingdom* [2021] ECHR 439 where the Grand Chamber agreed with the lower courts that per se, mass surveillance does not violate human rights, however it must meet certain requirements: (1) the use of an independent body to approve the application, and not the responsible minister. (2) The warrant must include the categories of communications to be examined with the requisite keywords to be used. (3) The list of so-called subject identifiers, which relate to the person under investigation had not been authorised. The Grand Chamber emphasised the need for judicial oversight to combat abuse of the system and that the law did not limit itself to mass surveillance in terms of preventing or investigating serious crimes. Further, Article 10 had also been violated due to the lack of safeguards, in terms of journalist's right to their sources, etc. See also P Bernal 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1(2) *Journal of Cyber Policy* 243 – 264, and M Zalnieriute '*Big Brother Watch and others v the United Kingdom*' (2022) 116(3) *American Journal of International Law* 585 – 592. Note the South African Constitutional Court judgment in *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* 2021 (3) SA 246 (CC) where the court held that bulk interception without the requisite directions and warrants was not authorised under Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) and the National Strategic Intelligence Act 39 of 1994 or under any other legal instrument, and the practice was thus unconstitutional. Note also *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702 which held that the retention of IP addresses from mass surveillance is permissible where a serious crime is being investigated. Interestingly, the Court of Justice of the European Union (CJEU) held that an IP address amounts to personal data, see *Breyer v Bundesrepublik Deutschland* EU:C:2016:779 para 25.

[125] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002. In *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* [2019] ZAGPPHC 384, Sutherland J declared that the 5-year retention period is not unconstitutional see paras 84 – 108. The period was not challenged in the Constitutional Court: *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* 2021 (3) SA 246 (CC) para 18. See also *Uzun v Germany* [2010] ECHR 2263, and *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702. See also S Shanapinda 'Asymmetry in South Africa's regulation of customer data protection: Unequal treatment between mobile network operators (MNOs) and over-the-top (OTT) service providers' (2019) 23 *The African Journal of Information and Communication (AJIC)* 1 at 5 – 12.

[126] *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702. Note, Article 2*(b)* of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) defines "traffic data" as meaning:

> "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".

Article 2*(c)* of Directive 2002/58/EC defines "location data" as meaning:

> "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

However, see D Ayala 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 214.

criminal investigations and prosecutions.[127]

The High Court of England and Wales approved the use of Automated Facial Recognition technology in the use of crime detection for its ability to positively and accurately detect criminals that have been involved in major crimes – a part of the judgment dealt with the issues surrounding data protection and the violation of the right to privacy.[128] The High Court of England and Wales found that it was necessary for the speedy and accurate identification of criminals (DNA and fingerprint evidence were met with a similar resistance when they were first used) that had been involved in various crimes, ranging from minor offences all the way to murder, and other serious crimes.[129] Based on the evidence before it, the Queen's Bench held that the processing of biometric facial data and the policies for storing, destruction as well as any other aspects in the light of data protection had met the safeguards as provided in the UK's Data Protection Act 2018.[130] Cases dealing with data protection in instances where there has been a collection of such via mass surveillance are on the rise.[131]

In terms of surveillance, a very fitting 80s pop song comes to mind, as many individuals possibly think that they "always feel like somebody's watchin' me".[132] Closed-circuit

---

[127] *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson & others* EU:C:2016:970 para 112, see also *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & others and Kärntner Landesregierung & others* EU:C:2014:238, *The Queen on the application of The National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department & another* [2018] EWHC 975 (Admin), *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258 and M White 'Is the incompatibility of UK data retention law with EU law really a victory?' (2021) 41(1) *Legal Studies* 130 – 155.

[128] *The Queen (on application of Bridges) v Chief Constable of South Wales Police & others* [2019] EWHC 2341 (Admin) paras 45 – 108. For a commentary on this case see BJ Gordon 'Automated facial recognition in law enforcement: *The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police*' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 30.

[129] *The Queen (on application of Bridges) v Chief Constable of South Wales Police & others* [2019] EWHC 2341 (Admin) paras 3 – 7; 45 – 108.

[130] *The Queen (on application of Bridges) v Chief Constable of South Wales Police & others* [2019] EWHC 2341 (Admin) para 148.

[131] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 23. See generally *The Queen (on application of Bridges) v Chief Constable of South Wales Police & others* [2019] EWHC 2341 (Admin).

[132] Genius Lyrics 'Rockwell – Somebody's Watching Me Lyrics' *https://genius.com/Rockwell-somebodys-watching-me-lyrics* (Accessed: 15 December 2022), D Gilson 'Michael Jackson & Michel Foucault walk into a bar' (2015) 143 *The Threepenny Review* 22 at 22 and for a history of the song and who are involved, see J Newman 'How "Somebody's Watching Me" Singer Rockwell created a paranoid pop classic' *Rolling Stone*, dated 7 December 2016. *https://www.rollingstone.com/music/music-features/how-somebodys-watching-me-singer-rockwell-created-a-paranoid-pop-classic-125907/amp/* (Accessed: 15 December 2022). Note, with the emergence of the "smart home" and the interconnectedness of daily tasks with the use of technology it may also create a feeling of being constantly watched: Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 473 – 482. It has been suggested that electronic devices that have no camera functions can even "watch" users, eg eReaders and smart phones or cellular phones, see MM Espino 'Sometimes I Feel Like Somebody's Watching Me... Read?: A comment on the need for heightened privacy rights for consumers of ebooks' (2013) 30(2) *UIC John Marshall Journal of Information Technology &*

television (CCTV) cameras, which are installed in shopping malls, businesses, government organisations, and educational institutions, etc. are a further form of surveillance.[133] Although they are generally installed as a crime prevention tool.[134] In light of the protection of fundamental rights and freedoms, the ECtHR has held that the installation of CCTV cameras in the workplace amounts to an interference with the personal sphere of the employee, especially where these are installed without the employees' knowledge.[135] A workplace is not limited to work or business-related interactions between employees, it also includes a certain amount of private interaction, ie outside the absolute inner circle. It is through their working lives that individuals have the greatest opportunity to develop relationships with others, and thus create a private social sphere. Hence, the covert use of CCTV cameras does interfere with the private lives of employees.[136] Employees must be informed of the reasons for using the CCTV cameras. These reasons may include (1) identifying any safety concerns due to the amount of public that enter the premises regularly; (2) the cameras are a crime deterrent; (3) are there any consequences for the employees, if they are caught disobeying company policies;[137] (4) and whether the cameras are necessary in light of the nature of the workplace.

Privacy Law 281 – 306, and R Toth & T Trifonova 'Somebody's Watching Me: Smartphone use tracking and reactivity' (2021) 4 *Computers in Human Behavior Reports* 100142.

[133] E Sychenko & D Chernyaeva 'The impact of the ECHR on employee's privacy protection' (2019) 12(2) *Italian Labour Law e-Journal* 171 – 188.

[134] G Saville 'Surveillance and crime prevention' (2004) 3 *Criminology & Public Policy* 493 – 496, EL Piza, BC Welsh, DP Farrington & AL Thomas 'CCTV surveillance for crime prevention' (2019) 18 *Criminology & Public Policy* 135 – 159, and for an actual study of the effect that CCTV cameras have on crime statistics for a city, namely Medellín, Columbia, see S Gómez, D Mejía & S Tobón 'The deterrent effect of surveillance cameras on crime' (2021) 40 (2) *Journal of Policy Analysis and Management* 553 – 571. Pietermaritzburg, KwaZulu-Natal, South Africa, has a similar system installed within the city centre, see Safe City Msunduzi NPC, *http://safecity.co.za/* (Accessed: 17 December 2022).

[135] *Köpke v Germany* [2010] ECHR 1725, *Antović and Mirković v Montenegro* [2017] ECHR 1068, and E Sychenko & D Chernyaeva 'The impact of the ECHR on employee's privacy protection' (2019) 12(2) *Italian Labour Law e-Journal* 171 – 188.

[136] *Antović and Mirković v Montenegro* [2017] ECHR 1068 paras 40 -45, see also *Köpke v Germany* [2010] ECHR 1725 and E Sychenko & D Chernyaeva 'The impact of the ECHR on employee's privacy protection' (2019) 12(2) *Italian Labour Law e-Journal* 171 – 188. Note also the discussion in *Lopez Ribalda & others v Spain* [2019] ECHR 752. However, in *Florindo de Almeida Vasconcelos Gramaxo v. Portugal* (European Court of Human Rights) application no. 26968/16 (13 December 2022), the ECtHR had to decide whether a geo-location device installed, with the employee's knowledge, in a company vehicle, which the employee was permitted to use for private trips, was an infringement of the employee's privacy. The device was installed to monitor both work and private related trips, so as to record who was responsible to pay the fuel costs for a specific trip with the use of the geo-location data. The employee was also required to compile a record of the trips he used the vehicle for, and when. The employee was a medical representative and was required to travel to see customers. The court acknowledged that geo-location data does amount to personal data, however, the installation of the geo-location device to monitor the employee's movements was not a violation of the right to privacy, as the devise was to act as a back-up and confirm the employee's records as to when the vehicle was used for work or private trips, and who was reposnsible for the payment of fuel and when. See also Chapter 4 of the thesis.

[137] Ie, the possibility of dismissal, based on the misconduct of the employee, and how such surveillance affects the rights of the employees in terms of data protection law, see *Lopez Ribalda & others v Spain* [2019] ECHR 752 para 116.

Where these considerations are met, then the interference with the rights and freedoms of the employees may be justified.[138]

The other form of surveillance mentioned above is cookies. Larson discusses in detail how cookies and other trackers are used to monitor and analyse the internet browsing habits of suspects via their IP addresses. Email communications are also monitored, ie the metadata therefrom is collected and analysed.[139] The arguments around surveillance are briefly explored in light of SA law in Chapter 4 of this thesis. Mass surveillance, where there is a link to the right to be forgotten, will only be discussed in that context and not in the context of the broader rights infringements that may occur – although these are of a very serious nature![140]

(d) Doxing

There is one other aspect to take note of, and this is called doxing. Doxing is distinct from the accidental or the incidental disclosure of facts in that information is published with malicious intent. The aim of doxing is to impede privacy, it may include photographs of persons, trade secrets, etc.[141] One of the issues that arise in this respect is when the data of an individual is released but the actions of that person have not warranted such exposure or release of personal data; what remedies does the person have to stop the disclosure or have the disclosure retracted, and claim compensation?[142] The harm is often the impairment of a person's reputation. Doxing does have a positive effect in that it uncovers or exposes corruption and identifies the perpetrators.[143]

---

[138] *Lopez Ribalda & others v Spain* [2019] ECHR 752 paras 87 – 95 and 109 – 137, and E Sychenko & D Chernyaeva 'The Impact of the ECHR on employee's privacy protection' (2019) 12(2) *Italian Labour Law e-Journal* 171 at 174 – 178.

[139] E Larson 'Tracking criminals with internet protocol Addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 – 358.

[140] *Uzun v Germany* [2010] ECHR 2263, *Big Brother Watch & others v The United Kingdom* [2021] ECHR 439, *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* 2021 (3) SA 246 (CC), Y Jooste 'Surveillance capitalism as white world-making' (2021) 53 (1) *Acta Academica* 44 – 67, and M Zalnieriute '*Big Brother Watch and others v the United Kingdom*' (2022) 116(3) *American Journal of International Law* 585 – 592.

[141] *OBG Ltd and another v Allan and others*; *Douglas and another v Hello! Ltd and others (No 3)*; *Mainstream Properties Ltd v Young and others* [2007] 4 All ER 545 para 255. See for a complete discussion on doxing: DM Douglas 'Doxing: A conceptual analysis' (2016) 18 *Ethics and Information Technology* 199 – 210, and D Trottier 'Denunciation and doxing: Towards a conceptual model of digital vigilantism' (2020) 21(3-4) *Global Crime* 196 – 212.

[142] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age,* (May 2016) at 51.

[143] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age,* (May 2016) at 51.

(e) Personal information/data is needed for . . . daily life

Personal data is generally needed to obtain something. In an application for various government documents, or even for a bank account or credit account, a certain amount of personal data must be provided to succeed. Online shopping often requires that a physical address be provided for delivery of the ordered items via courier. Depending on the options provided, online payments may require that credit card information be inserted for successful payment before the item(s) are packed and sent for delivery. As was briefly pointed out above, merely travelling through a city, with your cell phone in your pocket, where it logs into the various cell phone towers, creates data.[144] Even opening a social media account requires some personal information to create a profile.

In terms of a social media account, the personal information produced is processed and suggestions of possible connections are made.[145] An individual may customise and mark certain parts of their profile as private, alternatively that only certain persons will be able to read and comment on posts or opinions posted there.[146] Although an individual may control what they write or post on their profile, using Facebook as an example, an individual is unable to control what other Facebook users post about them and who has access to those posts.[147] These posts have led to defamation actions in SA and other countries, irrespective of the social media website on which they were written.[148] In Australia and England, defamation cases were successfully prosecuted where emojis were used.[149] It does not merely stop at comments, etc.,

---

[144] D Franzen *et al* 'Am I private and if so, how many? Communicating privacy guarantees of differential privacy with risk communication' In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '22*) 7 – 11 November 2022, Los Angelse, California, United States of America) 1125–1139.

[145] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 11 described this process as follows:

> "web-based [services which will require] individuals to:
> (a) construct a public or semi-public profile within a bounded system;
> (b) articulate a list of other users with whom they share a connection; and
> (c) view and traverse their list of connections and those made by others within the system.

See also paras 12 – 13. See also the following article, which was referred to in the judgment: A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129(2) *South African Law Journal* 375 – 402.

[146] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) paras 19- 20.

[147] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 21.

[148] *Isparta v Richter & another* 2013 (6) SA 529 (GNP) held it will also include a person that has been "tagged" in the post of the original author thereof – if they do not choose to remove the "tag" within a reasonable space of time they will automatically be associated with the post and hence they too will be liable for damages in a defamation claim.

[149] *Burrows v Houda* [2020] NSWDC 485, *Lord McAlpine of West Green v Bercow* [2013] EWHC 1342 (QB), and P Singh 'Can an emoji be considered as defamation? A legal analysis of *Burrows v Houda* [2020] NSWDC 485' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 26. *Encyclopedia Britannica* describes an emoji as

> "digital pictograms used widely throughout social media, texting, e-mail, and other computer-mediated communications. Emojis are used to express a range of objects and ideas, including human emotions, animals, geography, foods, and flags. The term emoji was born from two Japanese words: e, meaning 'picture,' and moji, meaning 'written character.'"

these posts may range from snide remarks of an ex-partner to revenge pornography.[150] These cases and similar issues with defamation on the internet, specifically in terms of social media websites are discussed later in the thesis.[151] It is important to note that the use of a social media account is not the only way to discredit and ruin the reputation of another person – a blog post, an online news article or any other form of online communication may be used. The information exposed may stem from legal and/or illegal means, ie via an interview, research or illegally through hacking.[152] Although there are specific categories of personal data that are classified as "sensitive" or "special", it is important to note that personal data is considered to be generally sensitive. This is because it is usually confidential and, in its nature, can be used easily to identify individuals. It follows, therefore, that speaking generally personal data should remain private and access thereto should be restricted as far as possible, in order to protect it from unauthorised use.[153]

V RESEARCH QUESTIONS AND A HYPOTHESIS

In terms of the topic: this being a critical analysis of the right to be forgotten in SA in light of the rights of freedom of expression and privacy, this thesis will set out, in detail, the CJEU's decisions in developing the right. The EU's framework and standards will be discussed and used to evaluate the SA constitutional position as well as POPI, and a possible way forward will be proposed. There will be a comparative element to the thesis, but in terms of what positions the countries have taken towards the right to be forgotten, ie the European Union and the United Kingdom have certainly preferred privacy over expression, unlike the United States

---

E Kendall 'emoji' *Encyclopedia Britannica*, 24 August 2022. *https://www.britannica.com/topic/emoji* (Accessed: 4 December 2022). There is a similar digital symbol called an emoticon, and this is defined as a

> "glyph used in computer-mediated communications that is meant to represent a facial expression in order to communicate the emotional state of the author. When the Internet was entirely text-based, between the late 1960s and the early 1990s, emoticons were rendered in ASCII and were read sideways, as the 'smiley' :-) indicates. The word emoticon comes from a combination of the words emotion and icon."

TM Senft 'emoticon' *Encyclopedia Britannica* 27 February 2022. *https://www.britannica.com/topic/emoticon* (Accessed: 4 December 2022).

[150] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 39 – 40.

[151] See Chapter 4 which deals with the rights of privacy and freedom of expression in the South African constitutional context. See also *Heroldt v Wills* 2013 (2) SA 530 (GSJ), *Isparta v Richter & another* 2013 (6) SA 529 (GNP).

[152] Hacking is discussed above. See also doxing discussed above. The information that may be exposed may include, but is certainly not limited to, phone numbers, addresses and banking details, etc., see J Le Blond 'German politicians' personal data leaked online' *The Guardian*, 4 January 2019. *https://www.theguardian.com/world/2019/jan/04 /german-politicians-personal-data-hacked-and-posted-online* (Accessed: 22 January 2019) and Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, at 50 - 51.

[153] See S Al-Fedaghi 'How sensitive is your personal information? In *Proceedings of the 2007 ACM symposium on Applied computing (SAC '07)* (11 – 15 March 2007, Seoul, Korea) 165 – 169.

of America. The EU's framework, as it was the main basis used in the development of POPI will be explained in some detail with references to other jurisdictions, where applicable. In order to achieve this aim, the following themes or questions will guide this discussion in dealing with the main topic:

(a) POPI, being based on Directive 95/46, does not have a specific right to be forgotten. Based on the arguments of the CJEU in *Google Spain* and comparing the relevant sections of POPI with Directive 95/46, the first issue to be investigated is whether POPI makes provision for a possible right to be forgotten for SA.

(b) The second question will be: what is the scope, content, or nature of the right to be forgotten? How have the statutory instruments defined the right to be forgotten? And how have the courts developed it? The case law that will be discussed will be drawn from the CJEU, the ECtHR and the various high courts in Europe and/or the EU. It will include a discussion of how they have further developed the principles as provided in *Google Spain*, as well as Article 17 of the GDPR. The established scope and content will be applied to POPI.

(c) One key consideration that will be analysed based on the current case law is the balancing of the right to be forgotten (as a part of the right to privacy) with that of freedom of expression. The courts, within the EU (as well as within Europe), took specific considerations into account when striking a balance between the two rights. The discussions and analysis will include investigating how the courts have dealt with personal data and the privacy continuum. Have the courts located personal data in the highly sensitive and private inner core of the continuum, or have they located it in the public outer reaches of the continuum? Also, how have the EU legislative instruments attempted to balance the rights of privacy with the right to freedom of expression? With regards to the SA perspective, what are the important considerations for striking a balance between privacy and freedom of expression, and how has the legislature tried to strike this balance?

(d) Lastly, are there any other important considerations that may have not been fully covered in the cases discussed, but would amount to useful considerations to keep in mind in the future, depending on the matters that arise before the courts? Keeping in mind that these considerations will have an impact on striking the balance between the right to be forgotten (as a form of privacy) and freedom of expression, as well as any

other specific rights, in order to achieve a fair outcome.

VI RATIONALE

The internet, as stated above, is one of the most disruptive, yet useful tools of our time, revolutionising how individuals can obtain information.[154] Furthermore, all individuals create data or information daily, whether it is by writing a text message in the form of an "SMS", "WhatsApp", or even a lengthy email. When obtaining official records kept at government departments, forms are completed to obtain specific documents, from driving licences to smart identification cards and passports or any other official documents. Often SA citizens require visas when travelling to Europe or America, and they will be required to produce personal information, such as identity numbers, passport numbers, whether they have enough money in their bank account, etc. to be issued with a visa.

An interesting feature fo the internet, and this too is disruptive, is that publishing of information, either by news websites, on blogs, etc., is no longer a singular or once-off event. It tends to be continuous, as it remains available long after it was initially published.[155]

The information requested in these forms is of a personal nature – it may include anything from banking details, proof of residence, cell phone numbers, identity numbers, and other personal information. This information is what individuals want protected, and fairly processed. If the information is leaked, intentionally, as well as accidentally, there should be adequate remedies available, to not only address compensation for damages for the inconvenience caused, but also for the further protection of the information that was leaked. Some data is incredibly sensitive, such as medical records. Individuals to whom it may pertain should have the right to have such data protected, and in the event that there is a danger that it may be exposed, possibly removed or withheld.

On a more personal note, the rhetoric of phone calls regarding the sale of cell phone numbers and the advertising pitches that follow on unsuspecting individuals is something that many people, myself included, find more irritating than useful. The fact that personal data has now become a commodity not only irritates but also means individuals are bombarded with calls at inconvenient times, causing stress. Apart from the aforementioned irritations, there is often a longing for personal information to remain out of the commercial stream and in the

[154] See 'Digital Rights' *https://www.article19.org/issue/digital-rights/* (Accessed 15 April 2019).
[155] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 193 and 240.

realm of privacy, where individuals may choose who may contact them and when such contact may occur. In many instances, private individuals do not want their personal information to be abused by search engines, various websites, etc. to track their movements or their preferences, in order to give them marketing or tailor-made information based on rumours, etc. as what happened in the Cambridge Analytica scandal.

AI is another area in which there is the potential to abuse personal information.

VII COMPARATIVE STUDY

The focus of the study is a critical analysis of the right to be forgotten in light of the rights of freedom of expression and privacy. The data protection laws that were previously, or that are currently, in force in the European Union (EU) inspired the SA legislation or at least a part of it. Since the repeal of Directive 95/46, the GDPR has been regarded as the global standard in data protection legislation. The European Parliament and the Council, in drafting the GDPR, have tried to find a middle ground, in protecting the rights to privacy and data protection, bearing in mind the right to freedom of expression. The decision of the CJEU in *Google Spain*[156] has had far-reaching consequences within the data protection landscape and in the development of the right to be forgotten.[157]

The internet, in essence, is a global, borderless tool; hence, extraterritorial legal regulation is a frequent possibility. By linking its data protection laws to its market power, the EU has become a global leader in the area of data protection.[158] The EU data protection laws are also much more restrictive than other jurisdictions.[159] Third-party countries to whom personal data is transferred must, in terms of the GDPR, have similar data protection standards.[160]

---

[156] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[157] Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 464.
[158] G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 465 – 466.
[159] G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 465 – 466.
[160] See as an example *Schrems v Data Protection Commissioner* EU:C:2015:650, *Data Protection Commission v Facebook Ireland and Maximillian Schrems* EU:C:2020:559, C Lam 'Unsafe harbor: The European Union's demand for heightened data privacy standards in *Schrems v. Irish Data Protection Commissioner*' (2017) 40(3) Electronic Supplementary *Boston College International and Comparative Law Review* 1 – 13, M Rotenberg '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26 *European Law Journal* 141 – 152, P Nebbia 'The *Schrems* judgments: A silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336, and MH Murphy 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) 71 *International and Comparative Law Quarterly* 245–262.

The GDPR has been labelled the new "gold standard", even in the field of surveillance, where companies originally from outside of the EU, that operate within the EU will need to implement "costly changes to [their] practices" where they are "dealing with data related to European citizens".[161] The GDPR carries hefty fines and penalties.[162] In terms of surveillance, the data collected, especially in light of big data, and the further processing as well as selling of that data, is a lucrative business. Surveillance is conducted through tracking, ie through the use of cookies. The data collected through the use of trackers (ie cookies) is often used to predict advertising patterns. Internet search engines use this data to sell advertising space.[163] It is practices such as these that are regulated by the GDPR as a part of the growing body of data protection legislation in the EU.[164] Consequently, Directive 95/46, and subsequently the GDPR, have had a wide influence.[165]

However, the EU's market power is not the only reason for the wide reach of the EU data protection regimes. The CJEU applied and/or applies the principles of Directive 95/46 and the GDPR strictly.[166] The CJEU holds Member States' Governments (including national, regional and local governments or government departments), as well as private companies, etc., accountable in terms of the GDPR.[167] For data subjects or individuals, it is important that a controller or processor who processes their personal information is held to account, especially

[161] J Andrew & M Baker 'The General Data Protection Regulation in the age of surveillance capitalism' (2021) 168 *Journal of Business Ethics* 565 at 565.
[162] J Andrew & M Baker 'The General Data Protection Regulation in the age of surveillance capitalism' (2021) 168 *Journal of Business Ethics* 565 at 565.
[163] J Andrew & M Baker 'The General Data Protection Regulation in the age of surveillance capitalism' (2021) 168 *Journal of Business Ethics* 565 at 568 – 569. Note also S Huneberg & K Berry 'Big data and the paradigmatic shift from passive insurer towards risk personalisation' (2022) 2 *Tydskrif vir die Suid-Afrikaanse Reg* 283 at 290 – 304, and XZ Pang 'Civil law protection of personal information in the era of big data' (2021) 8 *Open Access Library Journal* e8016 at 1 – 12. Internet websites will offer their services for "free", however, internet user's will "pay" with the personal data/information that the website collects with the use of cookies, whilst the internet user is on, and in certain off, the website – see E Mik 'Contracts governing the use of websites' (2016) *Singapore Journal of Legal Studies* 70 – 94.
[164] See generally the BGH, Urteil vom 23. Juni 2020 – KVR 69/19 – *Bundeskartellamt v Facebook*, I Graef, D Clifford, & P Valcke 'Fairness and enforcement: Bridging competition, data protection, and consumer law' (2018) 8(3) *International Data Privacy Law* 200 – 223, and J Andrew & M Baker 'The General Data Protection Regulation in the age of surveillance capitalism' (2021) 168 *Journal of Business Ethics* 565 at 570 – 573.
[165] Directive 95/46 was the first most comprehensive data protection legislation. P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 131, G Buttarelli 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 at 77, and G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 465 – 468.
[166] G Buttarelli 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 at 77.
[167] G Buttarelli 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 at 77 – 78.

where their human rights are infringed during the processing activities.[168] The strict application of both Directive 95/46 and the GDPR affects international business relations, and may even prevent certain business relations where the CJEU is of the opinion that the third country, to which data is transferred, does not have the same or similar data protection standards, as the EU.

This has led to countries, like SA, modelling their data protection legislation on the EU's model, so as to encourage the continued business relations between SA and the EU.[169]

The thesis will focus on the SA Protection of Personal Information Act 4 of 2013 (POPI), as commenced on 1 July 2020, specifically the right to be forgotten and its effect on the rights of freedom of expression and privacy in the SA context. A SA right to be forgotten will be conceptualised and analysed against the decisions of the EU.

Although the focus of the comparative study will be the EU's legislative regime and its interpretation and application of the right to be forgotten, where necessary, reference may be made to other legal jurisdictions, such as the United States and Canada. Like South Africa, the rights to privacy and freedom of expression have been included in both the United States Bill of Rights and the Canadian Charter of Rights and Freedoms. The manner in which the American and Canadian courts have interpreted and applied these rights has been referred to by the South African courts, including the Constitutional Court, on many occasions.

In evaluating the right to be forgotten, criticisms and positive attributes will be discussed to determine whether there are any lessons for SA in terms of the application of a South African right to be forgotten.

---

[168] G Buttarelli 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 at 78, C Kuner 'The path to recognition of data protection in India: The Role of the GDPR and International Standards' (2021) 33 *National Law School of India Review* 69 at 70 – 72, and G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 485.

[169] See generally, *Schrems v Data Protection Commissioner* EU:C:2015:650, *Data Protection Commission v Facebook Ireland and Maximillian Schrems* EU:C:2020:559, C Lam 'Unsafe harbor: The European Union's demand for heightened data privacy standards in *Schrems v. Irish Data Protection Commissioner*' (2017) 40(3) Electronic Supplementary *Boston College International and Comparative Law Review* 1 – 13, M Rotenberg '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26 *European Law Journal* 141 – 152, P Nebbia 'The *Schrems* judgments: a silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336, MH Murphy 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) 71 *International and Comparative Law Quarterly* 245–262, and V Bentotahewa, C Hewage & J Williams 'the normative power of the GDPR: A case study of data protection laws of South Asian countries' (2022) 3 *SN Computer Science* 183.

VIII LIMITATIONS

The thesis will not cover the Cambridge Analytica/Facebook scandal, although it may be referred to as an example of an infringement of both the right to privacy and freedom of expression, but only where there is an important feature that is relevant to the right to be forgotten. Furthermore, cybercrime, including hacking, will not be dealt with unless there is an important feature that is relevant to the right to be forgotten. Similarly, mass surveillance will also not form a large part of the study, except where this impacts data protection and the right to be forgotten.

The thesis represents the law as at 15 March 2024.[170]

IX RESEARCH METHODOLOGY

The thesis is not based on an empirical study. The thesis is a desktop review of the relevant primary and secondary sources. The primary sources will include judgments and the relevant legislative instruments (ie acts, statutes, regulations, directives, etc.) from the jurisdictions as outlined in the comparative study above. The legal concepts as provided for in the legislative instruments will be analysed and discussed in light of judgments as well as commentary and academic discussions will be analysed and discussed coherently, concisely and critically. The analysis and discussions will be guided by the research questions. The answers to the research questions may be followed by possible recommendations for legal amendments or inclusions into the current legislative instruments alternatively, there may be suggestions for further study. The commentary and academic discussions will include books, articles, papers, conference papers, various reports, etc., put differently, the thesis will include a literature review, and will analyse and discuss the ideas and concepts from these sources.

X CONCLUSION

Apart from the introduction, this thesis will concentrate on the European legal position (Chapter 2) and how the European courts have interpreted the provisions of the relevant data protection legisation (Chapter 3). Chapter 4 will focus on the rights to privacy and freedom of expression in SA. Chapter 5 centres on POPI and a possible right to be forgotten in SA. The

[170] After the submission of the thesis, the Constitutional Court finally delivered its judgment in *Botha v Smuts and another* [2024] ZACC 22; 2025 (1) SA 581 (CC); 2024 (12) BCLR 1477 (CC) on 9 October 2024. Argument in this matter had been heard on 9 November 2023. The case has been included in the thesis and discussed. There are also further cases and sources that have been added, and these additions include cases and academic commentary that were subsequently handed down or published after 15 March 2024.

last chapter (Chapter 6) will compare the positions presented, as well as critiquing, make recommendations, where necessary, and conclude the thesis.

Technology does prove to be a challenge when it comes to data protection, as pointed out above. The internet, being a cheaper, quicker, and more convenient tool to access information, including personal information, amplifies the need for laws that provide the mechanisms for people to turn to to protect their privacy. Trying to control the internet as a borderless research tool has certainly presented legislators in various states with a set of challenges. The abuse of processing personal information on the internet has a great potential to damage reputations. Hence, the right to be forgotten is a purely internet based right. How it is able to assist individuals with the protection of their right to privacy, especially in protecting their personal data, is certainly the main theme of this thesis.

CHAPTER 2

DIRECTIVE 95/46 AND THE GDPR

I INTRODUCTION

Privacy is one of the most valued rights in Europe. Is the right to privacy it's pre-eminent or "first amendment" right, to borrow United States (US) terminology?[171] This is not a question that needs to be answered in this thesis, however, it is interesting to note that Europe has two constitutional instruments.[172] These two instruments are the Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention)[173] and the Charter of Human Rights of the European Union (the Charter).[174] The Convention applies to those countries that are a part of the Council of Europe.[175] The Charter applies to those countries that are Member States of the European Union (the EU).[176] All 27 EU Member States adhere to both

[171] PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 3 – 4, and B Petkova 'Privacy as Europe's first amendment' (2019) 25 *European Law Journal* 140 – 154. Compare with F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 934. See also W Kerber & KK Zolna 'The German Facebook case: The law and economics of the relationship between competition and data protection law' (2022) 54 *European Journal of Law and Economics* 217 – 250 regarding the tension between the protection of privacy and the ever-expanding digital market. See also Grand Chamber's decision in *Meta Platforms Inc. & others v Bundeskartellamt* EU:C:2023:537, *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:276, and *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:277 where the CJEU was called upon in the Grand Chamber and the Fifth Section of General Court of the CJEU to balance right to privacy (and personal data protection) against the right to economic gain in light of the competition/anti-trust laws of the European Union. See also 'Court upholds request for information identified by search terms' (2023) 429 *EU Focus* 9 – 11.

[172] Regarding the relationship between the EU and the Court of Justice of the European Union (CJEU) with the Council of Europe and the European Court of Human Rights (ECtHR) refer to the following sources for a more discussion as it goes beyond the scope of this thesis. *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v Ireland* [2005] ECHR 440, *Opinion 2/13 of the Court of Justice of the European Union* EU:C:2014:2454, *Avotiņš v. Latvia* [2016] ECHR 440, P Gragl 'An olive branch from Strasbourg? Interpreting the European Court of Human Rights' resurrection of *Bosphorus* and reaction to *Opinion 2/13* in the *Avotiņš* Case: ECtHR 23 May 2016, Case No. 17502/07, *Avotiņš v Latvia*' (2017) 3(3) *European Constitutional Law Review* 551 – 567, Z Jelinić, & KK Radoja 'Mutual recognition of judicial decisions and the right to a fair trial with special focus on the ECHR'S findings in the Case of *Avotiņš v Latvia*' (2018) *EU and Comparative Law Issues and Challenges Series* 571 – 585, S O'Leary 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 – 31, and T Lock 'The future of EU Human Rights Law: Is accession to the ECHR still desirable? (2020) 7(2) *Journal of International and Comparative Law* 427 – 447. O'Leary in her article (at 5) states that despite the differences between the two courts

> "the European Court of Human Rights ('ECtHR') sought to accommodate the international obligations to which EU Member States had subscribed while seeking, nevertheless, to ensure compliance with their Convention obligations."

[173] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, as amended by Protocols Nos. 11, 14 and 15, and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 (the Convention).

[174] Charter of Human Rights of the European Union (2012/C 326/02) (the Charter).

[175] There are 46 Member States at the Council of Europe.

[176] There are 27 Member States in the European Union. For an overview of how the EU was formed see, F Laursen 'The founding treaties of the European Union and their reform' (31 August 2016) *Oxford Research Encyclopedia of Politics* 151

constitutional instruments. The right to privacy in the Convention is set out in Article 8. Article 8(1) provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence"[177] and Article 8(2) provides that the government shall not interfere with this right unless it is necessary for "the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[178]

The right to privacy in the Charter is set out in two Articles, namely in Article 7 and Article 8. Article 7 is worded exactly the same as Article 8(1) of the Convention. Article 8 of the Charter, is divided into three sub-sections, and provides expressly for the protection of personal data. Article 8(1) provides that everyone has the right to have their personal data protected. Article 8(2) provides that data must be processed fairly and that everyone has the right to access their personal data when it has been collected and processed. Article 8(3) provides for the establishment of an independent authority to enforce compliance with the protected right. Article 8 of the Charter is unique, as it is the first time that data protection has been conceptualised as a fundamental constitutional human right.[179]

However, even in Europe, the right to privacy must be balanced with the rights to freedom of expression and information. Article 10 of the Convention and Article 11 of the Charter provide for the protection of freedom of expression and information.[180]

The EU's data protection framework is inspired by the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, 1981 (Convention 108). It is currently the only internationally binding data protection instrument, as it includes not only countries that are members of the Council of Europe, but also countries such as Mauritius, Morocco, Cape Verde, Argentina, and Mexico.[181] Convention 108 will not be part of the main discussions of this thesis. First, South Africa (SA) has not

[177] Article 8(1) of the Convention.
[178] Article 8(2) of the Convention.
[179] Y McDermott 'Conceptualising the right to data protection in an era of big data' (2017) 4(1) *Big Data & Society* 1 – 7. *WM & Sovim SA v Luxembourg Business Registers* EU:C:2022:912 discusses the application of Article 8 of the Charter in the protection of personal data. See *LB v Hungary* [2023] ECHR 239 para 53.
[180] *Perincek v Switzerland* [2015] ECHR 907 paras 198 - 199, and *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702 para 59.
[181] For a complete list of countries, see: Council of Europe 'Chart of signatures and ratifications of Treaty 108', *https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108* (Accessed: 24 July 2023). See also S Kierkegaard, N Waters, G Greenleaf, *et al* '30 years on – The review of the Council of Europe Data Protection Convention 108' (2011) 27 *Computer Law & Security Review* 223 at 223 and M Marelli 'The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders' (2023) 50 *Computer Law & Security Review* 105849 1 at 10.

ratified Convention 108.[182] Second, although it is one of the two internationally significant data protection instruments, the other being the OECD Guidelines,[183] Convention 108 is technologically neutral in its approach. The reason for the technologically neutral approach is that it was drafted at a time when technology had not evolved as far as it has today, and Convention 108 "was designed to regulate what was in many respects a niche activity."[184] Third, Directive 95/46 was, and currently the GDPR is, the most authoritative data protection legislation globally, both being "cast in the lead roles" as the "gold standard" to follow when drafting data protection legislation. The articles therein are far more detailed compared to Convention 108.[185] Fourth, although the South African Law Reform Commission discusses

[182] Council of Europe 'Chart of signatures and ratifications of Treaty 108', *https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108* (Accessed: 24 July 2023).

[183] Organization for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data* (OECD Guidelines). South Africa is not a member of the OECD, but on 16 July 2023, the OECD (represented by the Secretary General) and South Africa (represented by the Minister of Finance) signed a Memorandum of Understanding for Co-operative Activities and Joint Work Programme to encourage the growth and development of "small, micro and medium enterprises, promoting trade and investment and improving the skills of the South African workforce." South Africa is listed by the OECD as a "mutually beneficial partner" alongside Brazil, China, India, and Indonesia, for the OECD Member States to consider as a country with investment opportunities. See 'South Africa and the OECD' *https://www.oecd.org/southafrica/south-africa-and-oecd.htm* (Accessed: 27 January 2024). The OECD Guidelines will be referenced, where applicable in the footnotes, as the SALRC referred thereto extensively when drafting the Protection of Personal Information Act 4 of 2013 – see the SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) and A Roos 'Core principles of data protection law' (2006) 39(1) *Comparative and International Law Journal of Southern Africa* 102 – 130. M Phillips 'International data-sharing norms: From the OECD to the General Data Protection Regulation (GDPR)' (2018) 137 *Human Genetics* 575 at 575 – 577 indicates that Member States and Non-Member States of the OECD have often based their national data protection legislation on the OECD Guidelines and not solely on Convention 108. The reason is that Convention 108 allows for data transfers between signatories and non-signatories, even where there is no strict compliance by the non-signatory country, whereas the OECD Guidelines requires substantial observance by Non-Member States to the OECD before data may be transferred to the Non-Member State.

[184] S Kierkegaard, N Waters, G Greenleaf, *et al* '30 years on – The review of the Council of Europe Data Protection Convention 108' (2011) 27 *Computer Law & Security Review* 223 at 223. Convention 108 has been modernised and is now referred to as the Modernised Convention for Protection of Individuals to the Processing of Personal Data, adopted on 18 May 2018 (Convention 108+). Convention 108+ includes more definitions and amplifies articles to be more inclusive of the recent technological advancements, although there are scholars that have argued against such inclusion, see generally S Kierkegaard, N Waters, G Greenleaf, *et al* '30 years on – The review of the Council of Europe Data Protection Convention 108' (2011) 27 *Computer Law & Security Review* 22. Convention 108+ has not as yet entered into force – see *LB v Hungary* [2023] ECHR 239 para 43 and M Marelli 'The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders' (2023) 50 *Computer Law & Security Review* 105849 1 at 10 – 11.

[185] LA Bygrave 'The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects' (2021) 40 *Computer Law & Security Review* 105460 1 at 2. See C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 136 states that Convention 108 provided basic data protection principles for the signatories thereto to follow. M Marelli 'The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders' (2023) 50 *Computer Law & Security Review* 105849 1 at 2 indicates that Directive 95/46 and the GDPR significantly expand on the principles detailed in Convention 108.

Convention 108 in its report, the proposed legislation leans towards Directive 95/46.[186]

Data or information, especially personal data or information, is generally sensitive and the collection and processing of such data have become a lucrative business. It is often referred to as the "new oil" that runs various industries, such as banking, and insurance[187] It is in response to these developments that data protection legislation has been developed to protect the privacy of internet users and individuals, often referred to as data subjects, especially during commercial transactions where personal data must be provided for the transaction to be completed.[188] This is particularly important in applications for bank loans and insurance policies, etc. There is also personal data that is even more sensitive, such as medical information, religious beliefs, and personal opinions, which need specific safeguards when

[186] SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 3.

[187] P MacDonnell 'The European Union's proposed equality and data protection rules: An existential problem for insurers?' (2015) 35(2) *Economic Affairs* 225 – 239. Although the article focusses on the insurance industry, it provides a good overview of the legislation that has been enacted to deal with how data, including personal data, is used in business. In the insurance industry, a point system has been developed. Personal information is processed in terms of this point system, and the system automatically decides what kind of risk factor a person is, and therefore how much they will need to pay for certain insurance products. Note also S Huneberg & K Berry 'Big data and the paradigmatic shift from passive insurer towards risk personalisation' (2022) 2 *Tydskrif vir die Suid-Afrikaanse Reg* 283 at 288 – 289. L Kugler 'The war over the value of personal data' (2018) 61(2) *Communications of the Association for Computing Machinery (ACM)* 17 – 19, in the introductory paragraph refers to personal data as "the new oil", because it powers social media platforms and social networking sites. Search engines can target advertisements, based on the searches of internet users, which bring in lucrative deals with companies seeking advertising space. G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303, provides the argument that data subjects should be able to know what the monetary value is of their personal data, ie how much do the big data companies earn therefrom. See also the introductory paragraphs in EL Carter 'Argentina's right to be forgotten' (2013) 27 *Emory International Law Review* 23 – 39. For a critique of data protection laws preventing the data economy, see: B Custers & G Malgieri 'Priceless data: Why the EU Fundamental right to data protection is at odds with trade in personal data' (2022) 45 *Computer Law & Security Review* 105683. Note also one of the biggest data breeches in recent history, namely, the Cambridge Analytica scandal, where data was harvested from millions of Facebook users' accounts, and then used to sway the voters in the US during the presidential elections – this was discussed in more detail in Chapter 1, see J Isaak & MJ Hanna 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) 51(8) *Computer* 56 – 59. Although, Cambridge Analytica will not be a topic discussed in the thesis; it is merely used as an example of a data breach and the need to protect internet users against the surreptitious practices of data harvesting. This includes selling the data to make a profit, and the illegal use thereof, to which data subjects or internet users have not consented. See also Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479. See also BGH, Urteil vom 23. Juni 2020 – KVR 69/19 – *Bundeskartellamt v Facebook* and K Weideman 'A matter of choice: The German Federal Supreme Court's interim decision in the abuse-of-dominance proceedings *Bundeskartellamt v. Facebook* (Case KVR 69/19)' (2020) 51 *International Review of Intellectual Property and Competition Law* 1168 – 1181, where, amongst other issues, Facebook was accused of processing personal data as trade-off for the use of their services, irrespective of whether the data was collected from Facebook or outside websites affiliated with Facebook. See also S van Deventer 'Problems relating to the formation of online contracts: A South African perspective' (2021) *South Africa Law Journal* 219 at 227, the services offered by Google, Facebook, and Co, are offered as "free", however users of these services "pay" with their personal data.

[188] P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 131.

processed.[189] The different parties involved, ie those that collect, control and process personal data as well as the individuals that provide their personal data, each has specific rights and responsibilities and assist in resolving possible conflicts between these rights and responsibilities.[190] A primary aim of Directive 95/46 is to ensure that a data subject's personal data may be processed only where they have provided their consent thereto, and then only for the specified purpose for which the consent was given.[191]

The focus of this chapter is to set out the relevant legislative instruments that have been developed in the EU to regulate the processing of personal data, and provide for protection from and remedies for an infringement of the data subject's privacy.[192]

The following topics will be discussed within the chapter: there will be a brief discussion of Directive 95/46,[193] as this was the original legislative tool used to define the right to be forgotten in the EU. SA's Protection of Personal Information Act 4 of 2013 (POPI) in many respects mirrors Directive 95/46.[194] The application of POPI, taking into account the Constitution of the Republic of South Africa, 1996 (Constitution) and relevant laws and interpretation of the legal concepts, may be guided, in certain respects, by the interpretation of

[189] P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 132 – 133.
[190] J Dumortier & DM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 at 225 – 227, P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 133 – 134 and 141, and R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 230.
[191] J Dumortier & DM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 at 226 – 227, and P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 135 – 136.
[192] LA Bygrave 'Privacy and data protection in an international perspective' (2010) 56(8) *Scandinavian Studies in Law* 165 at 166. Both 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 and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (referred to as the General Data Protection Regulation or the GDPR) require that sanctions for the infringement of data protection principles be implemented by the Member States to the European Union. See generally, Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 and C Hoofnagle, B van der Sloot & F Zuiderveen Borgesius 'The European Union general data protection regulation: What it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65 at 92 – 97. For an overview of the general development of data protection law in Europe, see D Edros 'Dead ringers? Legal persons and the deceased in European data protection law' (2021) 40 *Computer Law & Security Review* 105495 1 at 4 – 6.
[193] The full title is: 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.
[194] DL Donnelley '"Privacy by design" in the EU General Data Protection Regulation: A new privacy standard or the emperor's new clothes?' (2022) 139(3) *South African Law Journal* 541 at 554.

Directive 95/46.[195] The General Data Protection Regulation (GDPR)[196] will follow, as this is the current legislative instrument used in the EU to protect data, and has for the first time codified the right to be forgotten. Furthermore, how the two legislative instruments work together will be set out, in light of case law.

II DIRECTIVE 95/46

(a) Introduction

Directive 95/46/EC does not have a specific article that defines or sets out the right to be forgotten.[197] Instead, the right to be forgotten is a combination of articles that have been used in conjunction with one another to provide the protection that the right offers. The first court to define the right was the Court of Justice of the European Union (the CJEU) in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (*Google Spain*),[198] this is more fully explored in the next chapter.

What will be examined in this chapter are the objects and scope, the definitions as well as the basic principles governing the processing of personal data as provided in Directive 95/46, and which were important for the CJEU's decision in *Google Spain*. Furthermore, Directive 95/46 was drafted during a time when technology was not as advanced as it is today, and there was a need to amend, alternatively, adapt the current legislative scheme to meet the ever-changing technological advancements.[199] The GDPR took up and expanded on Directive 95/46.[200] In Recital 9 of the GDPR, the following statement is made: "objectives and principles

---

[195] Section 39(1) of the Constitution of the Republic of South Africa, 1996, provides for the use of both international and foreign laws and cases in the interpretation of the Constitution, or more specifically, the Bill of Rights.

[196] The full title is: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (referred to as the General Data Protection Regulation or the GDPR).

[197] 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 (Directive 95/46). I Walden 'The application of Directive 95/46/EC' (1996) 3 *EDI Law Review* 85 – 98, and for a criticism of whether Directive 95/46 is able to deal with the new challenges created by technology, see JC Buiterlaar 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 – 202, G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 437 – 440. This is unlike the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), which is briefly discussed later in this chapter.

[198] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[199] P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 – 142, and P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 – 194.

[200] P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A

of Directive 95/46/EC remain sound". Hence, there is a continuation of these principles within the GDPR.[201] The reason for the drafting of the GDPR was to ensure the harmonious and consistent application of these principles, as Directive 95/46 was not applied uniformly amongst the EU Member States.[202]

(b) Objectives and scope

The main objectives of Directive 95/46 are contained in the preamble and Article 1. The following brief discussion will provide some background to Directive 95/46. This discussion will include references to some of the recitals in the preamble. The purpose of the preamble is to assist with the interpretation of the Directive, and "put what follows *in context*".[203] In summary, Directive 95/46 requires that it be implemented within three years, by each Member State, from the date of enforcement.[204] Recital 2 reminds that "data-processing systems are designed to serve" natural persons, and that irrespective of their nationality and/or residence, the data processing systems are required to "respect fundamental rights and freedoms, notably the right to privacy". However, this must simultaneously contribute to "economic and social progress, trade expansion and the well-being of individuals" keeping in mind "the establishment and functioning of the internal [EU] market", which provides for the "free movement of goods, persons, services and capital".[205] Recital 10, in conjunction with Recitals 3 and 8 provides that EU Member States must, by safeguarding the fundamental rights and freedoms of data subjects, especially the right to privacy, ensure there is a high level of

sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 – 142.

[201] P Hustinx 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 28, and A Giurgiu & TA Larsen 'Roles and powers of national data protection authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and more "European" DPAs as guardians of consistency?' (2016) 2 *European Data Protection Law Review* 342 at 350.

[202] Recital 9 of the GDPR.

[203] Italics in original. T Klimas & J Vaiciukaite 'The law of recitals in European Community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61 at 64. See also *Puppinck & others v European Commission* EU:C:2019:1113 para 75, Opinion of Advocate General Bobek in *Puppinck & others v European Commission* (Case C-418/18P) EU:C:2019:640 para 93. Compare with *Capitec Bank Holdings Ltd & another v Coral Lagoon Investments 194 (Pty) Ltd & others* 2022 (1) SA 100 (SCA) paras 25 and 50. See also NA Papadopoulos 'Revisiting the preamble of the European Social Charter: Paper tiger or blessing in disguise?' (2022) 22 *Human Rights Law Review* 1 at 2, where the author states that preambles assist in setting out the framework or "object and purpose". See generally L Orgad 'The preamble in constitutional interpretation' (2010) 8(4) *International Journal of Constitutional Law* 714 – 738.

[204] Recital 69 and Article 1 of Directive 95/46, see also P Hustinx 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 9. Note Article 2 of the Treaty on the Functioning of the European Union (Consolidated 2016) (TFEU), formerly Treaty Establishing the Economic Community, signed at Rome, on 25 March 1957 (the Treaty of Rome) – see Article 358 of the TFEU.

[205] Recital 3 of Directive 95/46.

protection where personal data is processed, and ensure the functioning of, and the free flow of, data within the internal EU market, in line with the requirements of the Treaty on the Functioning of Europe.[206]

Recitals 18, 19 and 20 deal with controllers and their subsidiaries. These provide that both the controllers and subsidiaries must apply the applicable national law that implements Directive 95/46. However, Recital 20 provides that irrespective of whether the controller is established in a third country outside of the EU, the controller must, where processing the personal data of a data subject situated within an EU Member State, do so in accordance with the national legislation of that Member State implementing Directive 95/46.[207]

Recital 25, amongst others, provides and obliges controllers, and those processing data, to notify data subjects that their personal data is being collected to be processed, and the notification must provide the data subject an opportunity to check the data that is going to be processed and make any necessary corrections thereto or object to the processing thereof, depending on the circumstances.[208]

---

[206] Article 94 of the Treaty of Rome, now Article 115 of the TFEU, *IPI v Geoffrey Englebert & others* EU:C:2013:715 para 28, and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 66. Note also, Article 1 of Directive 95/46. See JM Fromholz 'The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461 at 468, where the author explains that the high level of protection includes limited exceptions to the provisions within Directive 95/46, thereby ensuring against the exploitation of personal data. Furthermore, at 462, Fromholz adds that data may only be transferred to those third countries that have similar, if not the same, data protection standards, as the EU, adding another layer to the high level of protection that is expected. What the EU Member States are required to do is to harmonise (ie approximate) their national laws with those of the applicable EU legislative instrument, taking into account the nuances between the national languages of each EU Member States. The more in harmony each of the national laws are, based on the legislation issued by the European Parliament and the Council of Europe, the easier it is to achieve the aim of an effective common market between the EU Member States. See E Herlin-Karnell 'Recent developments in the area of European criminal law' (2007) 14(1) *Maastricht Journal of European and Comparative Law* 15 at 35, K McAuliffe 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 at 98, 111, and 113 – 114, and R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 229 – 230. On the different legislative mechanisms that are used in the EU to obtain harmonisation of laws between the Member States, see F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 155 – 156. See J Law & EA Martin (eds) *Oxford Dictionary of Law* 7ed (2009), definition of "approximation of laws".

[207] The relevant part of Recital 20 of Directive 95/46 reads as follows:

> "the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; … in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice".

[208] Recital 25 of Directive 95/46 reads as follows:

> "Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult

The scope of Directive 95/46 is covered in Article 3. Article 3 provides that Directive 95/46 will apply whenever data is processed, including processing that is partially or completely automated. It is also applicable to data that is stored in a filing system (irrespective of whether the filing system is of a physical nature or computerised). Furthermore, Article 3 stipulates that Directive 95/46, will not apply when data is processed in light of "public security, defence, State security . . . and the activities of the State in areas of criminal matters", as well as where data is processed by a natural person in terms of a "purely personal or household activity".[209]

Article 4 provides that Member States must enact their own national legislation pursuant to Directive 95/46, and provides that where the controller is situated in a third country's territory, the national laws will still apply by virtue of international law.[210] Regarding the applicability of the national law, the focus of Directive 95/46 is placed on the data subject, rather than where the controller is situated.[211] Also, where the controller is not situated within the EU, but uses "equipment, automated or otherwise" that is situated within the EU or a specific Member State, the law of the Member State will apply.[212] In an opinion on the applicable law, the Article 29 Data Protection Working Party[213] (Article 29 WP) pointed out

---

the data, to request corrections and even to object to processing in certain circumstances."

[209] Article 3(1) and (2) of Directive 95/46. See *Tietosuojavaltuutettu (Jehovan todistajat — uskonnollinen yhdyskunta as intervening party)* EU:C:2018:551 paras 34 – 51 where the CJEU held that door-to-door preaching is not a purely household activity as it involves interaction with members of the public outside of the faith based group. See also *Ryneš v Úřad pro ochranu osobních údajů* EU:C:2014:2428 paras 19 – 35 where it was held that the concept of "purely personal or household activity" is narrow, and hence the keeping of address books and correspondence for one's personal use or in relation to one's private and family life falls within this concept, however at issue was that Mr Ryneš had installed surveillance cameras in order to protect his personal property, family, life, health, etc. These cameras were connected to a hard disk that stored the recordings of people that came onto the property. The CJEU held that this was an outward activity as it processed the data of persons, other than those living on the property or who were a part of the family, and so could not fall into the category of a "purely personal or household activity". Note also *Lindqvist* EU:C:2003:596 para 47, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* EU:C:2008:727 para 44, and *LB v Hungary* [2023] ECHR 239 para 48. See also N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 at 61 – 62.

[210] Article 4(1)*(b)* of Directive 95/46. As an example of the interaction between Directive 95/46 with the applicable national law of a Member State see *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388 paras 45 – 64.

[211] Recital 18 of Directive 95/46, and *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772, in which the CJEU applied both Directive 95/46 and the GDPR. In light of the GDPR see B Van Alsenoy & M Koekkoek 'Internet and jurisdiction after *Google Spain*: The extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[212] Note, although discussed later in this chapter, data processing includes activities such as collecting, the actual processing of data, as well as storage. See Article 2*(b)* of Directive 95/46.

[213] Article 29 of Directive 95/46 establishes the overarching watchdog for Directive 95/46 and the protection of personal data. Directive 95/46 also provides that the Article 29 Data Protection Working Party with the ability to provide guidelines and opinions on the implementation of Directive 95/46, for example see Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010.

that Directive 95/46 provides that the "external scope of EU law is an expression of its capacity to lay down rules in order to protect fundamental interests within its jurisdiction". This means that Member States, through their relevant authorities, are able to protect the rights of data subjects whose data is being processed outside the EU, where necessary.[214] This rule does not apply, however, if the equipment is situated within the EU or a specific Member State only for transitory purposes. Directive 95/46 requires that a representative of the controller must be established within an EU Member State, especially in light of possible legal actions where the provisions of Directive 95/46 are contravened.[215]

The biggest problem regarding Directive 95/46, according to academic commentators, was the inconsistent application thereof within the individual EU Member States.[216] The aim was to create a harmonised approach when dealing with the protection of personal data, but that was not achieved, even though the data protection principles provided in Directive 95/46 were comprehensive.[217] Companies faced different fines, depending on which Member State they were situated in, for contraventions in terms of the national legislation implemented and based on Directive 95/46.[218] The different approaches adopted by EU Member States were the cause of much confusion because the texts were transposed and translated into over 20 languages (ie into the national language of each Member State).[219] Due to the nature of a

[214] Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 at 10, and Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 211 – 212.

[215] Article 4(2) of Directive 95/46. See also R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 232, B Van Alsenoy & M Koekkoek 'Internet and jurisdiction after *Google Spain*: The extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[216] B Koritnik 'Discretion of the EU Member State when implementing the Data Protection Directive 95/46/EC' [2005] MurdochUeJlLaw 4, R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 232, and Y Poullet 'Is the general data protection regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 – 778.

[217] Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 207, and R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 238 – 239. See also Recital 9 of the GDPR. There is a possibility that these arguments begin to sound repetitive or circular, however, the consensus was that the principles were comprehensive and sensible, but each Member State interpreted them slightly differently, and there were a range of fines, hence there was no real consensus.

[218] F Galli '*Digital Rights Ireland* as an opportunity to foster a desirable approximation of data retention provisions' (2016) 23(3) *Maastricht Journal of European and Comparative Law* 460 at 463. The legislative texts need to be translated into over 20 languages, Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 207, and K McAuliffe 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 – 115.

[219] I Saltzman 'The status of national implementation of Directive 95/46/EC on the processing and free movement of personal data' (1996) 18(12) *European Intellectual Property Review* 680 – 683, and S Hurka & Y Steinebach 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 280.

directive, Member States are given some freedom in the adaptation thereof, specifically the interpretation of legal concepts.[220] Duina, using the implementation of the Equal Pay Directive[221] as an example, pointed out that some EU Member States do not implement directives completely, whereas others do.[222] One reason presented by Duina for not implementing a directive completely is the cost of implementation for the State.[223] Dumortier and Alonso Blas specifically dealt with the implementation and transposition of Directive 95/46 into the Belgian legal system.[224] The authors concluded that, in light of the existing data protection legislation operating in Belgium, the main areas of change included definitions, the territorial scope, and the "strict" requirement that the data subject must be informed "when data are collected from the data subject or when they are not collected from" them.[225] Edros pointed out that the Northern EU Member States placed a greater emphasis on freedom of expression, whereas the Eastern and Latin EU Member States focused their implementation on data protection.[226]

One possible reason for the original choice of using a directive for data protection was that it was the most commonly and powerfully used tool for the implementation of laws, and still allowed for a certain amount of leeway or flexibility for interpretation within each Member

[220] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, K McAuliffe 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 – 115, E Van Schagen 'More consistency and legal certainty in the private law *acquis*: A plea for better justification for the harmonization of private law' (2012) 19(1) *Maastricht Journal of European and Comparative Law* 37 – 62, and R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 – 244.

[221] Council Directive of 10 February 1975 on the approximation of the laws of the Member States relating to the application of the principle of equal pay for men and women (75/117/ EEC) OJ 1975, No L 45/ 19, 19.2.1975 (Equal Pay Directive).

[222] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 161. For an example of some of the issues faced by Belgium in the implementation of Directive 95/46, see J Dumortier & BM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 – 242.

[223] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, and J Dumortier & BM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 at 225 – 227.

[224] J Dumortier & BM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 – 242.

[225] J Dumortier & BM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 at 240 – 241. Note the remarks of the CJEU in *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2023:2 para 54, which highlights that the protection of rights requires a "consistent and homogeneous application" in terms of the GDPR.

[226] D Edors 'European Union data protection law and media Expression: Fundamentally off balance' (2016) 65 *International and Comparative Law Quarterly* 139 at 141.

State.[227] Each Member State retains some autonomy, and thereby keeps their individual identity when transposing EU law into its own legal system.[228] However, as described above, this lead to a fragmented approach in the transposition and implementation of Directive 95/46.

Due to the fragmented approach, the EU Council and Parliament decided that the new updated data protection laws would take the form of a regulation. Unlike a directive, a regulation comes into effect on a specific day without having to be transposed into national law and there is limited or no freedom for adaptation by each Member State. A regulation thus applies uniformly across the whole EU and promotes legal harmony.[229]

(c) Definitions

The following definitions, as set out in Article 2, are important to note regarding the right to be forgotten, especially in light of the discussions in the following chapter regarding the case law.

Article 2*(a)* refers to "personal data" and not "personal information".[230] It defines personal data as follows:[231]

> "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 social identity."

One possible reason for the use of the term "data" throughout Directive 95/46 instead of the

---

[227] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, K McAuliffe 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 at 114, E Van Schagen 'More consistency and legal certainty in the private law *acquis*: A plea for better justification for the harmonization of private law' (2012) 19(1) *Maastricht Journal of European and Comparative Law* 37 at 52, and S Hurka & Y Steinebach 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 278 and 282 – 283 – regarding the explanation for the choice of a directive for the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market.

[228] S Princen, F Schimmelfennig, R Sczepanski, H Smekal & R Zbiral 'Different yet the same? Differentiated integration and flexibility in implementation in the European Union' (2022) *West European Politics* 1 at 2.

[229] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 132, P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 182, Y Poullet 'Is the General Data Protection Regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774, and S Hurka & Y Steinebach 'Legal Instrument Choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 278 – 279. Note the comments on uniformity when interpreting EU laws by the CJEU in *UI v Österreichische Post AG* EU:C:2023:370 paras 29 and 48.

[230] The Protection of Personal Information Act 4 of 2013, which in s 1 sets out the definition for "personal information".

[231] Article 2*(a)* of Directive 95/46.

term "information" is because "personal data" includes the word "information" within its definition. The definition, provides for all ("any") information that relates to the data subject, whether created by the data subject or by a third person, but the data or information, whether directly or indirectly, must be capable of identifying the individual data subject.[232] The definition of "personal data", specifically with its inclusion of the words "any information", is certainly wide enough to encompass data created by both the data subject and a third person. The only limitations are that the information must relate to a natural person and that the data must be capable, either directly or indirectly, of identifying the data subject.[233] However, a complete discussion and debate on this point is beyond the scope of the thesis.[234]

Apart from the concept of "personal data", the notion of "processing of personal data" or "processing" is also defined in Article 2. This concept is defined as any action or procedure, even if automated, that permits for the[235]

> "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction [of personal data]".

In *Google Spain*, the CJEU had to decide whether an operator of a search engine falls into the definition of "controller".[236] A "controller" is defined in Article 2*(d)* as

---

[232] Article 2*(a)* of Directive 95/46. See generally Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data*, adopted 20 June 2007. See also C Docksey & H Hijmans 'The Court of Justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law' (2019) 5 *European Data Protection Law Review* 300 at 302 – 304, and A Esteve 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 at 45 – 46. See L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808 1 at 1 – 3 on de-identifying personal data and what that should entail.

[233] *Lindqvist* EU:C:2003:596 para 24, *College van burgemeester en wethouders van Rotterdam v Rijkeboer* EU:C:2009:293 paras 42 and 57, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 27, *YS v Minister voor Immigratie, Integratie en Asiel* EU:C:2014:2081 paras 40 – 48, 54 – 60, and 64 – 69, *Breyer v Bundesrepublik Deutschland* EU:C:2016:779 paras 40 – 45, *Nowak v Data Protection Commissioner* EU:C:2017:994 paras 31 – 35, *SRB v EDPS* EU:T:2023:219 paras 68 – 69, 73, and 88 – 93, *FF v Österreichische Datenschutzbehörde* EU:C:2023:369 paras 22 – 26, and *LB v Hungary* [2023] ECHR 239 para 48. See also Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data*, adopted 20 June 2007 at 7, C Bessant 'The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online' (2015) 16(2) *European Journal of Law and Technology* 1 at 4, and N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 at 61 – 72.

[234] For a discussion on the various elements of "personal data" and the surrounding debate see generally Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data*, adopted 20 June 2007, N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 at 45ffg, and C Docksey & H Hijmans 'The Court of Justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law' (2019) 5 *European Data Protection Law Review* 300 at 302 – 304.

[235] Article 2*(b)* of Directive 95/46.

[236] Article 2*(d)* of Directive 95/46. See also Article 29 Data Protection Working Party *Opinion 1/2010 on the*

> "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".

An important point to note about this definition is that a "controller" can be both a natural or juristic person, provided he, she or it determines the reason and method for processing personal data – this often includes the furtherance of their business.[237] The definition also provides for joint controllers that together decide on the reason and method for processing personal data.[238] In *Google Spain*, the CJEU held that the operator of a search engine "must be regarded as" a "controller" as it is the operator who "determines the purpose and means" of how the personal data will be processed in light of its activities with regards to the search tool, even where this is automated.[239] The concept of "controller" is deliberately wide. According to the Article 20 WP, this is to provide for a flexible approach to who may be classified as a controller.[240]

A "processor", as defined by Article 2*(e)* is a "natural or legal person, public authority,

---

concepts of "controller" and "processor", adopted on 16 February 2010.

[237] See generally L Kugler 'The war over the value of personal data' (2018) 61(2) *Communications of the Association for Computing Machinery (ACM)* 17 – 19, wherein the author described how data is used to "oil" (ie personal data), to fuel various new forms of business models in a variety of industries. See also S van Deventer 'Problems relating to the formation of online contracts: A South African perspective' (2021) *South Africa Law Journal* 219 at 227.

[238] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388 paras 25 – 44, and *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629 paras 64 – 85.

[239] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 31 – 33. See also *Tietosuojavaltuutettu (Jehovan todistajat — uskonnollinen yhdyskunta as intervening party)* EU:C:2018:551 paras 63 – 75 where the CJEU looked at the activities of the collecting data to maintain lists of people who do not want to be visited by the Jehovah Witness Community. The court held that these lists amounted to controlling personal data and thus the Community (or those responsible) are "controllers". In *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388 para 42 the CJEU held:

> "the recognition of joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that page contributes to ensuring more complete protection of the rights of persons visiting a fan page, in accordance with the requirements of Directive 95/46."

See paras 25 – 44 for a complete discussion of "controller" in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388. See also *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629. See also the following commentary: J Marosi 'Who controls a Facebook page?' *VerfBlog*, 6 June 2018, S Lindroos-Hovinheimo 'Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*' (2019) 28(2) *Information & Communications Technology Law* 225 – 238, and M Zalnieriute & G Churches 'When a "like" is not a "like": A new fragmented approach to data controllership' (2020) 83(4) *Modern Law Review* 861 – 876.

[240] Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, adopted on 16 February 2010 at 3. See also B Van Alsenoy 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (2012) 28 *Computer Law & Security Review* 25 at 30 – 32.

agency or any other body which processes personal data on behalf of the controller". Once again, it is worth noting that this is a very wide definition, especially in light of the phrase "any other body", and that it encapsulates all scenarios in which natural or juristic persons may process personal data on behalf of a controller.[241]

Lastly, Article 2*(h)* defines "the data subject's consent" as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[242] Article 29 WP has detailed what is required in terms of each of the elements in the definition.[243] In summary, where the data subject gives their consent to the processing, it must be without duress, and for an explicit purpose, ie no blanket or open consent.[244] This is reflected by the words or phrases "freely given", "specific" and "informed".[245] Consent is, in terms of Article 7, "one of the lawful grounds on which personal data processing has to be based".[246] Article 7*(a)*, which provides for consent as a ground for the lawful processing of personal data, goes on to state that the consent must be "unambiguous", ie it must be a positive declaration from the data subject that their personal data may be processed.[247]

The above definitions are intended to assist in understanding the aims of, what is possibly the heart of the legislation, the processing principles of personal data.[248] In essence,

---

[241] Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, adopted on 16 February 2010 at 24 – 26, and B Van Alsenoy 'Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC' (2012) 28 *Computer Law & Security Review* 25 at 32 – 33.

[242] Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011.

[243] Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011 at 11 – 21.

[244] Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011 at 12 – 21, and PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 4. See also Article 8 of Directive 95/46.

[245] Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011 at 12 – 21.

[246] European Data Protection Board *Guidelines 05/2020 on consent under Regulation 2016/679* adopted 4 May 2020 paras 8 – 9 at 6.

[247] Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011 at 21. See also European Data Protection Board *Guidelines 05/2020 on consent under Regulation 2016/679* adopted 4 May 2020 paras 8 – 9 at 6. See also A Esteve 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 at 40 – 44 regarding the inadequate consent practices of Google and Facebook. Compare with G Jenkins 'An extended doctrine of implied consent – A digital mediator?' (2021) 52 *International Review of Intellectual Property and Competition Law* 706 – 733.

[248] In Directive 95/46, these are referred to as the "general rules on the lawfulness of the processing of personal data". See generally: D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283, P Hustinx 'EU Data Protection Law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 10 – 12. See, for a critical discussion on the 10th anniversary of

many of these definitions are similar to those in the GDPR, which may be interpreted to show that they are adaptable, even with the rapid growth of the internet.[249]

However, the internet has posed new challenges to the protection of the right to privacy and personal data, due to the ease with which data may be accessed. This has led to the Article 29 WP to acknowledge that the definitions in Directive 95/46 were not easy to apply within complex working environments, in light of the globalisation brought about by the internet.[250] De Hert and Papakonstantinou argued that the CJEU has stretched Directive 95/46 to its imaginable limits of interpretation and implementation to achieve its ultimate aim, namely the protection of personal data and the right to privacy of the data subjects.[251] Hence, there was a need for a new data protection law.[252] However, as pointed out by De Hert and Papakonstantinou, the flexible approach adopted in the interpretation of Directive 95/46 certainly provides guidance for interpretation and application of the GDPR.[253]

(d) The principles for the processing of personal data

Article 5 requires that the processing of personal data must be lawful within the limits or general rules as set out in Article 6.[254] These Articles will be discussed under themes based on internationally recognised lawful personal data processing principles. [255] The following themes

Directive 95/46, see Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 – 217.

[249] P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 180 – 182.

[250] Article 29 Data Protection Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, adopted on 16 February 2010, Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 207, R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 239, and P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 135.

[251] P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 180.

[252] R Wong 'Data protection: The future of privacy' (2011) 27 *Computer Law & Security* 53 – 57.

[253] P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 180 – 182. See also R Wong 'Data protection: The future of privacy' (2011) 27 *Computer Law & Security* 53 – 57.

[254] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 53 – 59, and *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601.

[255] The principles will be based on: A Roos 'Core principles of data protection law' (2006) 39(1) *Comparative and International Law Journal of Southern Africa* 102 at 107 – 130, OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) paras 7 – 14, A Mantelero 'Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution' (2012) 3(2) *European Journal for Law and Technology*, A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 213 at 214 – 215 and 219 – 223, M Goddard 'The EU General Data Protection Regulation (GDPR): European Regulation that has a global impact' (2017) 59(6) *International Journal of Market Research* 703 – 705, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 – 26. See also the Protection

will be used for the discussion: the legitimacy of data processing, purpose specific, minimality, information quality, retention and restriction of records, security safeguards, accountability and data subject participation.[256]

(i) Legitimacy of processing

The first of these principles is set out in Article 6*(a)* and it provides that the processing of data must be fair and lawful. This Article must be read together with Article 7, which sets out the grounds for lawful processing that must be met for the processing of personal data to be considered lawful. These grounds include:

1 consent;

2 the processing is necessary for the performance of a contract;

3 the processing is necessary to comply with a legal obligation;

4 the processing is necessary to protect the data subject's vital interests;

5 the processing relates to the performance of an obligation that is in the public interest or in the exercise of an official duty "vested in the controller or in a third party to whom the data is disclosed"; and

6 the processing is necessary for the pursuit of the legitimate or lawful interests of the controller or a third party for whom the data has been collected. It must be noted, however, that this processing cannot override the protection of the data subject's fundamental rights and freedoms.[257]

The last two grounds for lawful processing (5 and 6) played a significant role in *Google Spain*. This is because, in terms of Article 14 of the Directive, a data subject has a right to object to the processing of their personal data in terms of these two sub-articles.[258] For this

---

of Personal Information Act 4 of 2014, specifically the Conditions for Lawful Processing of Personal Information, sections 8 – 25.

[256] Article 5 of the GDPR.

[257] Articles 6(1)*(a)* and 7 of Directive 95/46. Article 6(1)*(a)* states:

"1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully".

Article 5(1)*(b)* of the GDPR. See also s 9 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) paras 9 and 10.

[258] Article 7 of Directive 95/46, see D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 284 – 285 and P Hustinx 'EU Data Protection Law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 10.

reason, it will be helpful to set out these two criteria in full. They read as follows:[259]

> "Member States shall provide that personal data may be processed only if:
>
> ...
>
> *(e)* processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
>
> *(f)* processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

(ii) Purpose specification

The second principle is set out in Article 6(1)*(b)* and it is sometimes referred to as the "collection limitation purpose".[260] This principle provides that personal data may be collected only for a specified purpose, and this purpose must be explicit and legitimate. An important consequence of this principle is that personal data may not be processed for a purpose other than the purpose for which it was originally collected. However, where it is in the public interest, alternatively where it is required by law, then personal data may be archived or stored and processed for historical, statistical and scientific research.[261]

---

[259] Note the rest of Article 7 reads as follows:

> "Member States shall provide that personal data may be processed only if:
> *(a)* the data subject has unambiguously given his consent; or
> *(b)* processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
> *(c)* processing is necessary for compliance with a legal obligation to which the controller is subject; or
> *(d)* processing is necessary in order to protect the vital interests of the data subject".

[260] Article 6(1)*(b)* of Directive 95/46, and reads as follows:

"1. Member States shall provide that personal data must be:
> *(a)* . . .
> *(b)* collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".

See also Article 5(1)*(b)* of the GDPR, sections 13 and 14 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 7.

[261] V Mayer-Schönberger & Y Padova 'Regime change? Enabling big data through Europe's new Data Protection Regulation' (2016) XVII *The Columbia Scientific & Technology Law Review* 315 at 330 – 3331, and P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 185, 189, and 194. Important to note is that the further processing of personal data for historical, statistical and scientific research, provided that the necessary safeguards are in place, is not considered as being contrary to the original reason for which the data was collected.

(iii) Minimality

The third principle is set out in Article 6(1)*(c)* of Directive 95/46, and is often termed the "minimality principle".[262] As its name suggests, personal data that has been collected must be "adequate, relevant and not excessive" in terms of the purpose for which it is collected.[263]

(iv) Information quality

The fourth principle is set out in Article 6(1)*(d)* and it simply provides that information that has been collected must be of high quality and accurate.[264] Put differently, this principle provides that the personal data to be collected must be of high quality, accurate and up-to-date, and not incomplete. If it is unclear whether this principle can be achieved, provision must be made for the rectification or erasure of the personal information that has been collected.[265]

(v) Retention of records

The fifth principle, which is set out in Article 6(1)*(e),* provides that data should be kept for only as long as it is needed for the adequate processing thereof.[266] However, where there is a need,

---

See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 286 – 287.

[262] Article 6 of Directive 95/46 reads as follows:

> "1. Member States shall provide that personal data must be:
>
> . . .
>
> *(c)* adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."

See also Article 5(1)*(c)* of the GDPR, s 10 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5.

[263] D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 284, and PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 8 – 9.

[264] Article 6 of Directive 95/46 reads as follows:

> "1. Member States shall provide that personal data must be:
>
> . . .
>
> *(d)* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified".

See also Article 5(1)*(d)* of the GDPR, s 16 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 8, and D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 284.

[265] D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 284. See sections 9 to 12 and 16 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 4.

[266] Article 6(1)*(e)* of Directive 95/46, reads as follows:

> "1. Member States shall provide that personal data must be:
>
> . . .
>
> *(e)* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States

or it is required by law, that the data be stored for a longer period, then the appropriate safeguards must be in place to ensure that the data is protected.[267]

(vi) Confidentiality and security of processing

The sixth principle provides for the security as well as the confidentiality of the processing of personal data and is set out in both Articles 16 and 17. Article 16 provides that any person who is processing personal data on behalf of a controller or who has access to the data subject's personal data must not process that data, unless authorised and instructed thereto by the controller.[268]

Article 17 goes on to state that the controller, a person on the controller's behalf (ie a processor) or a processor acting on behalf of the State, must have sufficient technical and organisational security in place so as to prevent the unauthorised or unlawful disclosure, access, or transmission of personal data.[269] Where a processor acting on behalf of the State (as a controller) processes personal data, the processor may act only on the instructions of the controller, and on the obligations as set out in the relevant legislative instrument. To ensure that these measures are applied, the relevant contractual clauses, alternatively the relevant legislative instrument, must be reduced to writing.[270]

---

shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use."

See also Article 5(1)*(e)* of the GDPR, s 14 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5. See also *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197.

[267] This is the case where the data is stored for historical, statistical and scientific research. The private or public organisation must meet the safeguards set out by the relevant legislation drafted by the EU Member State in which they are situated. See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285 – 286. See also Article 6 of Directive 95/46.

[268] Article 16 of Directive 95/46. See also Articles 5(1)(a) and 12 of the GDPR, sections 17 – 18 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 4, and the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 12, and D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 292 and P Hustinx 'EU Data Protection Law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 14.

[269] Article 17 of Directive 95/46, see D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 292 and P Hustinx 'EU Data Protection Law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 12. See sections 19 to 22 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5 and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 11.

[270] There is nothing specifically mentioned regarding the signature of these contractual clauses or legislative instrument – the reason may simply be because these may be attached or form a part of an electronic communication, ie email or other text message, and will therefore not contain a formal "handwritten" signature.

(vii) Accountability

The seventh principle is set out in Article 6(2). This article is aimed at promoting accountability and provides that controllers must apply the principles that are set out above, as well as below and relevant protections when they are processing personal data.[271]

(viii) The data subject's right to participate

The last principle is set out in Articles 10, 11, 12 and 14. These articles collectively provide that the data subject not only has a right to participate but also a right to be informed when their personal data is being processed.

Article 10 provides that when personal data is collected directly from the data subject, the following information must be provided to the data subject: the identity of the controller processing the data, the reason or purpose for the processing, and any further information considered necessary. This further information can include the identity of third parties, where they will be processing the personal data and whether it is compulsory or voluntary to provide the personal data, in line with the purpose.[272]

Article 11 focuses on the scenario where personal data has not been collected directly from the data subject, ie where the personal data is collected from another source or third party. Article 11(1) provides where the data is not collected directly from the data subject, then the controller must provide the data subject with the following information, and it must be provided "no later than at the time when the data are first disclosed": the identity of the controller or its representative, the reason for processing the data, and any further information that may be required under the circumstances. However, the controller need not inform the data subject where the data is processed for historical or scientific research,[273] or where informing the data

[271] Article 6(2) of Directive 95/46 reads as follows: "It shall be for the controller to ensure that paragraph 1 is complied with." Note also the provisions of Article 23 of Directive 95/46, which prescribes that controllers must be fined where they do not apply the principles when processing personal data. See also Recital 85 and Article 5(2) of the GDPR, s 8 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 14.

[272] Article 10 of Directive 95/46, see D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 290. See sections 17 and 18 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 12.

[273] Article 11(2) of Directive 95/46. Note also D Ayala 'Shore to Shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 212 where the author points out that data can be collected everywhere, especially because individuals (ie data subjects) often use technological devices, eg computers, laptops, cell phones, etc. and these technological devices, especially where the are internet enabled, collect, process, and store data of the person using the device. Data is also collected when a data subject visits a webpage – see C Röttgen 'Like or Dislike—Web Tracking' in T Hoeren & B Kolany-

subject of the further processing, would require an effort that is disproportionate to the purpose for processing, or "disclosure is expressly laid down by law".[274]

Article 12 provides that a data subject has the right to access and thereby obtain from the controller, or the relevant person processing their data, the following information:

1 whether data relating to the data subject is being processed by the controller or a third party;

2 the purpose for processing the data; and

3 to whom the data is exposed, as well as the logic involved during the automatic processing of data including the outcomes of the automated process.

The information must be provided to the data subject within reasonable intervals and without undue delay or expense. Furthermore, the data subject has the right to rectify, erase or block the processing of their data where it is inaccurate or incomplete. The rectification, erasure or blocking of personal data must be communicated by the controller to any relevant third parties.[275] Article 11(1)*(c)* expressly provides that data subjects must be made aware of the right to access and rectify their data.[276]

Article 14, as briefly mentioned above,[277] provides a data subject with the right to object to the processing of their personal information in two specific instances.[278] The first of these

Raiser (eds) *Big Data in Context: Legal, Social and Technological Insights* (2018) at 74.

[274] This would also include the need to provide further information regarding the additional processing of the personal data. Article 11(2) of Directive 95/46, See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 286 – 287. See also Articles 13 – 14 of the GDPR, sections 17 and 18 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5 of the thesis, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 12.

[275] Article 12 of Directive 95/46. See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285, P Hustinx 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' EU: European Data Protection Supervisor (Statewatch: Monitoring the State and Civil Liberties in Europe, 15 September 2014) at 13 – 14, A Esteve 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 at 44 – 45. See also Articles 16 – 19 of the GDPR, sections 23 to 25 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5 and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 13.

[276] D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285.

[277] See the discussion on Article 7 of Directive 95/46.

[278] Article 14 of Directive 95/46, and Article 18 of the GDPR. See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285. See sections 23 to 25 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 13.

objections relates to those instances "referred to in Article 7*(e)* and *(f)*".[279] The second objection provides that the data subject may object "to the processing of his personal data", where the controller processes it for the purposes of direct marketing.[280] The objections must be based on persuasive reasons that are relevant to the data subject's personal circumstances, unless national legislation provides otherwise. Data subjects may object to their information being processed for the purposes of direct marketing, and this objection, based on requesting their personal information must be free of charge.[281]

(e) Conclusion

Apart from the articles set out above, Directive 95/46 also provides for a supervisory authority or data protection regulator or officer and for the Article 29 WP,[282] the cross-border transfer of data to both European Union Member States and third countries,[283] sanctions for breaches of articles contained in Directive 95/46,[284] codes of conduct[285] and other miscellaneous provisions in relation to data protection.[286] Articles 4(1) and 32 require that each Member State must enact

[279] Article 14*(a)* of Directive 95/46.
[280] Article 14*(b)* of Directive 95/46.
[281] Under this right also falls the right to object to the automated processing of data, in terms of Article 15, however, where a decision regarding a data subject will be made by automated means, such means must be outlined in a contract. See D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285 and A Esteve 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 at 44 – 45.
[282] Articles 28 to 30 of Directive 95/46. Note also Articles 18 to 21 of Directive 95/46 in relation to the notifications to be given to the supervisory authority.
[283] Articles 25 and 26 of Directive 95/46. The EU and the United States, in light of Article 25(6) enacted the Commission Decision 2000/520/EC of 26 July 2000, known as the "Safe Harbour Privacy Principles" which was declared invalid in *Schrems v Data Protection Commissioner* EU:C:2015:650. After the invalidation of the Safe Harbour Privacy Principles, the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, known as the 'EU-US Privacy Shield', was implemented and this was also declared invalid in *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559. A complete discussion of these judgments is beyond the scope of the thesis, however, where necessary, and in completing the arguments surrounding the right to be forgotten, the relevant parts of these judgments shall be referenced. For a discussion on these judgments and the debates surrounding them (it is very interesting), see T Ojanen 'Making the essence of fundamental rights real: The Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter' (2016) 12 *European Constitutional Law Review* 318 – 329, C Lam 'Unsafe Harbor: The European Union's demand for heightened data privacy standards in *Schrems v. Irish Data Protection Commissioner*' (2017) 40(3) Electronic Supplementary *Boston College International and Comparative Law Review* 1 – 13, S Bu-Pasha 'Cross-border issues under EU Data Protection Law with regards to personal data protection, (2017) 26(3) *Information & Communications Technology Law* 213 – 228, M Rotenberg '*Schrems II*, from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26 *European Law Journal* 141 – 152, P Nebbia 'The *Schrems* judgments: A silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336, and MH Murphy 'Assessing the implications of *Schrems II* for EU–US data flow' (2021) 71 *International and Comparative Law Quarterly* 245–262.
[284] Articles 22 to 24 of Directive 95/46. See also M Burdon, B Lane & P von Nessen 'The mandatory notification of data breaches: Issues arising' (2010) 26 *Computer Law & Security Review* 115 – 129.
[285] Article 27 of Directive 95/46.
[286] Articles 32 to 34 of Directive 95/46.

legislation pursuant to Directive 95/46. However, when doing so Member States have a certain amount of freedom concerning how far to enact the directive and the ultimate application thereof, even though an approximated or harmonious approach is preferred. Unfortunately, this flexibility has produced a fragmented data protection landscape throughout the EU.[287] Furthermore, Directive 95/46 provided that each Member State must enact its national law within three years of the date on which the directive came into force. While some Member States kept to the time limit, others did not.[288]

Directive 95/46 has been used to deal with the tricky questions of finding personal information available on the internet, and a good example of this is seen in *Google Spain*, where the CJEU, in light of the right to freedom of expression and privacy, briefly set out that internet searches have simplified obtaining information, including personal information, with the use of a few keystrokes.[289]

Directive 95/46 was repealed on 25 May 2018 by the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).[290] Poullet,[291] and De Hert and Papakonstantinou[292] point out that the transposition of Directive 95/46 by the EU Member States into their national legislation was inconsistent and that this resulted in a fragmented statutory landscape. Under the GDPR, however, they point out further, there will be a more integrated and harmonious statutory landscape. This is because Member States do not have the freedom to decide for themselves whether and to what extent a

[287] This has been more fully discussed under '(b) Objective and scope' above. Recital 9 of the GDPR. See generally F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, where the author provides a succinct discussion of how directives are implemented.

[288] See generally F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, and R Thomson, R Torenvlied & J Arregui 'The paradox of compliance: Infringements and delays in transposing European Union directives' (2007) 37 *British Journal of Political Science* 685 – 709. For specific examples see S Chalton 'The transposition into UK law of EU Directive 95/46/EC (the Data Protection Directive)' (1997) 11(1) *International Review of Law, Computers & Technology* 25 – 32, O Estadella-Yuste 'Spain is on the road to implementing EU Directive 95/46' (1997) 11(1) *International Review of Law Computers & Technology* 33 – 46, and J Dumortier & DM Alonso Blas 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 – 242.

[289] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 36, see also Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 212 – 216.

[290] Article 99 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

[291] Y Poullet 'Is the general data protection regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774.

[292] P De Hert & V Papakonstantinou 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 132.

regulation should be applied in their own specific jurisdictions.[293] A further point to note is that when a regulation is adopted by the Council of European and Parliament, it comes into force across the EU, ie in all Member States, on the same day and there is no delay in its implementation.[294] Lastly, the data protection framework of the EU needed to be reformed, in order to meet the new challenges posed by technology in protecting personal data and the right to privacy.[295]

The key provisions of the GDPR in light of the right to be forgotten are set out and discussed in the next section.

III THE GDPR

(a) Introduction

This is a brief discussion of the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).[296] The GDPR was designed to meet the need of protecting personal data in light of technological advancements, such as

[293] See generally, Recital 9 of the GDPR, F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, where the author provides a succinct discussion of how directives are implemented, R Thomson, R Torenvlied & J Arregui 'The paradox of compliance: Infringements and delays in transposing European Union Directives' (2007) 37 *British Journal of Political Science* 685 – 709, and S Hurka & Y Steinebach 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 278 – 279, 281, and 283. See also the comments on uniformity when interpreting EU laws by the CJEU in *UI v Österreichische Post AG* EU:C:2023:370 paras 29 and 48.

[294] See generally, F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, and S Hurka & Y Steinebach 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 281.

[295] Recital 6 of the GDPR, and M Burri & R Schär 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 479 at 480 – 481, and C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 135.

[296] See generally P De Hert & V Papakonstantinou 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 – 142, M Burri & R Schär 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 479 – 511, Y Poullet 'Is the General Data Protection Regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 – 778, S Bhaimia 'The General Data Protection Regulation: The next generation of EU Data Protection' (2018) 18 *Legal Information Management* 21 – 27, C Hoofnagle, B van der Sloot & F Zuiderveen Borgesius 'The European Union General Data Protection Regulation: What it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65 – 98, C Docksey & H Hijmans 'The Court of Justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law' (2019) 5 *European Data Protection Law Review* 300 at 313 – 316, ML Jones & ME Kaminski 'An American's guide to the GDPR' (2020) 98 *Denver Law Review* 93 – 128, G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 440 – 442, A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 2 – 3, and F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 – 938. See also *Ibex RSA Holdco Ltd & another v Tiso Blackstar Group (Pty) Ltd & others* [2024] ZASCA 166 para 27.

the internet, email, etc.[297] Directive 95/46 was drafted during a period when the internet and email were relatively new.[298] Hence, there was uncertainty as to how Directive 95/46 applied in an ever-changing online environment. Furthermore, the domestication of Directive 95/46 in the various Member States created a fragmented approach to the field of data protection, despite there being certain basic principles that every Member State had to adhere to.[299] Unlike the Directive, the GDPR data protection framework provides a coherent approach, with strong enforcement mechanisms to ensure compliance therewith.[300] Simultaneously, with the GDPR, although to a limited extent, it is also applicable to criminal matters, the EU enacted Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive).[301] The Law Enforcement Directive goes hand-in-hand with the GDPR, by specifically protecting the rights of data subjects that find themselves, either as accused, witness or complainants, within criminal law proceedings.[302] The Law Enforcement

[297] See Recital 6 of the GDPR, P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 180 – 181, M Burri & R Schär 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 479 at 480 – 481, E Peuker 'The EU General Data Protection Regulation: Powerful tool for data subjects?' *VerfBlog*, 22 June 2016.

[298] M Kędzior 'GDPR and beyond—a year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 506.

[299] A Roos 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected "Content Principles"' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* #7985 1 at 3.

[300] A Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected "content principles"' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* #7985 1 at 3. See the discussion under "(b) Objectives and scope" under Directive 95/46 above for a more in-depth discussion and with additional reasons as to why the GDPR was drafted.

[301] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive). The Law Enforcement Directive came into force on 4 May 2016, ie the day it was published in the Official Journal of the European Union – Article 64, which reads: 'Entry into force. This Directive shall enter into force on the day following that of its publication in the Official Journal of the European Union.' See generally, M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 479 – 480.

[302] See generally *VS (Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost, third party)* EU:C:2023:49 for a discussion on the application of the Law Enforcement Directive in light of the collection of biometric and genetic data, M Kędzior 'GDPR and beyond—a year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 508, and for a general comment on how rights are protected during criminal proceedings (not necessarily referencing the applicable legal principles). See also K Belogubets 'The protection of personal data in the context of law enforcement: recent case law of the European Court of Human Rights' (2021) 22 *ERA Forum* 231 – 243. Lastly, there is one further directive to note in light of criminal investigations, namely Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), which concerns itself with the protection of privacy during criminal investigations where, after an application to court, the investigators obtain an order "authorising the interception, recording and storage of" the tele- and electronic communications of suspects deemed to "have committed serious criminal offences". See *HYA & others* EU:C:2023:102 as an example of how the Directive on

Directive will not be dealt with in this thesis, unless there is a specific aspect that needs to be covered in light of data protection and the right to be forgotten.

One significant aspect of the GDPR is that the aims and objectives have been clarified and are more definitive; they are also more expansive than the previous provisions.[303] It is important to note that it came into effect after only the CJEU had established the right to be forgotten for the first time.[304] The GDPR codifies the right to be forgotten in Article 17.

The discussion herein will follow the same pattern as the discussion of Directive 95/46 set out above, ie the objects and scope, the definitions and the basic principles regarding the processing of personal data as provided in the GDPR, and the focus will be on the equivalent articles in Directive 95/46, as used in *Google Spain*. However, Article 17 will be discussed separately as this is the first time that it was specifically expressed in EU legislation.

(b) Objectives and scope

Like Directive 95/46, the objectives of the GDPR are set out in the preamble and Article 1. Article 1 provides that the GDPR's main focus is the protection of the rights of natural persons during the processing of their personal data.[305] Once again, certain Recitals will be referred to as they provide the context or reason for drafting the GDPR.[306] Recitals, 4, 9, 10, 11, 13, 16, 65 and 66 are important for this discussion. Recital 4 states that data protection is not an absolute right, but must be considered and balanced with the fundamental rights and freedoms enshrined in the Charter, and that "it must be considered in relation to its function in society".[307]

---

privacy and electronic communications was applied, first with Directive 95/46, and now with the GDPR. A complete discussion of this topic is beyond the scope of this thesis.

[303] P De Hert & V Papakonstantinou 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 134 – 137.

[304] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[305] S Abiteboul & J Stoyanovich 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation' (2019) 11(3) *Journal of Data and Information Quality* 1 at 2. *B v Latvijas Republikas Saeima* EU:C:2021:504 held that the GDPR prohibits the release of information that is detrimental to the data subject, ie the availability of the penalty points that a person had collected for driving offences. The CJEU held that there are alternative methods that will provide access to the relevant persons, who are in need of such information, eg the person must establish why they have an interest in the information, etc. See also *LB v Hungary* [2023] ECHR 239 para 52.

[306] T Klimas & J Vaiciukaite "The law of recitals in European Community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61 at 64. See also *Puppinck & others v European Commission* EU:C:2019:1113 para 75, Opinion of Advocate General Bobek in *Puppinck & others v European Commission* (Case C-418/18P) EU:C:2019:640 para 93. Compare with *Capitec Bank Holdings Ltd & another v Coral Lagoon Investments 194 (Pty) Ltd & others* 2022 (1) SA 100 (SCA) paras 25 and 50.

[307] Recital 4 of the GDPR, expresses the following rights that need to be considered:

> "in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

Although Recital 4 states that data protection is not an absolute right,[308] Recitals 9, 10, 11 and 13 all emphasise the notion that personal data must be afforded a high level of protection throughout the EU. Recitals 9, 10, 11 and 13 do not only applaud the principles and objectives of Directive 95/46 as comprehensive, but also point out, as fully discussed above, that Member States failed to apply the principles uniformly.[309] However, since the GDPR is in the form of a regulation, Member States have no discretion when it comes to the application of the GDPR within their jurisdictions, and this promotes a consistent and harmonious approach throughout the EU.[310] Recital 13 specifically calls for uniformity in the level of protection to aid the free flow of personal data within the internal EU market, and the various data supervisory authorities of each Member State are responsible to achieve this uniformity.

Recital 65 provides that data subjects may implement the right to be forgotten where "the retention of [personal] data infringes this Regulation", and Recital 66 aims to strengthen the right to be forgotten "in the online environment". Where the retention of the information is lawful then the right to be forgotten must be balanced with[311]

> "the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims."

Recital 65 echoes the sentiments stated by the CJEU in *Google Spain*.[312] In *Google Spain*, the court held that the right to be forgotten of the data subject is not absolute, and must be balanced against the rights, freedoms and interests of internet users.[313]

---

[308] *JM* EU:C:2023:501 para 78.

[309] See *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2023:2 para 54 where the CJEU stressed that the GDPR must be applied uniformly across the EU, ie there must be a "consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data throughout the European Union."

[310] Poullet points out that there is limited "manoeuverability" but largely the entire Regulation will now detail the approach that all EU Member States must take in the implementation and application of the principles to protect the personal data of data subjects – see Y Poullet 'Is the General Data Protection Regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774. See also M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 490ffg.

[311] See the judgments of *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:276 paras 212 – 216 and *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:277 paras 165 – 169.

[312] *Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonzále*z EU:C:2014:317 para 81. See also JS Van Oyen, M Lange & S Kreinsen, 'The Right to Be Forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 at 306 – 307.

[313] Specifically, the data subject's rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter). See *Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 68 – 69, see

Recital 66 requires the removal of links, copies and replications of the impugned information. The controller processing the personal data, using the available technology, and taking the necessary reasonable steps, must inform other controllers that are also processing the data, that the data will be erased.[314]

There are two further articles that are important to this discussion, namely Articles 2 and 3. Article 2 sets out the scope of the GDPR, and provides that the GDPR applies to all processing of personal data, whether or not the processing is carried out by automated means.[315] However, Recital 16 provides that the processing of personal data in terms of issues relating to the national security of the individual Member States, or the common EU foreign and security policy, will not be subjected to the provisions of the GDPR.[316]

Article 3 deals with the territorial scope of the GDPR. The GDPR applies, irrespective of whether the personal data will be processed within the EU or not, to all EU citizens. The GDPR creates a limited global territorial scope, as it applies to all processing that affects the EU citizens' personal data.[317]

(c) Definitions

Unlike Directive 95/46, the GDPR contains a long list of definitions (23 in total, whereas Directive 95/46 only had 8). While some of these are relevant for the right to be forgotten, others are not. The definitions are set out in Article 4 of the GDPR.[318] Those definitions that

---

also *Bernard Connolly v European Commission* EU:C:2001:127 para 37 and *Rechnungshof v Österreichischer Rundfunk & others and two other cases* EU:C:2003:294 para 68. Recital 65 further states that if a child has given their consent to the processing of their personal data but does not fully understand the risks involved, they may request the removal of their data, especially on the internet, even when they are an adult. See M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 201. Note also the comments made in *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791 para 120 – 122, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258 para 48.

[314] S Ziegler, E Evequoz, & AM Pacheco Huamani 'The impact of the European General Data Protection Regulation (GDPR) on future data business models: Toward a new paradigm and business opportunities' in A Aagaard (ed) *Digital Business Models* (2019) at 214.

[315] See BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 133 – 135.

[316] *Ligue des droits humains v Conseil des ministres* EU:C:2022:491 paras 67, and 83 – 84. C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 138.

[317] Article 3 and Recitals 14 and 122 of the GDPR. See also Y Poullet 'Is the General Data Protection Regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774, M Zalnieriute '*Google LLC v. Commission nationale de l'informatique et des libertés* (*CNIL*)' (2020) 114(2) *The American Journal of International Law* 261 – 267, C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 138, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[318] Tikkinen-Piri *et al* point out that several of the new definitions are there to manage the processing operations

are relevant to the right to be forgotten will be discussed hereunder.

Article 4(1) of the GDPR contains the definition of "personal data".[319] The definition has remained largely the same as the definition in Article 2*(a)* of Directive 95/46, but has been expanded to include more "identifiers". The full list of identifiers is as follows: "*a name*, an identification number, *location data*, *an online identifier* or one or more factors specific to the physical, physiological, *genetic*, mental, economic, cultural or social identity of that natural person".[320] The GDPR, in meeting the issues posed by technological advancements, has "location data" and "online identifier" to cover this aspect.[321]

"Processing" is defined in Article 4(2). Unlike Article 2*(b)* of Directive 95/46, which referred to the "processing of personal data ('processing')", Article 4(2) refers simply to "processing", although nothing seems to turn on this difference. More importantly, the definition has largely stayed the same, although it does now include the processing of personal data sets, as well as the structuring of data. These additions may all allude to the GDPR's attempt to include the operations of search engines, including their search tools, in the definition of "processing".[322]

---

of data intensive companies or big data companies and strengthen the protection of data subjects where their data is being processed by data intensive companies to meet their processing objectives – see C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 138. See also M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 495 – 496.

[319] Note, the debate surrounding whether the word "data" or "information" should have been used, is a debate that goes beyond the scope of the thesis, see the definition of "personal data" in terms of Directive 95/46, and the footnote listing the sources that elaborate on this debate. Note that the information must "relate to" an identifiable natural person, as was discussed briefly in terms of Article 2*(a)* of Directive 95/46, see *Nowak v Data Protection Commissioner* EU:C:2017:994 paras 31 – 35, *SRB v EDPS* EU:T:2023:219 paras 68 – 69, 73, and 88 – 93, *FF v Österreichische Datenschutzbehörde* EU:C:2023:369 paras 22 – 26, and *JM* EU:C:2023:501 paras 41 – 45. For a brief discussion on *Nowak v Data Protection Commissioner* EU:C:2017:994 see N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 at 66 (see also the complete discussion on the definition on "personal data" at 61 – 72). The General Court of the CJEU in *SRB v EDPS* EU:T:2023:219 defined the scope of the definition of "personal data" as provided in Article 3(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018, however Article 3(1) reads exactly the same as Article 4(1) of the GDPR. Hence, it is useful to note the discussion in *SRB v EDPS*.

[320] The additional identifiers have been italicised for ease of reference.

[321] Location data is important with reference to mobile devices or cell phones, that send their location to cell phone towers, and the Global Positioning System or GPS used for navigation and tracking of individuals, especially in criminal investigations. See *Uzun v Germany* [2010] ECHR 2263, and *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702. See also L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808 1 at 1 – 3 regarding de-identifying personal data.

[322] Regarding the retention or storage of personal data, which amounts to processing as per the definition in the GDPR, the CJEU in *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* EU:C:2022:702 and *VD & SR* EU:C:2022:703 confirmed that the indiscriminate retention of personal data, irrespective of time periods, is not authorised in terms of the GDPR. It was confirmed that the retention of especially traffic and

The definition of a "controller" has also remained the same. Article 4(7) of the GDPR thus defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data".[323] It also provides that "where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination, may be provided for by Union or Member State law". The reference to "Union or Member State law" differs from Article 2 of Directive 95/46, which refers to "national or Community law". While the reference to "Union or Member State law" provides better clarification – especially to those outside the EU – nothing turns on this difference. Article 26 of the GDPR defines joint controllers as "two or more controllers who jointly determine the purposes and means of processing".[324] Article 26 further requires the communication of their arrangement, as joint controllers, to the data subject. Articles 13 and 14 of the GDPR require joint controllers must be transparent as to their responsibilities and duties to data subjects.[325]

A "processor" is defined in Article 4(8) and this definition has largely stayed the same as the definition in Article 2*(e)* of Directive 95/46, with the only difference being a minor one,

---

location data amounts to an infringement on the right to a private life, as this data reflects the data subject's personal movement. Specifically, in *VD & SR*, which relates to digital marketing, the CJEU held that the relevant national legislation was not the basis on which data may be retained by private actors, only the State authorities, in terms of the legislative framework, may do so. In *Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH* the CJEU held that such data, including IP addresses, may be retained to combat serious crime. This will not be discussed further as it is beyond the scope of the thesis, however where there is a reference to the right to be forgotten, that part alone may form a part of a discussion. Note in *Breyer v Bundesrepublik Deutschland* EU:C:2016:779 the CJEU held that an IP address amounts to personal data, as it is an "online identifier", see also *SRB v EDPS* EU:T:2023:219 paras 88 – 93, and *JM* EU:C:2023:501 para 46. See also N Purtova 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 at 62 – 65. In light of unstructured personal data EM Weitzenboeck, P Lison, M Cyndecka & M Langford 'The GDPR and unstructured data: Is anonymization possible' (2022) 12(3) *International Data Privacy Law* 184 at 186 – 188.

[323] Chapter IV of the GDPR, provides for the duties of both controller and processors in light of the processing and protection of personal data. See specifically Article 24 regarding the functions of controllers. Furthermore, Section 4 of Chapter IV there is provision for a data protection officer (in South Africa this position if referred to as the information officer, sections 55 and 56 of the Protection of Personal Information Act 4 of 2013). See also *ZS v Zweckverband "Kommunale Informationsverarbeitung Sachsen" KISA, Körperschaft desöffentlichen Rechts* EU:C:2023:81 on a discussion of Article 38 dealing with the position of the data protection officer, in light of their duties as provided for in Article 39. See *X-FAB Dresden GmbH & Co. KG v FC* EU:C:2023:79 regarding the dismissal of a data protection officer due to a "conflict of interest" between their functions as a data protection officer and their further functions in terms of the company.

[324] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388 paras 25 – 44, and *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629 paras 64 – 85.

[325] Article 13 of the GDPR relates to "information to be provided where personal data are collected from the data subject". Article 14 on the other hand relates to "information to be provided where personal data have not been obtained from the data subject". See C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 142, see also D Ayala 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 212 regarding the collection of data generally.

ie the word "any" was dropped from "any other body", but nothing seems to turn on this difference.[326]

"Consent" is defined in Article 4(11) of the GDPR, as follows: "any freely given, specific, informed and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (my emphasis).[327] The concept is essentially similar to the definition of "data subject's consent" as provided in Directive 95/46.[328] However, the term "unambiguous"[329] did not appear in the equivalent definition in Directive 95/46. According to the European Data Protection Board (EDPB),[330] the term "unambiguous" is aimed at ensuring that the data subject's consent is provided by way of a positive act or declaration, such as a written statement.[331] In this respect, it is important to note that the need to provide active consent means that consent may also be actively withdrawn and that data subjects do have control over their personal data.[332]

---

[326] Article 4(8) of the GDPR "processor" means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". See C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 142. Note also, Chapter IV of the GDPR, which provides for the duties of both controller and processors, as explained above.

[327] Article 4(11) is to be read with Article 7 and Recitals 32, 33, 42, and 43 of the GDPR regarding the controller's responsibilities where consent is at issue. Note also Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679*, revised and adopted 10 April 2018, European Data Protection Board *Guidelines 05/2020 on consent under Regulation 2016/679* adopted 4 May 2020 paras 8 – 9 at 6. See also C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 139, and M Gerhold 'Rote Ampel für Geisterfahrer: Zur (hoffentlich letzten) EuGH-Entscheidung in Sachen Vorratsdatenspeicherung, *VerfBlog*, 21 September 2022.

[328] Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679*, revised and adopted 10 April 2018 at 4 – 5.

[329] Neither did "by a statement or by a clear affirmative action", but it works hand-in-hand with the phrase "unambiguous" as explained in the text – see C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 139.

[330] The European Data Protection Board replaced the Article 29 Data Protection Working Party.

[331] European Data Protection Board *Guidelines 05/2020 on consent under Regulation 2016/679* adopted 4 May 2020 paras 75ffg at 148ffg. Note also *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 para 52. Compare with G Jenkins 'An extended doctrine of implied consent – A digital mediator?' (2021) 52 *International Review of Intellectual Property and Competition Law* 706 – 733.

[332] European Data Protection Board *Guidelines 05/2020 on consent under Regulation 2016/679* adopted 4 May 2020 para 10 at 7. The CJEU's *Grand Chamber in Meta Platforms Inc. & others v Bundeskartellamt* EU:C:2023:537 paras 140 – 154 held that Meta/Facebook as the dominant social media network company (and also as the dominant "partner" in the user agreement) must obtain the user's specific consent to process the user's data to show advertising material that matches their interests. This includes the collection and processing of data that is obtained both on Facebook, as well as other related Meta social networks, and personal data collected off Facebook, such as internet browsing habits, and the type of cell phone a user accessed Facebook from. For a comment on *Meta Platforms v Bundeskartellamt* see O Brook & M Eben 'Another missed opportunity? Case C-252/21 *Meta Platforms v Bundeskartellamt* and the relationship between EU competition law and national laws' (2023) *Journal of European Competition Law & Practice* 1 – 5, and I Graef '*Meta platforms*: How the CJEU leaves competition and data protection authorities with an assignment' (2023) 30(3) *Maastricht Journal of*

Lastly, one of the new definitions is "supervisory authority". This definition, which did not appear in Directive 95/46, is found in Article 4(21) of the GDPR and simply states that a supervisory authority is "an independent public authority which is established by a Member State pursuant to Article 51". In terms of the GDPR, the national supervisory authority within each Member State must, after an investigation finds that a data subject was not "afforded an adequate level of protection", irrespective of the reason for the "inadequacy", take steps to have the "inadequacy" remedied.[333] Furthermore, once a Member State's supervisory authority has found an "inadequacy", that Member State's supervisory authority must take steps to remedy the "inadequacy" regardless of the reason.[334]

The above is the backdrop to the principles that possibly form the core regarding the lawful processing of personal data.

(d) Principles and the right to be forgotten

The GDPR encourages that data protection is "by design and by default".[335] Put differently, the GDPR promotes mechanisms to protect the privacy of data subjects and these must feature or

---

European and Comparative Law 325 – 334. See also W Kerber & KK Zolna 'The German Facebook case: The law and economics of the relationship between competition and data protection law' (2022) 54 *European Journal of Law and Economics* 217 – 250 for a summary of the debates before the matter was heard by the CJEU's Grand Chamber, including the interaction between the competitive data market and privacy. See also *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:276, and *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:277 where the CJEU's Fifth Section of the General Court came to similar conclusions. Balancing the right to privacy with the right to economic gain in light of competition laws is not a specific focus of the thesis, it is still important to mention. Lastly, the following article is still important to note as it details the digital dominance of social media websites generally on the internet, and how they are monopolising data subjects by offering various services, such as online shopping, etc.: B Ong & DJ Toh 'Digital dominance and social media platforms: Are competition authorities up to the task?' (2023) 54 *International Review of Intellectual Property and Competition Law* 527 – 572.

[333] *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2024:239 para 34.

[334] European Data Protection Board *Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements* adopted 2 February 2021.

[335] Article 25 and Recitals 78 and 108 of the GDPR, *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 paras 66 – 67, M Goddard 'The EU General Data Protection Regulation (GDPR): European Regulation that has a global impact' (2017) 59(6) *International Journal of Market Research* 703 at 703, M Veale, R Binns & J Ausloos 'When data protection by design and data subject rights clash' (2018) 8(2) *International Data Privacy Law* 105 – 123, and S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 – 27. For a comprehensive discussion on "privacy by design" as well as for extra information, see DL Donnelly *Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020). For a critical look at the concept of "privacy by design see BJ Koops & R Leenes 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data protection law' (2014) 28(2) *International Review of Law, Computers & Technology* 159 – 171, although written before the enactment the GDPR, it provides a useful guide as to how the concept should be approached and implemented. In relation specifically to mobile technology see, E Stiakakis, CK Georgiadis & A Andronoudi 'Users' perceptions about mobile security breaches' (2016) 14 *Information Systems and e-Business Management* 857 – 882.

be built into systems and processes which are used to process personal data. Data protection that is "by design and by default" requires that concrete, adequate, reasonable technical measures are in place, where personal data is being processed, to ensure the privacy of the data subject. Whether these measures are adequate and reasonable will depend on the data being processed, the reason for the processing, the nature of the data controller's business, as well as any cost implications. This also includes that "both at the time of the determination of the means for processing and at the time of the processing itself", the implemented "technical and organisation measure" may include

> "pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[336]

In other words, those that process personal data must adhere to the data processing principles that are clearly set out in Article 5 of the GDPR.[337] Similarly, as in the discussion in Directive 95/46, the themes regarding the processing of personal data will be used. These themes are: the legitimacy of data processing, purpose specific, minimality, information quality, retention and restriction of records, security safeguards, accountability and data subject participation.[338] The principles in the GDPR are similarly worded as those in Directive 95/46, hence the discussion will be kept to a minimum.

(i) Legitimacy of processing

The first principle is found in Article 5(1)*(a)* and it provides that personal data must be

---

[336] Article 25 of the GDPR, and see generally DL Donnelley '"Privacy by design" in the EU General Data Protection Regulation: A new privacy standard or the emperor's new clothes?' (2022) 139(3) *South African Law Journal* 541 – 575.

[337] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 53 – 59, *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, and M Burri & R Schär 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490.

[338] Article 5 of the GDPR. Note also A Roos 'Core principles of data protection law' (2006) 39(1) *Comparative and International Law Journal of Southern Africa* 107 – 130, OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) paras 7 – 14, A Mantelero 'Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution' (2012) 3(2) *European Journal for Law and Technology*, A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 213 at 223 – 226, M Goddard 'The EU General Data Protection Regulation (GDPR): European Regulation that has a global impact' (2017) 59(6) *International Journal of Market Research* 703 – 705, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 24. See also the Protection of Personal Information Act 4 of 2014, specifically the Conditions for Lawful Processing of Personal Information, sections 8 – 25.

processed in a transparent, fair and lawful manner. Unlike Article 5(1)*(a)*, Article 6(1)*(a)* of Directive 95/46 did not include the term "transparent". The requirement of transparency, however, is not new. The principle is referred to as "lawfulness, fairness and transparency".[339] Processing in terms of this principle includes, taking into account any other conventions, informing the data subject of who will have access to their personal data,[340] notifying the data subject when data is received from a third party and controllers.[341] Processors must be open or transparent regarding the reasons for processing.[342]

Article 6 of the GDPR is headed "lawfulness of processing" and provides that the processing of personal data will be lawful only where one of the following justifications apply, namely, (a) the data subject has consented thereto,[343] (b) processing is in terms of a contractual relationship between the data subject and the controller, (c) the controller needs to process the data to comply with a legal obligation, (d) it is necessary to process the data subject's data to protect their "vital interests", (e) processing is in light of a public interest obligation or "in the exercise of official authority vested in the controller", and (f) the processing is in the interests of the controller or a third-party, as long as the processing of the personal data does not impact

---

[339] Article 5(1)*(a)* of the GDPR reads:

> "1. Personal data shall be:
> *(a)* processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")".

Article 5(1)*(a)* needs to be read with Article 6 of the GDPR. Articles 6(1)*(a)* and 7 of Directive 95/46. See also sections 9, 17 and 18 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) paras 9 and 10. *VS v Inspektor v Inspektorata kam Visshia sadeben savet* EU:C:2022:967, M Burri & R Schär 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490 and 492, S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 5 – 8, 10, and 25. Note also *VS (Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost, third party)* EU:C:2023:49.

[340] Article 13 of the GPDR, S Bhaimia 'The General Data Protection Regulation: The next generation of EU Data Protection' (2018) 18 *Legal Information Management* 21 at 25.

[341] Article 14 of the GDPR, S Bhaimia 'The General Data Protection Regulation: The next generation of EU Data Protection' (2018) 18 *Legal Information Management* 21 at 25. See also D Ayala 'Shore to Shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 212 regarding the collection of data generally.

[342] Article 12 of the GDPR.

[343] See *UZ v Bundesrepublik Deutschland* EU:C:2023:373 paras 72 – 73 and 75 where the CJEU confirmed that consent is not required where one of the other grounds of lawful processing of data is present, ie such as where the controller fulfils a legitimate or public interest obligation, such as where a court exercises it judicial powers in processing the personal data, this amounting to processing having been done within the public interest or "in the exercise of official authority". See also *Meta Platforms Inc. & others v Bundeskartellamt* EU:C:2023:537 para 154, where the court held:

> "point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator."

adversely on the data subjects interests or fundamental freedoms (this last point does not apply to public authorities who need to process personal data in the performance of their duties).[344] Hence, consent is merely one of six justifications that applies to the processing of personal data. Put differently; there is no need to obtain the consent of the data subject every time personal data is processed. It is important to note, however, that in such a case, the processing must be in terms of one of the other five grounds or justifications provided in Article 6(1).[345]

(ii) Purpose specification

This second principle is contained in Article 5(1)*(b)*.[346] It provides that personal data must be collected for a specified, explicit and legitimate purpose only. The GDPR has retained the exception that allows for the collection of data for historical, statistical and scientific research. If further processing of personal data is required, it may be compatible with the original reason for such collection.

---

[344] *OT v Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, *VS v Inspektor v Inspektorata kam Visshia sadeben savet* EU:C:2022:967, and *UZ v Bundesrepublik Deutschland* EU:C:2023:373 paras 55 – 58. See generally *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums* EU:C:2023:270, where the CJEU applied Article 6(1)*(c)* and *(e)*, with Article 6(3) and Article 88 of the GDPR, in relation to the processing of personal data in the context of employment. See also *Meta Platforms Inc. & others v Bundeskartellamt* EU:C:2023:537 para 126 where the Grand Chamber held:

> "for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party."

See also the judgments of *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:276 paras 212 – 216 and *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:277 paras 165 – 169.

[345] *UZ v Bundesrepublik Deutschland* EU:C:2023:373 paras 72 – 73 and 75.

[346] Article 5(1)*(b)* of the GDPR reads as follows:

> "1. Personal data shall be:
> *(a)* . . .
> *(b)* collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation")".

Article 6(1)*(b)* of Directive 95/46, see also sections 13 and 14 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 7. See generally, *'SS' SIA v Valsts ieņēmumu dienests* EU:C:2022:124 paras 48 – 58, and *VS v Inspektor v Inspektorata kam Visshia sadeben savet* EU:C:2022:967. M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490 and 493 – 494, S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25, D Hadwick 'Peer reviewed articles: "Behind the one-way mirror: Reviewing the legality of EU tax algorithmic governance"' (2022) 31(4) *EC Tax Review* 184 at 189, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 10 – 11, 12 – 13, and 25.

(iii) Minimality

The third principle is set out in Article 5(1)*(c)* of the GDPR, refers to "data minimisation."[347] Data minimisation fits in with Article 25 and Recitals 78 and 108 of the GDPR, which specifically require that personal data protection must be automatic, ie "by design and by default". Controllers must collect only the minimum amount of personal data necessary for processing purposes.[348]

(iv) Information quality

This fourth principle provided in Article 5(1)*(d)* requires that data must be accurate and current.[349] If the personal data is outdated, then, in light of the purpose for processing, every effort must be made to erase and rectify the personal data without hesitation.[350] The GDPR specifically states that the corrections must be made "without delay". It is generally accepted

---

[347] Article 5(1)*(c)* of the GDPR reads as follows:

> "1. Personal data shall be:
>
> . . .
>
> *(c)* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")".

See also Article 6(1)*(c)* of Directive 95/4, and s 10 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5. M Burri & R Schär 'The reform of the EU Data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490 and 494, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 13 – 14, and 25.

[348] PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 6 – 9, E Stiakakis, CK Georgiadis & A Andronoudi 'Users' perceptions about mobile security breaches' (2016) 14 *Information Systems and e-Business Management* 857 – 882, S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25, C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 135, 139 142, 146 and148, DL Donnelly *Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020).

[349] Article 5(1)*(d)* of the GDPR reads as follows:

> "1. Personal data shall be:
>
> . . .
>
> *(d)* accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy")".

Article 6(1)*(d)* of Directive 95/46, see also s 16 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 8, M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490, S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25, A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 14 – 15, and 25.

[350] Article 89 of the GDPR it titled "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" and provides the general safeguards where data is processed for historical, statistical and scientific research, as well as the criteria, etc that must be followed where the personal data is archived for later research. S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25.

that "without delay" or "without due delay" means that the controller has about one month to carry out the request.[351]

(v) Retention of records

This fifth principle as provided in Article 5(1)*(e)* and is simply referred to as "storage limitation", and requires that the personal data that identifies the data subject should be kept for only as long as it is needed for the adequate processing thereof.[352] Once again, this sub-article provides for the archiving of personal data where it is in the interests of the public, and for historical, statistical and scientific research in terms of Article 89 of the GPDR.[353]

(vi) Confidentiality and security of processing

Article 5(1)*(f)* details the sixth principle, which provides that personal data must be kept confidential and secured against any breach, destruction, loss or damage, irrespective of whether this occurs accidentally or is accessed through unauthorised means.[354] Prevention must

---

[351] J Connolly 'The right to erasure: Comparative perspectives on an emerging privacy right' (2021) 46(1) *Alternative Law Journal* 58 at 62.

[352] Article 5(1)*(e)* of the GDPR, reads as follows:

> "1. Personal data shall be:
>
> . . .
>
> *(e)* kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")."

Article 6(1)*(e)* of Directive 95/46, see also s 14 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5. M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490 and 494, S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 15 – 16, and 26.

[353] Articles 5(1)*(e)* and 89 of the GDPR. Compare with *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258.

[354] Article 5(1)*(f)* of the GPDR reads as follows:

> "1. Personal data shall be:
>
> . . .
>
> *(f)* processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")".

Article 16 of Directive 95/46, see sections 19 to 22 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5 and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 11, M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 489 – 490 and 493, and S Bhaimia 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 at 25. See also PTJ Wolters 'The security of personal data under the GDPR: A harmonized duty or a shared responsibility?' (2017) 7(3) *International Data Privacy Law* 165 – 178 regarding the application of the GDPR to cloud storage and access, where the data, on the

be made with the appropriate technical and/or organisational measures. This is referred to as the principle of "integrity and confidentiality".[355] Specifically, Recital 49 provides that confidentiality is required not just during processing but also where personal data is stored (which is a part of processing in terms of Article 4(2)) and transmitted.[356]

(vii) Accountability

Article 5(2), which is the seventh principle in this list, simply refers to the principle of "accountability" and places the responsibility of complying with the data processing principles on the controllers.[357] If there is a breach of the data processing principles, Recital 85 of the GDPR provides that the controller must prove that the breach will not affect the rights of the data subject. Accountability runs through the GDPR like a thread, for example, in Article 35, where there is a possibility of a "high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".[358]

(viii) The data subject's right to participate

The last principle is not provided for in Article 5. Instead, the GDPR has devoted an entire chapter to it, namely Chapter III. Chapter III is entitled "Rights of the Data Subject" and is divided into 12 articles (Article 12 to Article 23). The thesis, however, will focus only on those articles that relate to the principle of participation. The principle of participation is dealt with

instruction of company A (eg in Germany) is stored in a cloud by company B (eg in the Netherlands), and company A needs to access this data on a regular basis for the functioning of its business.

[355] See also Recitals 39, 49, 75, 83, and 85 of the GDPR, Articles 28, 32, and 38 set out the requirements for the various actors that are involved in the processing of personal data with regards to keeping the personal data confidential. See A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 16 – 17, 20 – 21, and 26.

[356] Recital 49 of the GDPR.

[357] Article 5(2) of Directive 95/46 reads as follows: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")." Note also Recital 85 of the GDPR. Articles 6(2) and 23 of Directive 95/46, see also s 8 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) para 14. See *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 paras 83 and 90, where the court held, read with Articles 19 and 24, that this included communicating to third parties the withdrawal of the data subject's consent to process their personal information. In *UZ v Bundesrepublik Deutschland* EU:C:2023:373 para 53 the CJEU held that the controller or processor of the personal data "must be able to demonstrate its compliance with each of the principles set out in" Article 5(1). See also C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 139, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 21 – 23, 24, and 26.

[358] K Demetzou, 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review* 105342 1 at 3 – 4.

under the headings, "Right of access by the data subject" (Article 15), "Rectification and erasure" (Articles 16 – 20) and "Right to object and automated individual decision-making" (Articles 21 – 22).[359]

Briefly, Article 15 provides the data subject with the right to access their personal data, and thereby receive confirmation from the controller whether their personal data is being processed.[360] If the data subject's data is being processed, he or she is also entitled to receive the following information:

(a) the reason for the processing;

(b) the category of personal information being processed;

(c) who will and why they will obtain the personal data;[361]

(d) the time period that the personal data will be stored;

(e) the data subject may request that the controller rectify or erases the personal data or restricts the processing thereof;

(f) the data subject has the right to complain to the supervisory authority;

(g) where the personal data was sourced from, if not directly from the data subject; and,

(h) where an automated decision will be made, how the automated decision will be made, and any consequences of the automated decision making.

Article 16 provides for the right to rectify personal data without undue delay on the part of the controller. Article 17 provides for the right to be forgotten, and this will be discussed in the next section. The right to restrict processing is detailed in Article 18. It provides that the controller must restrict processing in the following instances:

(a) where the accuracy of the personal data is challenged;

[359] Articles 16 – 20 of the GDPR, Articles 10, 11, 12, and 14 of Directive 95/46, sections 17, 18, 23, 24, and 25 of the Protection of Personal Information Act 4 of 2013, discussed in Chapter 5, and OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013) paras 12 and 13.

[360] See *RW v Österreichische Post AG* EU:C:2023:3 para 28 onwards for a discussion and application of Article 15 of the GDPR, see also *FF v Österreichische Datenschutzbehörde* EU:C:2023:369 paras 34 – 35, 39 – 40, 45, and 53, where "information" in terms of Article 15 was interpreted to refer to the "personal data" of the data subject, and "the controller must provide a copy" of the personal data that they have of the data subject, subject to the relevant request made by the data subject, *JM* EU:C:2023:501 pars 50 – 59, and paras 64 – 66 regarding the importance of transparency towards the data subject, *FT v DW* EU:C:2023:811 paras 50 – 52, and 79 where it was held that a data subject is to be provided one free copy of the data that is being processed, as it is essential for transparency and confirming the accuracy of the personal data being processed.

[361] *RW v Österreichische Post AG* EU:C:2023:3 paras 43, 46 – 47, note also Recital 4 of the GDPR.

(b) in terms of unlawful processing, including the objection to erasure;[362]

(c) where the personal data is no longer needed by the controller; and,

(d) if the data subject has objected to the legitimacy of the processing, and this needs to be verified.

Regarding the phrase "objection to erasure": the term "erasure" is not defined in the GDPR.[363] However, the data subject may object to erasure and request the retention of the information rather or access thereto be restricted instead. The data subject may need legal proof that the specific processing request was carried out, eg applications for a licence or payment of a fee.[364] De Hert *et al* suggest that the reason for the objection to the erasure may be more to regulate the right to data portability (ie the data subject may transfer their data from one controller to another) rather than regulating the right to be forgotten (or erasure)).[365]

Article 19 provides that the data subject must be notified when their personal data is rectified, erased, or the processing thereof has been restricted.[366] According to Hoofnagle *et al* restricting the process of personal data is a new concept.[367] In Article 19, "restriction of processing" means "the marking of stored personal data with the aim of limiting their processing in the future". Restricting the processing of personal data may involve pausing any further processing activities until issues such as the "fairness and lawfulness of a processing activity" have been examined and answered. It may also involve pausing any further processing activities due to inaccuracies, etc.[368] Article 20 provides for data portability, which provides that personal data, at the request of the data subject, may be transmitted, without obstruction, from one controller to another.[369]

---

[362] *UZ v Bundesrepublik Deutschland* EU:C:2023:373 para 51.

[363] A Bunn 'Children and the "right to be forgotten": What the right to erasure means for European children, and why Australian children should be afforded a similar right' (2019) 170(1) *Media International Australia* 37 at 38 – 39.

[364] C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 140.

[365] P De Hert, V Papakonstantinou, G Malgieri, L Beslay & I Sanchez 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34(2) *Computer Law & Security Review* 193 at 198.

[366] *RW v Österreichische Post AG* EU:C:2023:3 para 40.

[367] C Hoofnagle, B Van der Sloot & F Zuiderveen Borgesius 'The European Union General Data Protection Regulation: What it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65 at 89.

[368] C Hoofnagle, B Van der Sloot & F Zuiderveen Borgesius 'The European Union General Data Protection Regulation: What it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65 at 89 – 90.

[369] See *X, Z v Autoriteit Persoonsgegevens* EU:C:2022:216 para 31. See also M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 at 7 – 14.

In terms of Article 21, the data subject may object to the processing of personal data, where the processing is in terms of Article 6(1)*(e)* and *(f)*, based on their personal circumstances.[370] Following such an objection, the personal data of the objecting data subject may be processed only where the controller presents legitimate reasons that override the objecting data subject's interests. The data subject, in terms of Article 22, may not be subjected to solely automated decisions, "including profiling, which produce legal effects concerning him or her or which similarly significantly affects him or her".[371] The process used for automated decision-making must be outlined to the data subject.[372]

(e) The right to be forgotten

Given its significance for this thesis, Article 17 is discussed alone. Article 17 is titled "Right to erasure (right to be forgotten)". This article is particularly significant for the right to be forgotten because it was adopted following the judgment of the CJEU in *Google Spain*[373] and is the very first legislative provision in which the right to be forgotten was expressed within the EU.[374] Article 17 reads as follows:

> "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> *(a)* the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;[375]
>
> *(b)* the data subject withdraws consent on which the processing is based according to point

[370] Article 6(1)*(e)* provides for processing of personal data where this is in the public interest or where the controller has been vested with official authority. Article 6(1)*(f)* provides for processing where this is in pursuance of a controller or third party's legitimate interest. For both of these sub-articles, the rights of the controllers or third parties must be balanced with the rights and freedoms of the data subject, especially where the personal data belongs to a child.

[371] Article 22 of the GDPR.

[372] D Elgesem 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 at 285.

[373] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 paras 50 – 51, and *Hurbain v Belgium* [2023] ECHR 948 para 70.

[374] AM Bobadilla 'Digital rights in Europe after the entry into force of regulations for the protection of personal data: Before and after the right to be forgotten' (2023) 28(4) *Communication Law and Policy* 313 at 331.

[375] Opinion of Advocate General Rantos in *Meta Platforms Ireland Inc., formerly Facebook Inc., & others v Bundeskartellamt* (Case C-252/21) EU:C:2022:704, delivered on 20 September 2022, compare with the Opinion of Advocate General Campos Sánchez-Bordona in *UI v Österreichische Post AG* (C-300/21) EU:C:2022:756, delivered on 6 October 2022. For a discussion on the two opinions, see M Nettesheim 'Digital autonomy in contractual relationships: On the relationship between contractual autonomy and control over data' *VerfBlog*, 18 October 2022.

(a) of Article 6(1), or point *(a)* of Article 9(2), and where there is no other legal ground for the processing;[376]

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);[377]

(d) the personal data have been unlawfully processed;[378]

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

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).[379]

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.[380]

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points *(h)* and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims."

---

[376] *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 paras 66 – 67, and *Meta Platforms Inc. & others v Bundeskartellamt* EU:C:2023:537 paras 74 – 85.
[377] Article 21 of the GDPR is titled the "Right to object" and replaces Article 14 of Directive 95/46, see *GC & others v CNIL* EU:C:2019:773 para 55.
[378] *UZ v Bundesrepublik Deutschland* EU:C:2023:373 para 50.
[379] See *GC & others v CNIL* EU:C:2019:773 para 55.
[380] *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 paras 91 – 99. See F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 931.

Based on Article 17(1), the EDPB summarised the instances where data may be erased (or forgotten)[381] and provided guidelines that elaborate further on these listed grounds, amplifying each and providing examples for each instance and their application.[382] The guidelines note that processing remains necessary in terms of freedom of expression and information, in terms of a legal obligation, in the interest of the public for public health, to archive information for historical, research and statistical purposes, and lastly, for the development of a legal defence.[383]

The guidelines provide useful criteria to keep in mind when balancing the various competing rights between all the parties that are involved, especially between the data subject and general internet users.[384] The EDPB has listed the "classic criteria" within the guidelines, and these are as follows (paraphrased):[385]

> "he or she does not play a role in public life . . . the information at stake is not related to his or her professional life but affects his or her privacy . . . the information constitutes hate speech,

[381] "Erasure" is not defined in the GDPR, see A Bunn 'Children and the "right to be forgotten": What the right to erasure means for European children, and why Australian children should be afforded a similar right' (2019) 170(1) *Media International Australia* 37 at 38 – 39. However, in the European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 at 4 (para 4) the EDPB states: "this document aims to interpret the Right to be Forgotten in the search engines cases in light of the provisions of Article 17 GDPR (the 'Right to request delisting')." Later in these guidelines the EDPB at page 5 (para 6) emphatically states that the guidelines will focus on what the controllers must do when receiving a de-listing request in terms of Article 17(1) of the GDPR. Furthermore, at page 5 of the guidelines (para 9) the EDPB states: "Delisting requests do not result in the personal data being completely erased. Indeed, the personal data will neither be erased from the source website nor from the index and cache of the search engine provider". Important to note is that the information is still available on the website of the controller, and thus accessible to internet users, with the use of alternative search terms. The EDPB further (at 5, para 10) notes that in

> "exceptional cases, they will need to carry out actual and full erasure in their indexes or caches. For example, in the event that search engine providers would stop respecting robots.txt requests implemented by the original publisher, they would actually have a duty to fully erase the URL to the content, as opposed to delist which is mainly based on data subject's name."

See also F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 931 – 933.

[382] See European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 at 6 – 11 – as a discussion of each is somewhat beyond the scope of this chapter – the important point to note is the right to be forgotten has been formalised and codified, and that the scope of the right has been defined, not only in the GDPR, but also through the cases. The cases will often determine the application within specific contexts – and each case is decided on its own facts. Note also the comments made in D Edros 'The "right to be forgotten" beyond the EU: An analysis of wider G20 regulatory action and potential next steps' (2021) 13(1) *Journal of Media Law* 1 – 35.

[383] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 at 13 – 16.

[384] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 paras 19, 30, 32, 45, 47, 50, 52, 62, 65, and 80. See also TS Cabral 'Forgetful AI: AI and the right to erasure under the GDPR' (2020) 6 *European Data Protection Law Review* 378 – 389.

[385] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 para 32.

slander, libel or similar offences in the area of expression against him or her pursuant to a court order . . . the data appears to be a verified fact but is factually inaccurate . . . the data relates to a relatively minor criminal offence that happened a long time ago and causes prejudice to the data subject."

The data subject's reasons for the erasure or the request to de-list or de-index are also important considerations in light of the balancing exercise between privacy and personality rights of the data subject, against freedom of expression and to impart and/or receive information of internet users.[386] The data subject must detail their personal circumstance as a part of the application to de-list, ie the right to be forgotten, to provide a background for the balancing exercise.[387]

Apart from the EDPB, the CJEU in *GC v CNIL*[388] took the opportunity to make a few observations on Article 17 of the GDPR, especially in comparison to *Google Spain's* right to be forgotten in terms of Directive 95/46:

(a) Article 17 of the GDPR, similarly to Articles 12*(b)* and 14*(a)* of Directive 95/46, requires that data be published only for as long as it is absolutely necessary,[389] and thereafter must be removed by the controller, without undue delay.[390]

(b) Article 17(3), expressly provides that the right to erasure cannot exclude necessary processing in terms of the right to freedom of expression and information.[391] In other words, the GDPR expressly requires that the balancing of the Charter rights of those pursuing a request for erasure, against the Charter rights of internet users' right to freedom of expression and information. Measures must be taken to guarantee all

[386] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 paras 19, 30, 32, 45, 47, 50, 52, 62, 65, and 80. In respect to the impact that the right to be forgotten has on artificial intelligence and machine learning see TS Cabral 'Forgetful AI: AI and the right to erasure under the GDPR' (2020) 6 *European Data Protection Law Review* 378 – 389.
[387] European Data Protection Board *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR* adopted 7 July 2020 para 32.
[388] *GC & others v CNIL* EU:C:2019:773, see also *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 48 – 50 and *Biancardi v Italy* [2021] ECHR 972 para 28.
[389] *GC & others v CNIL* EU:C:2019:773 para 54.
[390] *GC & others v CNIL* EU:C:2019:773 para 55. Note the request should be carried out within a month, see J Connolly 'The right to erasure: Comparative perspectives on an emerging privacy right' (2021) 46(1) *Alternative Law Journal* 58 at 62.
[391] *GC & others v CNIL* EU:C:2019:773 para 57. The right to freedom of expression and information is guaranteed in Article 11 of the Charter, and is also specifically mentioned in recital 4 of the GDPR. Recital 4 reads as follows:

> "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

Charter rights.[392]

(c) Furthermore, the protection of both the rights to privacy and personal data are not absolute,[393] and balanced against the right to freedom of expression and information,[394] specifically, the data subject's rights cannot automatically overrule the rights of the greater community to information.[395]

There are few points to note about Article 17, and its construction, namely, that two distinct rights, ie the right to erasure and the right to be forgotten, have been combined into one single Article.[396] Ausloos also explains that the duty is placed on controllers to inform third parties of erasure notices, where they, ie the controllers, have made such information public.[397] Ausloos later details that the title in its current form, ie "Right to erasure ('right to forgotten')", leads to confusion as to the precise meaning of the Article. He further opines that the legislators have left a "slogan" in the title with the use of quotation marks.[398] However, the right as a whole provides clarity and certainty on how it may be used to protect privacy, but also it will affect freedom of expression and information.[399]

Lastly, as stated above, the national supervisory authority has the power to request a controller, after the completion of an investigation, to take appropriate measures to rectify any "inadequacy" in the protection of a data subject's personal data.[400] The CJEU held that the rectification may include ordering the controller to, in light of Article 17(1), read with Article 58(2) of the GDPR,[401] adopt appropriate measures to correct the "inadequacy". The CJEU held

---

[392] *GC & others v CNIL* EU:C:2019:773 paras 58 – 61. This balancing exercise is a necessary element in the enquiry. See also *TU, RE v Google Spain LLC* EU:C:2022:962. Note F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 391.

[393] Articles 7 and 8 of the Charter. See also *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791 para 120 – 122, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258 para 48.

[394] *GC & others v CNIL* EU:C:2019:773 para 57.

[395] *GC & others v CNIL* EU:C:2019:773. Article 52(1) of the Charter requires that any limitations imposed on any one of the Charter rights may only be in terms of a law of general limitation, respecting the essence of those rights, and limiting the right only as far as necessary in the circumstances (ie the principle of proportionality) – *GC & others v CNIL* EU:C:2019:773 para 58, and see also *Volker und Markus Schecke GbR & Eifert v Land Hessen* EU:C:2010:662 para 50.

[396] J Ausloos *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018 at 84.

[397] J Ausloos *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018 at 84.

[398] J Ausloos *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018 at 86 and 196 onwards.

[399] J Ausloos *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018 at 86 and 196 onwards.

[400] *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2024:239 para 34.

[401] Briefly, Article 58 of the GDPR provides for the various powers of the national supervisory authority with

that this includes ordering the controller to "erase unlawfully processed personal data" irrespective of whether the data subject has filed a request for erasure or not.[402] The CJEU held that where there is a large number of data subjects that have not asserted their rights under Article 17, because they are unaware of the processing, ie they have not received prior notice of the processing, should not be deprived of this protection, merely because they are unaware that their personal data is being processed.[403]

(f) Conclusion

The GDPR, in overview provides for the responsibilities of both controllers and processors of personal data (Chapter IV),[404] these linking to the articles discussed in terms of the principles. Article 25 is important to note, it requires the safeguarding of personal data "by default and by design", taking into account technological advancements, costs, nature of the data and any other risks (eg technological failures). Burri and Schär have argued that this has significantly increased the responsibilities placed on controllers and processors because they will need to prove that they have complied with the GDPR where a breach of one of the provisions impacts on the rights of the data subject.[405]

The GDPR also controls in which circumstances personal data is transferred to third

---

investigatory powers – to investigate where there has been a breach in the protection of personal data (Article 58(1). Where the investigation proves that there has been a breach, then the supervisory authority must order any corrective measures, as contained in Article 58(2). Article 58(3) provides the supervisory authority with various advisory and authorisation powers.

[402] *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2024:239 paras 42 and 46.

[403] *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2024:239 paras 44 – 45. The CJEU held that this remedy may apply irrespective from where the personal data was collected, ie personally from the data subject or from a third party – see paras 47 – 53.

[404] The CJEU in *UZ v Bundesrepublik Deutschland* EU:C:2023:373 para 63 emphasised there is a distinction between the "lawful processing of data" as required by Article 6 of the GDPR and the obligations of the controller. Merely because the controller has not met all of its obligations, as required in terms of Articles 26 – 30 will not mean that the data has been processed unlawfully, provided that the requirements provided in Articles 5 (data processing principles) and 6 (lawful processing of data) have been met. Hence, where the controller infringes their obligations as provided in Articles 26 – 30 of the GDPR will not amount to "'unlawful processing' of data within the meaning of" Articles 17 and 18, read with Articles 5 and 6 of the GDPR (paras 67 and 69).

[405] Apart from what is mentioned in the text, a complete discussion of the requirements set out in Article 25 of the GDPR is beyond the scope of the thesis. M Burri & R Schär 'The reform of the EU data protection framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 at 493 – 495, E Stiakakis, CK Georgiadis & A Andronoudi 'Users' perceptions about mobile security breaches' (2016) 14 *Information Systems and e-Business Management* 857 – 882, C Tikkinen-Piri, A Rohunen & J Markkula 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 at 142, and DL Donnelly *Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020) at 178 – 219.

countries or international organisations (Chapter V).[406] Further, the GDPR provides for the rights and responsibilities of the independent supervisory authority, as well as the EDPB (Chapter VI).[407] Further relevant provisions to note are those providing for co-operation between the Member States and the need to apply the GDPR consistently throughout the EU (Chapter VII), as well as the remedies, liabilities and penalties, should personal data be breached (Chapter VIII).[408]

The GDPR was designed to be easily, or speedily, integrated into the existing EU as well as national data protection legal frameworks. As pointed out in the beginning, the design not only emphasises but also encourages a consistent application throughout the EU when applying the GDPR. The consistent application of the GDPR will provide certainty in relation to the rights and responsibilities of all persons involved in data processing, including data subjects, controllers and processors, throughout the EU. In light of business confidence relations between the EU Member States, it is vital to avoid divergent approaches in applying the GDPR.[409] In line with the approach of consistency of implementation, the GDPR encourages that data must only be processed for the original reason for which it was provided, unless the processing is for historical, scientific or statistical research.[410]

IV TRANSITION BETWEEN DIRECTIVE 95/46 AND THE GDPR

(a) Introduction

Like any piece of new legislation, once the GDPR came into operation, the relationship between Directive 95/46 and the GDPR gave rise to complex and difficult transitional questions, especially insofar as the interpretation and application of the GDPR during the transitional period was concerned. The CJEU provided some guidance on how to manage the transition period. Although the CJEU dealt with these transitional issues in a number of cases among the most interesting are *Deutsche Post AG v Hauptzollamt Köln*[411] and *Data Protection*

[406] M Kędzior 'GDPR and beyond—A year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 506.
[407] See *ZS v Zweckverband "Kommunale Informationsverarbeitung Sachsen" KISA, Körperschaft desöffentlichen Rechts* EU:C:2023:81.
[408] M Kędzior 'GDPR and beyond—A year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 506. There are further provisions that deal with the implementation of the GDPR within the EU data protection law landscape (Chapter IX) and further final provisions (Chapter X).
[409] M Kędzior 'GDPR and beyond—a year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 507 – 509.
[410] M Kędzior 'GDPR and beyond—A year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 at 507 at 508.
[411] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26.

Commission v Facebook Ireland & Schrems.[412] What is common to both (and of those not specifically discussed) is that the request for a preliminary hearing was submitted to the CJEU under Directive 95/46, but the GDPR was passed before the actual hearing took place.[413] In each instance, the CJEU would answer the submitted preliminary question or questions by either applying both pieces of legislation or merely the one, depending on the circumstances of the case.[414]

(b) Deutsche Post AG v Hauptzollamt Köln

The brief facts of *Deutsche Post AG v Hauptzollamt Köln*[415] are as follows. The Hauptzollamt Köln[416] required the Deutsche Post[417] to provide them with the tax identification numbers and where the tax returns are filed of all natural persons, directly, or indirectly, involved in customs matters.[418] If the Deutsche Post failed to do so, the Hauptzollamt Köln threatened to withdraw its authorisation for the handling of customs matters. The Deutsche Post complained that the list was too large. Furthermore, those officials that are directly involved with customs matters were willing to share their tax identification numbers, but those who were indirectly or not at all involved were unwilling to share the information.[419] The issue was, whether, in terms of the applicable EU legislation, this tax information was necessary for the Deutsche Post to receive its clearance to manage customs matters.[420]

---

[412] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (referred to as *Schrems II*). See also P Nebbia 'The *Schrems* judgments: A silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336.

[413] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26, *Google LLC v Commission Nationale de l'Informatique et des Libertes (CNIL)* EU:C:2019:772, *Bundesverband eV v Planet49 GmbH* EU:C:2019:801, and *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*).

[414] Some of the cases will be explored and discussed in the next chapter, as their main topic was the right to be forgotten, ie, *GC & others v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773, *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772. However, the comments from the CJEU regarding the transition between Directive 95/46 and the GDPR will be discussed in this chapter. See also the comments of the CJEU regarding the need for uniformity within the EU where directives and regulations are interpreted by the courts in *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2023:2 para 54 and *UI v Österreichische Post AG* EU:C:2023:370 paras 29 and 48.

[415] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26.

[416] The Hauptzollamt Köln is the Main Customs Office in Cologne, Germany.

[417] The Deutsche Post is the German Postal Services.

[418] This included the advisory and supervisory boards, principal managers, managing directors, divisional heads, accounting managers, those in charge of customs matters, and all involved in customs matters.

[419] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 25 – 29.

[420] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 35 and 40. Para 30 sets out the question from the referring court as follows:

> "In those circumstances the Finanzgericht Düsseldorf (Finance Court, Düsseldorf) decided to stay proceedings and seek a preliminary ruling from the Court on the following question:
> "Is the second subparagraph of Article 24(1) of [Implementing Regulation 2015/2447] to be interpreted as meaning that this provision permits the customs authority to request the applicant to inform it of the tax identification numbers issued by the Federal Central Tax Office for the purpose of income tax

The CJEU firstly acknowledged that the question or issue was originally referred under Directive 95/46, but since the referral, the GDPR had come into operation. The issue, therefore, had to be answered in relation to both pieces of legislation.[421] The important point to note from this judgment is that the CJEU held that the tax identification numbers, and thereby the tax information of natural persons, amount to personal data. The CJEU held that the request must be limited to the personal tax data of those who control the management of the juristic person and those that manage or deal with the customs matters within that juristic person.[422] The CJEU re-iterated that the principles for the processing of personal data must be respected, as well as complied with in terms of both Directive 95/46 and the GDPR. And further, the personal tax data of each natural person is collected for a specified reason, and due to the nature of the data, the quality must be of a high standard.[423] Personal data must also be processed fairly and the data subject has a right to be informed where their personal data is transferred, in light of the

collection and the tax offices responsible for the income tax assessment of the members of the applicant's supervisory board, its managing directors, divisional heads, accounting managers, head of the customs department as well as those individuals responsible for customs matters and those dealing with customs matters employed by the applicant?""

In para 40, the CJEU clarified the question as follows:

> "By its question, the referring court seeks, in essence, to ascertain whether the second subparagraph of Article 24(1) of Implementing Regulation 2015/2447, read in the light of Directive 95/46 and Regulation 2016/679, must be interpreted as meaning that the customs authorities may require an applicant for AEO status to send to it the tax identification numbers, allocated for the purposes of collection of income tax, concerning the members of its supervisory board and its wage-earning employees who hold posts as directors, divisional heads, and accounting managers, with responsibility for customs matters, including those who are responsible for the management of customs matters and those in charge of dealing with such matters, as well as details of the tax offices responsible for the taxation of all those persons."

The relevant legislation is the Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code. The Commission Implementing Regulation (EU) No 2015/2447 was used to provide consistency in the implementation of the Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code. Article 24 for consistent implementation of Article 39 of the Code, the personal tax data of the those working in the customs unit of a juristic person will be required in the assessment for granting the status of an economic operator in light of customs matters.

[421] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 36 – 39.

[422] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 50 and 55 – 56. In *Bara & others v Preşedintele Casei Naţionale de Asigurări de Sănătate & others* EU:C:2015:638 para 29, and *Puškár v Finančné riaditeľstvo Slovenskej republiky & another* EU:C:2017:725 para 41 the CJEU held that tax identification numbers are personal data as they amount to identifiers, ie the tax identification number may be used to identify a natural person. Note also, *LB v Hungary* [2023] ECHR 239 where the ECtHR held that the disclosure of the home address on the internet of a tax defaulter does not meet the ultimate aim of the relevant legislation, ie the collection of the relevant taxes to ensure the economic well-being of the country. See also *Rechnungshof v Österreichischer Rundfunk & others* EU:C:2003:294 para 64, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy & Satamedia Oy* EU:C:2008:727 para 35, and *Huber v Bundesrepublik Deutschland* ECLI:EU:C:2008:724 para 43.

[423] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 53 – 58, Articles 6 and 7 of Directive 95/46, Articles 5 and 6 of the GDPR, *Rechnungshof v Österreichischer Rundfunk & others and two other cases* EU:C:2003:294 para 65, and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 71. See also *Rechnungshof v Österreichischer Rundfunk & others and two other cases* EU:C:2003:294 para 52, and *Schwarz v Stadt Bochum* EU:C:2013:670 para 26, which require that the right to a private life must be respected where personal data is processed.

employer's obligations, to the customs authorities for further processing.[424] The CJEU held that the collection of tax data:

(a) by the employer to ensure that the relevant income tax is deducted, and

(b) in compliance with the relevant legislation to ensure their authorised status to manage customs matters,

are legitimate grounds in terms of the data processing principles, and may only be processed for those specified reasons.[425] The CJEU emphasised that it is only the tax data of those mentioned in the relevant legislation that may be processed, bearing in mind that the processing thereof must be limited to achieve the required authorisation to manage customs matters.[426]

---

[424] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 para 59, Article 6 of Directive 95/46 and Article 5 of the GDPR. See also *Bara & others v Președintele Casei Naționale de Asigurări de Sănătate & others* EU:C:2015:638 para 34.

[425] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 60 – 61.

[426] *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26 paras 65 – 66. Compare with the approach of the ECtHR in *LB v Hungary* [2021] ECHR 2 (Fourth Section) where the tax authority published the data subject's name and home address on a list of tax defaulters – here the majority concluded that the information appears in Hungarian, it will only attract a small group of interested readers and not a global audience, and it will only attract and be available to those readers that are genuinely interested in the information, and was thus reasonable in the circumstances (para 68). In the dissenting opinion of Ravarani J and Schukking J. The judges found that the publication of the home address is unnecessary to achieve the aim of the legislation, further coupled that information published on the internet is never truly private, is easily replicated by third persons and distributed, the possible consequences may amount to the data subject becoming a victim of crime, ie theft. An appeal was noted in *LB v Hungary* and the decision came before the Grand Chamber, ie *LB v Hungary* [2023] ECHR 239, which handed down judgment on 9 March 2023. The majority in the Grand Chamber agreed with the dissenting opinion of the Fourth Section, ie that it was not necessary for the government to include on the list of tax defaulters the home address of the data subject. The majority provided a set of factors that authorities (irrespective of whether they are in the executive, legislature, or judiciary) need to consider where legislation will impact on the personal data and thus the privacy (ie the private life – Article 8 of the Convention) of a data subject, these are set out in para 128, namely:

> "(i) the public interest in dissemination of the information in question . . . but also to (ii) the nature of the disclosed information . . . (iii) the repercussions on and risk of harm to the enjoyment of private life of the persons concerned . . . (iv) the potential reach of the medium used for the dissemination of the information, in particular, that of the Internet . . . and also to (v) basic data protection principles including those on purpose limitation, storage limitation, data minimisation and data accuracy . . . In this connection, the existence of procedural safeguards may also play an important role".

The court applied these principles and held that the Hungarian Government had not struck a proper balance between all the competing rights and had completely ignored the potential repercussions that a data subject may suffer where their home address is freely available on the internet. The court mentioned that the unaltered re-publication of the personal information means that the home address is published to a wider audience than was originally attended, and the potential to misuse this information by the public is great. The majority further held that the publication of the home address, although ensuring that the information was accurate, was not necessary for the aim of the government which was the "collection of relevant personal data in the interests of the economic well-being of the country" (see paras 136 – 140). In the Grand Chamber Kūris J drafted a concurring opinion; Serghides J partly concurred and partly dissented with the majority; and Wojtyczek J and Paczolay J wrote a dissenting opinion against the majority's judgment. Kūris J concurred with the majority and added that the government had not only failed to strike a fair balance between all the respective rights as to whether it was necessary to publish the home address of the data subject, but that the publication of the home address did not serve a "legitimate interest or any legitimate aim" (see para 27 of Kūris J's opinion). Serghides J agreed with the overall discussion that the Hungarian government had failed to strike a fair balance between the rights of the respective parties. However, Serghides J stated that first, the impugned legislation failed to provide the data subject

(c) Data Protection Commission v Facebook Ireland & Schrems

In *Data Protection Commission v Facebook Ireland & Schrems*,[427] also referred to as *Schrems II*, Mr Maximillian Schrems, was a law student from Austria, and also a Facebook user since 2008. Mr Schrems's complaint was that Facebook Ireland would transfer some or all of his data to Facebook Inc., United States (US), where it was processed. The essence of the complaint, with the Data Protection Commissioner of Ireland, was that the US laws do not offer adequate protection where personal data is processed. Mr Schrems requested a suspension or prohibition against the transfer of his personal data to the US.[428] Mr Schrems was challenging the so-called EU-US Privacy Shield; however, the complete argument is beyond the scope of this chapter.[429]

With regards to the applicable law, the CJEU held that the complaint originated before the repeal of Directive 95/46 by the GDPR, effective from 25 May 2018. By this date, the Irish Data Protection Commissioner had not made a final decision on Mr Schrems's complaint. It is in the absence of that final decision, which will require that the preliminary ruling be answered

with the ability to consent to the disclosure of his personal data on the internet (paras 4 – 8 of Serghides J's opinion). Secondly, the majority failed to consider impugned legislation failed to provide the Hungarian courts with a proportionality test to allow them to determine the balance to be struck between the rights and interests of the parties, and thus not providing for this vital test in the legislation breached the right to privacy (see paras 9 – 13 of Serghides J's opinion). Wojtyczek J's and Paczolay J's dissent was as follows: (1) the tax authority published the information based on a factual enquiry, and not in light of considerations that required the balancing of competing rights. According to Wojtyczek J and Paczolay J it would be unreasonable to require the tax authority to balance the competing rights of the various parties. The publication of the list of tax defaulters, which included personal data, was a general measure used to deter tax defaulters from committing tax fraud, evasion of paying tax, etc. (2) The nature of the information and the publication thereof "did not affect an important aspect of the" data subject's identity, existence, or their privacy generally. (3) The legislation had certain safeguards in place before such information may be published (these included the amount of tax outstanding and time that the amount had been outstanding for around 180 days, etc.). (4) The inclusion of the home address ensured the accuracy of the information published and who the actual defaulter was. The data subject's tax number was not revealed, as this was considered, due to the nature thereof to amount to sensitive information. The publication of at least the home address, or some other personal data, prevented the defaulting taxpayer (ie data subject) from enjoying anonymity for evading his duty to pay the required tax. (5) The publication of the personal data was temporary, once the outstanding amount was paid, the data subject's name would be removed from the list of tax defaulters (see paras 25 – 33 of Wojtyczek J's and Paczolay J's dissenting opinion). See also R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 271 – 273.

[427] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (referred to as *Schrems II*). See also P Nebbia 'The *Schrems* judgments: A silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336.

[428] In *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*) had successfully challenged the EU-US Privacy Shield Decision, ie Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S.

[429] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. See the discussion in the footnote regarding the transfer of data in '(d) Conclusion' under the discussion of Directive 95/46.

in light of the GDPR, instead of Directive 95/46, as Directive 95/46 was no longer in force.[430] Furthermore, emphasis was placed on the need for the consistent application of the EU-US Privacy Shield in light of the current data protection principles in the GDPR.[431] The CJEU examined the EU-US Privacy Shield in light of the data protection principles set out in the GDPR, and held that the transfer of personal data to a third country may only be undertaken where the level of protection of personal data is fundamentally equal to that of the EU, especially where the protection of human rights are concerned.[432] After examining, the relevant legal principles, the CJEU held that the US legal provisions do not provide the fundamentally equal safeguards as under the GDPR in the protection of the fundamental rights against unauthorised access by the US State authorities, where personal data is processed.[433]

(d) Conclusion

Depending on the particular circumstances of the matter before the CJEU, as shown by the two cases discussed, it may be necessary, as in *Deutsche Post AG v Hauptzollamt Köln* to decide the case using both Directive 95/46, especially, where the referring question was framed under Directive 95/46, and the need for those instances to provide guidance under the GDPR, will require that both pieces of legislation be used. However, *Data Protection Commission v Facebook Ireland & Schrems* show that there will be instances in which only the GDPR will be used, this is possibly best explained as the need for consistent application of the applicable principles, whereas, under Directive 95/46, there were inconsistencies amongst the Member States.

V CONCLUSION

Both Directive 95/46 and the GDPR have set a solid background against which the right to be forgotten operates in light of the processing principles for personal data. Both Directive 95/46 and the GDPR were designed to meet the need to protect personal data, as it was commonly

[430] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*) paras 77 – 79. Compare with *Google LLC v Commission Nationale de l'Informatique et des Libertes (CNIL)* EU:C:2019:772, *Bundesverband eV v Planet49 GmbH* EU:C:2019:801.
[431] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*) paras 8 (quoting Recital 10), 21, 48 and 101.
[432] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*) paras 90 – 105. Specifically, the CJEU held that the rights of natural persons must have the similar meaning and scope in their protection that corresponds to those of the Charter of Fundamental Rights of the European Union, see *Åklagaren v Åkerberg Fransson* EU:C:2013:105 para 44, and *Menci v Procura della Repubblica* EU:C:2018:197 paras 22 and 24.
[433] *Data Protection Commission v Facebook Ireland & Schrems* EU:C:2020:559 (or *Schrems II*) para 105.

collected and stored at the time of the enactment of the legislation. Although, the essence of the principles have not changed between Directive 95/46 and the GDPR, the principles were certainly updated to meet the demands to protect personal data in a technologically driven world, since the distribution of information merely happens at the click of a mouse, and the collection of data or information, whether generally or of a personal nature, is made easier with the use of search engines. Apart from the cases discussed in this chapter, the next chapter focusses on the protection of personal data, in light of the right to be forgotten, and how this has been achieved with the use of the legislative instruments.

CHAPTER 3

GOOGLE SPAIN AND THE RIGHT TO BE FORGOTTEN

I INTRODUCTION

> "Nothing fixes a thing so intensely in memory as the wish to forget it."[434]

How easily do individuals wish to forget a bad experience? Maybe it's something that one never wants to remember again. Often these memories lead to the funniest stories. Human memory does fade, and bad experiences are often forgotten as time moves on. The idea of forgetting, or erasing a bad memory straight away, is often rather appealing, especially where these may be found in recordings (video or written). Forgetting bad memories is a vital part of developing our self-image.[435] Forgetting assists individuals to control their identity and the development of their own self-image. Both remembering and forgetting are vital for individual self-growth.[436] Put differently, forgetting allows us to develop and share our own unique stories, shielding deeply personal information, and conveying those highlights that have left the most lasting impression on our own lives.[437]

As much as human memory may fail[438] – the internet does not forget. Even before the leading case of *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (*Google*

---

[434] The quote is from Michel de Montaigne as quoted in EF Villaronga, P Kiesberg & T Li 'Humans forget, machines remember: Artificial Intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304. See also J Ausloos 'The 'right to be forgotten' – Worth remembering?' (2012) 28 *Computer Law & Security Review* 143 – 152, M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 196 and CM Wulff 'The right to be forgotten in Post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 256 – 258.

[435] Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 468 – 473.

[436] Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 470 – 471.

[437] Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 472.

[438] Where a person is unable to forget the smallest details of their lives, including what they ate on a specific day, is known as "hyperthymesia" or "hyperthymestic syndrome" and may be described as follows

> "[it is] based on the Greek word thymesis which means 'remembering,' and hyper meaning 'more than normal.' The two defining features of hyperthymesia are: 1) the person spends an abnormally large amount of time thinking about his or her personal past, and 2) the person has an extraordinary capacity to recall specific events from their personal past. Thus, hyperthymesia differs from superior memory which refers to the supranormal ability to acquire and recall new information but not autobiographical information."

See ES Parker, L Cahill & JL McGaugh 'A case of unusual autobiographical remembering' (2006) 12 *Neurocase* 35 at 47, see also BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 231 and 252 – 253, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 470 – 471.

Spain),[439] the so-called right to be forgotten addressed "an urgent problem of the digital age".[440] This problem involves the fact that there is often no escaping what has been placed on the internet – namely every photo, comment, status update, even tweets on Twitter (now X), live forever in a cloud.[441] The "digital footprints" (data created by individuals themselves)[442] and "digital shadows" (data created about individuals by others)[443] are often relentless. In most instances, there is almost no way of escaping them, and in certain instances they cause more harm than good, depending on the circumstances of each data subject.[444]

The internet's eternal memory of human life may lead to information being taken out of context and used against an individual.[445] The idea of the right to be forgotten is designed to counteract the eternal memory of the internet and de-commodify personal data.[446] Counteracting the eternal memory of the internet and de-commodifying personal data, in certain circumstances, have the potential to tip the balance in favour of privacy over freedom of expression.[447] The right to be forgotten is an answer, or solution, to obtain a clean slate, and start again.[448] The basic definition of the right to be forgotten is:[449]

---

[439] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[440] J Rosen 'Symposium issue: The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88; G Sartor 'The right to be forgotten: Balancing interests in the flux of time' (2016) 24 *International Journal of Law and Information Technology* 72 at 76; MJ Kelly & D Satola 'The right to be forgotten' (2017) 1 *University of Illinois Law Review* 1 at 4.
[441] J Rosen 'Symposium issue: The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88. See also D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 762.
[442] BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 230 – 231.
[443] BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 230 – 231, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 482.
[444] BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 251 – 252. See also J Rosen 'The web means the end of forgetting' *New York Times Magazine*, dated 21 July 2010, *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022). See also J Rosen 'Free speech, privacy, and the web that never forgets' (2011) 9 *Journal on Telecommunications & High Technology Law* 345 – 356, and M Crockett 'The Internet (Never) Forgets' (2017) 19 *SMU Science and Technology Law Review* 151 – 181.
[445] Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018).
[446] G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303, M Botes, A Olckers & M Labuschaigne 'Data commercialisation in the South African health care context' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 36, Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479, DW Woods & R Böhme 'The commodification of consent' (2022) 115 *Computers & Security* 102605 1 – 12 and LJ Hoffmann 'Commodification beyond data: Regulating the separation of information from noise' (2023) 2 *European Law Open* 424 – 433.
[447] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[448] BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 250 – 252.
[449] MJ Kelly & D Satola 'The right to be forgotten' (2017) 1 *University of Illinois Law Review* 1 at 3. Compare with S Chandok & L Manocha 'Right to be forgotten: A step forward in the implementation of privacy laws in India' (2018) 6 *Supremo Amicus* 445 – 457.

> "the right of an individual to erase, limit, or alter past records that can be misleading, redundant, anachronistic, embarrassing, or contain irrelevant data associated with the person, likely by name, so that those past records do not continue to impede present perceptions of that individual."

However, the right to be forgotten is not a completely new concept,[450] although, in recent times, it has become more important, especially in light of the explosion of information that is now available on the internet – whether it be news platforms or social media web pages.[451] The idea of forgetting past human behaviour has been a part of society's fabric in other forms.[452] First, the expungement of criminal records after the effluxion/passage of time or reasonable amount of time has passed, allowing convicted persons to reintegrate and rehabilitate fully into society, without a criminal misdemeanour being held against them, especially where they have served their sentence and lived crime-free for a number of years, is arguably the oldest form that the right to be forgotten has taken.[453] This idea of rehabilitating criminals – especially in Europe – can be said to find its origins in the French law "*le droit à l'oubli* — or the 'right of oblivion'".[454] Similarly, insolvents are automatically able to rehabilitate themselves once the necessary time period has lapsed.[455]

Secondly, the news is seen as a "perishable commodity" – what may be the main headlines this week will no longer captivate the interests of society the next day or next week or next month. These headlines may be in print form (ie newspapers or journals), on television,

---

[450] G Sartor 'The right to be forgotten: Balancing interests in the flux of time' (2016) 24 *International Journal of Law and Information Technology* 72 at 75.

[451] Also referred to as social networking sites. MJ Kelly & D Satola 'The right to be forgotten' (2017) 1 *University of Illinois Law Review* 1 at 4; NNG de Andrade 'Oblivion: The right to be different … from oneself: Reproposing the right to be forgotten' (February 2012) 13 *IDP* 122 at 127 – 128

[452] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015).

[453] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 4; Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018). With regards to South African law, this procedure is governed by sections 271A – 271D of the Criminal Procedure Act 51 of 1977; D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 765. See BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I, Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) and *Biancardi v Italy* [2021] ECHR 972.

[454] J Rosen 'Symposium issue: The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88.

[455] BJ Koops 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 at 250 – 252, NNG de Andrade 'Oblivion: The right to be different … from oneself: Reproposing the right to be forgotten' (February 2012) 13 *IDP. Revista de Internet, Derecho y Política* 122 at 133, D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 765 fn28, E Carava, 'Personal data kept in companies registers: The denial of the right to be forgotten' (2017) 3 *European Data Protection Law Review* 287 at 291 – 292, see also *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014: 317, and *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197.

or, in some cases, in a blog post.[456] As such the headlines and those individuals that have made the headlines will most likely not be remembered, unless they are a public person, such as an actor, singer, or where the event has left an indelible mark on human history.[457] It was along these lines, a news article about a past insolvency that brought the right to be forgotten into the limelight.

This chapter delves into the jurisprudence surrounding the right to be forgotten, with a particular emphasis on its application in Europe.[458] This will include how the courts have applied the right, not only in *Google Spain*, but also in subsequent decisions. The focus of the chapter is to provide an overall understanding of the concepts, along with their definition and application, in light of the facts and circumstances of each case. Europe, especially the EU is one of the major global market force. Hence, the GDPR[459] has become highly influential due to the EU's regulations being tied to its market dominance.[460] The Court of Justice of the European Union (the CJEU) also holds both state and private organisations accountable to the provisions of the data protection laws,[461] ensuring that the data subject's human rights are protected during the processing activities.[462]

The outline for this chapter is as follows: *Google Spain* and how the right to be forgotten was defined and applied by the CJEU, followed by academic commentary on *Google Spain*, as well as the further development of the right to be forgotten in subsequent case law.

II GOOGLE SPAIN AND THE RIGHT TO BE FORGOTTEN HITS THE LIMELIGHT

Google Spain,[463] the landmark decision of the CJEU, caused quite a stir when the case was

[456] AP Hurter & MG Van Buer 'The newspaper production/distribution problem' (1996) 17(1) *Journal of Business Logistics* 85 at 85 – 86 where the authors define newspapers as a perishable commodity.
[457] Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression* (2015) at 4 – 5.
[458] The jurisdictions include, the European Regional Courts (ie the Court of Justice of the European Union and the European Court of Human Rights), the highest appeal courts of the individual European States, including the United Kingdom. See generally the commentary by A O'Neill 'BREXIT, democracy and the rule of law' (2020) *European Law Journal* 1 – 46.
[459] Previously Directive 95/46.
[460] G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 465 – 466.
[461] In this instance, reference is made to both Directive 95/46 and the GDPR, generally.
[462] G Buttarelli 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 at 78, D Ayala 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 at 213 and 216, C Kuner 'The path to recognition of data protection in India: The role of the GDPR and international standards' (2021) 33 *National Law School of India Review* 69 at 70 – 72, and G Çapar 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 at 485.
[463] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See also *Biancardi v Italy*

handed down.[464] The following is a short overview of the facts and principles involved in the case, which focused on clarifying the extent of the right to be forgotten.

(a) Facts and issues raised

Mr Mario Costeja González, a Spanish national, lodged an application on 5 March 2010,[465] with the Agencia Española de Protección de Datos (AEPD),[466] requesting that Google (Google Spain SL and/or Google Inc.),[467] de-index, de-list or de-reference internet links to two legal notices that appeared on the results page, when his name was used as the search terms. The legal notices, dated 19 January 1998 and 9 March 1998, were published in a newspaper widely circulated in Catalonia called *La Vanguardia Ediciones SL* (*La Vanguardia*). The notices were for the auctioning of his house as a result of unpaid social security debts, which were settled. Mr González's request also included that *La Vanguardia* removes the unwanted notices from its website. *La Vanguardia*, in the process of digitising its archives, had included old news articles, classified information, legal notices, etc. and placed these on its website.

The AEPD granted the removal request against Google but not against *La Vanguardia*.

[2021] ECHR 972 paras 19 – 22 *Hurbain v Belgium* [2023] ECHR 948 para 71ffg. The following are case discussions on *Google Spain*: E Kelsey '*Google Spain SL and Google Inc v AEPD and Mario Costeja Gonzalez*: protection of personal data, freedom of information and the "right to be forgotten"' (2014) 4 *European Human Rights Law Review* 395-400, S Kulk & F Zuiderveen Borgesius '*Google Spain v. González*: Did the court forget about freedom of expression?' (2014) 5 *European Journal of Risk Regulation* 389 – 398, A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 120ffg, and OJ Gstrein, 'The judgment that will be forgotten: How the ECJ missed an opportunity in *Google vs CNIL* (C-507/17)', *VerfBlog*, 25 September 2019.

[464] Y Poullet 'Is the General Data Protection Regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 775, T Bertram, E Bursztein, S Caro *et al* 'Five years of the right to be forgotten' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*) (11 – 15 November 2019, London United Kingdom) 959 at 959 and 956, and OJ Gstrein 'Right to be forgotten: European data imperialism, national privilege, or universal human right?' (2020) 13(1) *Review of European Administrative Law* 125 at 125 – 126.

[465] Note, due to the nature of a directive and the implementation thereof within each individual Member State, each Member State was expected within 3 years of the date of commencement of Directive 95/46 to transpose and adapt it into their own legal systems – for a discussion on the implementation of directives, see Chapter 2. See F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, B Koritnik 'Discretion of the EU Member State when implementing the Data Protection Directive 95/46/EC' [2005] MurdochUeJlLaw 4, K McAuliffe 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 – 115, E Van Schagen 'More consistency and legal certainty in the private law acquis: A plea for better justification for the harmonization of private law' (2012) 19(1) *Maastricht Journal of European and Comparative Law* 37 – 62, and R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 – 244.

[466] The Spanish Data Protection Authority.

[467] "Google" will be used where both Google Inc. and Google Spain SL were referred to together in relation to the issue discussed by the CJEU, depending on the discussion and the findings of the CJEU, they may also be referred to separately for clarification. Google Inc is the parent company in the United States and Google Spain SL is the local subsidiary for the Spanish market. See *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 43.

La Vanguardia could not remove the notices since their publication was based on a court order, to advertise the auction, as a part of legal proceedings against Mr González. The AEPD argued that Google could remove the links to the notices on the results page when Mr González's name was typed into the search function, in order to no longer reflect the links. AEPD justified this conclusion on the ground that "operators of search engines [such as Google] are subject to data protection legislation [ie Directive 95/46] given that they carry out data processing for which they are responsible and act as intermediaries in the information society" and where the "locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense".[468] However, there was no need to erase the data or have the data completely removed from the website, especially where the data was retained due to legal or statutory processes.[469]

Google Spain SL as well as Google Inc. brought separate applications or actions against the AEPD before the Audiencia Nacional (the Spanish National High Court). The Audiencia Nacional amalgamated the actions and decided to stay the proceedings, in order to gain guidance from the CJEU.

The issue before the CJEU was whether search engines owe individuals an obligation to protect their personal data. The rationale was based on the fact that search engines process personal data[470] sourced from the content on third-party websites by indexing and then listing the data making it available indefinitely to internet users. The Audiencia Nacional was essentially asking the CJEU for guidance in interpreting Directive 95/46 in light of the current technology "which appeared after the directives" were published.[471]

This overarching issue was divided into three questions or issues with questions 1 and 2 having several sub-questions. Based on the answers to these questions the Audiencia Nacional would make its ruling. The most important questions for this thesis are 2(c), 2(d) and 3. Combined, these simply refer to whether search engines, where a request is made in terms of the relevant law, must "erase/forget" certain personal data about a person. Specifically, with regards to question 3, whether it is possible that data published in terms of a court order may

[468] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 17.
[469] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 17. Compare with BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and for a summary see *Hurbain v Belgium* [2023] ECHR 948 paras 127 – 130 in relation to archives.
[470] Article 2*(a)* of Directive 95/46 defines "personal data" 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 social identity".
[471] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 19.

be "forgotten".

In summary, these questions dealt with various aspects, including the scope and consequences, of forgetting information obtained on the internet, specifically the modification of search engine algorithms to exclude certain information from search results when a person's name is used as the search terms. Question 1 focused on the territorial jurisdiction of the right to be forgotten.[472] Questions 2(a) and 2(b) examined the responsibility and the role of search engine operators in data processing,[473] whereas questions 2(c) and (d) asked whether

[472] Question 1 in full reads as follows:

> "1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:
>
> (a) must it be considered that an "establishment", within the meaning of Article 4(1)*(a)* of Directive 95/46, exists when any one or more of the following circumstances arise:
>
> – when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,
>
> or
>
> – when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,
>
> or
>
> – when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?
>
> (b) Must Article 4(1)*(c)* of Directive 95/46 be interpreted as meaning that there is "use of equipment … situated on the territory of the said Member State":
>
> – when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,
>
> or
>
> – when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?
>
> (c) Is it possible to regard as a use of equipment, in the terms of Article 4(1)*(c)* of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?
>
> (d) Regardless of the answers to the foregoing questions and particularly in the event that the Court … considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present:
>
> must Directive 95/46 … be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of … Union citizens is possible?"

For a general discussion on algorithms and defining specific algorithms, in light of trade, and the implementation of the right to be forgotten, see R Seyfert 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1542 – 1558.

[473] Question 2(a) and (b) were phrased:

> "2. As regards the activity of search engines as providers of content in relation to Directive 95/46 …:
>
> (a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in

information may be forgotten generally.[474] Question 3 considered whether lawfully published information may be forgotten.[475]

Questions 1 and 2(a) and 2(b) will be dealt with briefly, as they set out the basis or background for questions 2(c) and 2(d) and 3. The CJEU did not address the questions in the sequence outlined in its judgment, but instead dealt with them in order of convenience with regards to the conclusions they drew. This discussion does not follow the CJEU's order in discussing the relevant issues as well as the format used to set out the necessary legal framework and facts.

(b) Legal framework

The Court Justice begins *Google Spain* by quoting the relevant recitals from the preamble and articles from Directive 95/46 in full,[476] only those provisions relevant to question 3 are set out in full for this discussion, as the focus is on the right to forget legally published information on the internet. As discussed in the previous chapter, Directive 95/46 was designed to protect the rights and freedoms of individuals (in this instance the focus is on natural persons).[477] The

---

Article 2*(b)* of Directive 95/46?

(b) If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described:
must Article 2*(d)* of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the "controller" of the personal data contained in the web pages that it indexes?"

[474] Questions 2(c) and (d) read:

"2. As regards the activity of search engines as providers of content in relation to Directive 95/46 …:
. . .

(c) In the event that the answer to the foregoing question is affirmative:
may the [AEPD], protecting the rights embodied in [Article] 12*(b)* and [subparagraph *(a)* of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d) In the event that the answer to the foregoing question is affirmative:
would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?"

[475] Question 3 was simply set out as follows:

"3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked:
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 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?"

[476] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 3 – 13.

[477] Individuals or natural persons are referred to throughout Directive 95/46 as well as *Google Spain* (and any other cases) as "data subjects" – there is no specific definition of "data subject" in Article 2, however in Article

particular right that is sought to be protected is the right to privacy "with respect to the processing of personal data, and removing obstacles for the free flow of such data".[478] The relevant provisions are recitals 10, and 25 of the Preamble and Articles 6, 7, 12, and 14.[479]

Recital 10 provides that there is a high level of protection when processing a data subject's personal data, specifically to ensure the protection of their fundamental rights and freedoms, and Recital 25 states that whoever is collecting the data subject's data to process, must notify the data subject about the processing of their personal information. In addition, Recital 25 also provides that a data subject may correct and object to the processing of their data.

Article 6 of Directive 95/46 sets out various principles for data quality and among the most important of these principles is that personal data is processed fairly and lawfully, is collected for a specified, explicit and legitimate purpose and is adequate and not excessive for the purpose for which it is collected. The data itself must also be adequate, relevant and not excessive with regards to the purpose for which it is collected, and only kept for as long as necessary.[480] Directive 95/46 specifies six grounds for the lawful processing of personal data. One of these is Article 7*(f)*, which specifically provides that personal data may be processed where it is necessary for the legitimate interests of the controller, or the legitimate interests of a third party to whom such data has been disclosed, unless it infringes "the interests [or] fundamental rights and freedoms of the data subject".

The "Right of access" is set out in Article 12. The relevant part of this Article states that[481]

> "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 …".

Article 14 deals with "The data subject's right to object" and the relevant part of this Article

---

2*(a)* the following is written "natural person ("data subject")", in light of the definition of "personal data".

[478] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 3.

[479] Although these provisions were discussed in Chapter 2, they are set out here for ease of reference, in light of the CJEU's discussions and conclusions reached in terms of the right to be forgotten.

[480] See Article 6 of Directive 95/46. Article 6 is discussed in the previous chapter in more detail. *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 7.

[481] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 10. Article 12 is found in Section V: The data subject's right to access data and is in Chapter II of Directive 95/46.

states that:[482]

> "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. . .".

Lastly, with respect to Spanish Law, the CJEU stated that Directive 95/46 "was transposed into Spanish Law by Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088)."[483]

(c) Jurisdiction and the responsibility of operators

The findings made by the CJEU in questions 1 (physical jurisdiction) and 2(a) and (b) (responsibility of operators) are important to note for questions 2(c) and (d) and 3. Question 1 dealt with the physical jurisdiction of Directive 95/46. The CJEU found that, although Google Spain SL, is a subsidiary of Google Inc. in the US, Google Spain SL is a controller in terms of Directive 95/46.[484] As a subsidiary of the main company, Google Spain SL's responsibility was to operate and "promote and sell advertising space" and orientate the services of the search engine company to that of the local Spanish market.[485] Hence, the CJEU held that the Spanish courts as well as the AEPD had the necessary authority in terms of jurisdiction to deal with the matter.[486]

Questions 2(a) and 2(b) dealt with the responsibilities that the operators owed to data subjects in terms of Directive 95/46.[487] The CJEU found that even though the processing of the

---

[482] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 11.
[483] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 13.
[484] Article 4(1)*(a)* of Directive 95/46; *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 45 – 61.
[485] This aspect is fully set out in *L'Oréal SA and others v eBay International AG and others* EU:C:2011:474 para 61ffg. See also A Esteve 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 at 39 – 40.
[486] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 45 – 61. See the analogy used in *L'Oréal SA and others v eBay International AG and others* EU:C:2011:474 paras 62 – 63.
[487] Article 2 sets out the definitions and the relevant ones are:

> "For the purposes of this Directive:
>
> . . .
>
> *(b)* "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

information in this case, namely indexing, storing and subsequently making it available to the public, happened automatically,[488] it did not mean that the operators had less responsibilities towards the data subjects. Merely displaying the information on a results page amounts to processing of data. Or, put differently, the mere fact that the search engine tool finds, orders and makes available data by arranging the links to the relevant data (including personal data) requested by an internet user on the results page,[489] amounts to the dissemination of data, which is included in the definition of data processing.[490] The processing of the data has an effect on the personal rights of the data subject.[491] In addition, the CJEU also found that because these processing activities are carried out by search engines, the operators of search engines must be considered as the "controller[s]" of data, as set out in Directive 95/46.[492]

(d) The scope of "the right to be forgotten"

(i) Generally forgetting information: Questions 2(c) and (d)

The CJEU held that the combined effect of Articles 12*(b)* and 14*(a)* of Directive 95/46 (ie the right to object, and the right to request a deletion) forms the right to be forgotten. Operators of search engines will be responsible, where a request is made, to remove links displayed on a results page, which leads to the data subject's personal information. The operator will need to adhere to the objection request even if the personal information is not erased on the third party's website.[493] The request must be based on a search done using the data subject's name.

. . .

(d) "controller" shall mean 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; . . ."

[488] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 133 – 135.

[489] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 26 – 28, 30 and 57. *Lindqvist* EU:C:2003:596 para 25 held that the uploading and displaying personal data on a webpage, whether done automatically or not, amounts to processing in terms of Articles 2*(b)* and 3(1) of Directive 95/46. See also *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* EU:C:2008:727 paras 48 – 49 and *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 para 20, and H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 558.

[490] See Articles 2*(b)* and 3(1) of Directive 95/46, and H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 558.

[491] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 58 and 66; see also *Rechnungshof v Österreichischer Rundfunk and others and two other cases* EU:C:2003:294 para 70; *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* EU:C:2009:293 para 47; and *IPI v Geoffrey Englebert and others* EU:C:2013:715 para 28. See *LB v Hungary* [2023] ECHR 239 para 47 where the court stated that all relevant rights need to be balanced.

[492] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 33.

[493] This will include lawfully published information, as discussed below.

The operators of search engines will often, through their automatic processing affect the data subject's fundamental rights and especially Article 7 (the right to a private life),[494] and Article 8 (the right to data protection),[495] of the Charter of Fundamental Rights of the European Union (Charter).[496] In terms of Article 12*(b)* of Directive 95/46, the data subject may request the controller to erase, rectify or block data processing – where the processing does not comply with the data quality principles or the legitimate processing principles set out in Articles 6 and 7 of Directive 95/46, respectively.[497] However, in some instances, data may be kept and further processed for historical, scientific or statistical purposes, but it will be up to the controller of data to either anonymize the data, depending on the circumstances, or to make sure that the data is as accurate and up-to-date and is processed only for the shortest period needed. The data should only be processed for the time period needed and for the reasons provided, otherwise it must be deleted or erased.[498]

One concern regarding the erasure of data is that the internet users' right to information may be infringed. The CJEU argued that search engines play a "decisive role in the dissemination of data".[499] The activity of search engines impacts especially on the Charter rights of privacy and data protection of individuals. The aim of Directive 95/46 is to protect and set out guidelines to provide for an "effective and complete protection of data subjects", especially the right to privacy of those data subjects.[500] The advantage of using a search engine is that it creates a structured overview of the data or information based on the search term

[494] Article 7 of the Charter of Fundamental Rights of the European Union states:
"Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications."
[495] Article 8 Charter of Fundamental Rights of the European Union reads as follows:
"Protection of personal data
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 to 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."
[496] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 68 – 69, see also *Bernard Connolly v European Commission* EU:C:2001:127 para 37 and *Rechnungshof v Österreichischer Rundfunk and others and two other cases* EU:C:2003:294 para 68.
[497] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 71 – 72, see also *Rechnungshof v Österreichischer Rundfunk and others and two other cases* EU:C:2003:294 para 65; *ASNEF and FECEMD v Administración del Estado* EU:C:2011:777 para 26 and *Worten v ACT* EU:C:2013:355 para 33.
[498] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 72. Comapre with *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 193 and 240 of Chaskalson AJ's judgment.
[499] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 36. P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627.
[500] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 38.

keywords.[501] The information is free, easily replicated and stored by internet users.[502] However, search engines also gain an economic advantage with the sale of personal data.[503] The CJEU weighed up the economic advantage of free data and the internet users' right to information[504] against the rights to a private life and data protection guaranteed in the Charter.[505] The CJEU held that, subject to the caveats set out hereafter, the right to privacy will generally override the right to economic gain and access to information.[506] The CJEU, however, added the following caveats:

(a) the right to economic gain and access to information may override the rights to a private life and data protection depending on the role of the person in public life, for example, if the data subject is a celebrity or politician. This is because the extent to which a data subject's privacy will be protected, depends on their integrity; on how they conduct themselves in private or have conducted themselves in the past.[507]

(b) the right to economic gain and access to information may override the rights to a private life and data protection depending on whether the information is published in light of legal proceedings or is legally required to be published.[508]

---

[501] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 80. See also *eDate Advertising GmbH v X, Martinez and another v MGN Limited* EU:C:2011:685 para 45.
[502] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 84.
[503] See the comments in Chapter 2 and G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479.
[504] Note, although not explicitly mentioned during the case, the right to freedom of expression and information is set out in Article 11 of the Charter. Article 52 of the Charter is titled "Scope and interpretation of rights and principles", and provides the mechanism for the balancing of competing rights and freedoms, important to note is the following:

> "1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

[505] Found in Articles 7 and 8, respectively, of the Charter. Note also the remarks in *LB v Hungary* [2023] ECHR 239 para 47.
[506] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 81 and 97. See also *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 para 165, H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 561 – 562, and S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 323 and 346. Note also the comments made by G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479.
[507] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 81 and *TU, RE v Google LLC* EU:C:2022:962 para 62. See also H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 561 – 562, and S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 323.
[508] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 80 – 81 and 99.

(ii) Can lawfully published information be forgotten?

Question 3 went a step further than questions 2(c) and 2(d) above. In terms of this question, the Audiencia Nacional asked the CJEU whether information that was published in terms of a relevant legal obligation at the time of publication may be removed.[509] This includes information published in terms of a legal obligation (ie a notice) and where that information is true, but is now offensive or prejudicial to the data subject. Put differently, the Audiencia Nacional asked the CJEU whether lawfully published information may simply be "forgotten" after the passage of time.[510] This discussion is important as the court set out the factors to be considered where personal data is published in terms of a lawful obligation.[511]

In a further discussion regarding Article 12*(b)* of Directive 95/46 the CJEU mentioned that the processing of personal data may, after the lapse of time, become incompatible with Directive 95/46. The reasons for this are that the data may be inaccurate, irrelevant and "excessive in relation to the purpose for processing thereof", the data may be outdated, or it may have been stored for longer than necessary, excluded is data required to be kept for historical, statistical or scientific purposes.[512] Based on the foregoing even lawful/legitimate accurate processing of data may over time become unlawful, or rather incompatible, with the objects of Directive 95/46.[513] This will be the case when the circumstances have changed, and the processing of the data is "inadequate, irrelevant or no longer relevant, or excessive in

[509] Article 7*(c)* of Directive 95/46 provides for the processing of personal information in terms of a legal obligation, it is likely that this includes both documents issued by the courts, as well as notices required in terms of relevant legislation, eg Articles 10 and 11 of Directive 95/46 requires that responsible parties must inform data subjects or all who will have access to the personal data collected by them and whether these will be processed further. See F Boehm & P de Hert 'Notification, an important safeguard against the improper use of surveillance - Finally recognized in case law and EU law' (2012) 3(3) *European Journal of Law and Technology*, and B Van Alsenoy 'Allocating responsibility among controllers, processors, and "everything in between": The definition of actors and roles in Directive 95/46/EC' (2012) 28 *Computer Law & Security Review* 25 at 30. Note, Directive 95/46 provides that in two of the six grounds, the data subject may object to the processing of their personal data, namely, Articles 7*(e)* and *(f)*, see Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 10.

[510] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 89.

[511] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 and Article 29 Data Protection Working Party *Update of Opinion 8/2010 on applicable law in light of the Court of Justice judgment in Google Spain*, adopted 16 December 2015. See also S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 339 – 341.

[512] Article 6(1)*(c)* to *(e)* of Directive 95/46; *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 72 and 90.

[513] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 93. See also H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 561.

relation to" its original purpose.[514] In such a case, the data appearing "in the list of results must be erased."[515] However, in the case of keeping registers, this is determined by the factors set out in Article 6(1)*(c)* to *(e)* of Directive 95/46. Where a request for erasure is made in terms of Articles 12*(b)* and 14*(a)* of Directive 96/46, the data must have been processed in accordance with Article 7*(f)*. [516] Article 7*(f)* of Directive 95/46 provides that personal data may be processed in terms of a lawful interest of the responsible party. The CJEU in deciding whether the request for erasure should be granted, pointed out that the reason for the processing of the personal data must be valid for the entire period that the data is being processed, especially where the data is processed for a lengthy continuous period. Taking into account the passage of time and the need to protect the fundamental rights and freedoms of the data subject, an important consideration is that the data may no longer reflect the current circumstances of the

[514] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 94. See also C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 551. In *CN v European Parliament* EU:T:2015:926, briefly, CN, the applicant, was an Official of the European Council. CN lodged a petition with the relevant committee regarding support to be granted to officials where they or their family members suffer from health-related issues. In terms of the relevant forms, CN ticked various boxes, which amongst others, provided for the publication of the petition and outcome on the European Parliament's website. The CJEU held that consent, even for the processing and publication of sensitive data, is one of the grounds for lawful processing, and thus does not impact adversely on the privacy of the data subject. The ticking of the relevant boxes amounted to providing their express consent. In this instance, although CN had requested that the data be removed from the website, which was done by the European Parliament, there had been a delay. The CJEU held that the delay was justifiable in the circumstances, because it had taken some time to locate the relevant initial records to successfully remove the data. Hence, there was no breach committed by the European Parliament against the applicant. Note (para 94), the court did cite *Google Spain*, however it pointed out the cases differ significantly, because in *Google Spain*, the applicant had not given his consent, whereas CN had. One can surmise that where the information is published electronically only, and there is no paper trial, then the information may be easily removed, where consent is withdrawn. Recently, in *TU, RE v Google LLC* EU:C:2022:962, the CJEU, based on similar arguments as in *Google Spain*, paved the way specifically for photos and thumbnails to be forgotten, ie to be de-listed or de-referenced, where these form a part of articles reporting on the activities of the data subject. The facts, briefly, TU and RE requested that three articles, that included photos (that Google used to display as thumbnails with the link to the original articles), contained inaccurate information. Google had refused to accede to the request. The CJEU provided guidance for courts and search engine operators where they receive requests for de-linking (the CJEU specifically referred to de-referencing) by stating that the data subjects must provide adequate proof for the courts or operators to assess and make the relevant decision, based on a balancing the relevant rights of the data subjects and the public. For a summary of *TU, RE v Google LLC* see OJ Gstrein 'The right to be forgotten in 2022: Luxembourg judges keep surfing the legislative void' *VerfBlog*, 20 December 2020, and *Hurbain v Belgium* [2023] ECHR 948 paras 86 – 87.

[515] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 94, using *Google Spain's* facts, the outstanding social security debts were then paid in full by Mr González over a period of time, and Mr González had been rehabilitated. Compare with *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197 where Mr Manni had waited for the relevant time period to elapse before applying for his information to be forgotten, ie that the information be de-linked from his name, where his name is used for an internet search. See also *LB v Hungary* [2023] ECHR 239 para 50.

[516] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 95. Article 7*(f)* states that personal data may only be processed where

> "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1)".

data subject.[517]

Based on the foregoing considerations, and in answering the specific issue in question 3, which was the de-linking/de-referencing legally published information, the CJEU held that the Audiencia Nacional will need to decide whether the information should still be available, balancing the public's right of access to the information and Mr González's right to privacy and data protection. The CJEU examined the facts placed before it by the Audiencia Nacional, and found that due to the passage of time since the initial processing of the data to the date of judgment, there seemed to be no reason as to why the links should not be removed, in light of a search conducted using Mr González's name as the search term.[518]

The CJEU concluded that the answer to question 3 is that Articles 12*(b)* and 14*(a)* of Directive 95/46 are to be interpreted to mean that where the information is to be forgotten or erased, a court is required, in terms of the facts of the matter before it, to balance the data subject's right to privacy and data protection and the public's right to freedom of information. The de-linking/erasure requests need only be made to the search engine, there is no need to make a simultaneous request to the third-party publisher to remove or anonymise the information.

Noting the arguments and the caveats above,[519] which will mean that not every circumstance will be covered by the right to be forgotten, this is amplified in the case discussion later in the chapter.[520]

---

[517] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 95 – 97. Unlawfully published data must be erased immediately, however, generally unlawfully published data is often on the dark web, where erasure is impossible, see generally Recital 55 of Directive 95/46, B Van Alsenoy 'Allocating responsibility among controllers, processors, and "everything in between": The definition of actors and roles in Directive 95/46/EC' (2012) 28 *Computer Law & Security Review* 25 at 29, M Cunningham 'Privacy law that does not protect privacy, forgetting the right to be forgotten' (2017) 65(3) *Buffalo Law Review* 495 at 530 – 532, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 460 – 461.

[518] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 98 – 99. See also *Google LLC v CNIL* EU:C:2019:772 para 44. Note also *Hurbain v Belgium* [2023] ECHR 948 paras 106 – 112, where the ECtHR discusses the Spanish Constitutional Court judgment of 4 June 2018 (no. 58/2018). At para 111 it was noted that where the information concerns past events, which do not impact on the present circumstances of the data subject, and these events do not add to the public debate, will most often lead to the information being de-linked or de-referenced (ie "forgotten"). See also BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and the summary of the German judgment in *Hurbain v Belgium* [2023] ECHR 948 paras 127 – 130 in relation to archives.

[519] Ie, the caveats are (1) is the data subject a prominent individual or do they have a role to play in public life, put differently, is the person an actor, a politician, etc.? (2) is the information required to be published in terms of legal proceedings?

[520] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 99. See also *NT1 & another v Google LLC & another* [2018] 3 All ER 581, where one of the applicants was unsuccessful in his erasure request, this judgment is discussed below. In *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197 the CJEU held that depending on the facts of each individual case, erasure may not be the only solution. In certain instances, it may be enough to merely block or limit access thereto. The

III WHAT THE ACADEMICS THOUGHT OF GOOGLE SPAIN

The CJEU and the European Court of Human Rights (ECtHR), together with the national courts within the European Union (EU), have developed the right to be forgotten in the context of both EU as well as national data protection legislation. The national courts, in particular, have interpreted the principle in *Google Spain* in terms of national constitutional instruments,[521] thereby incorporating the right into their national legal systems. But before turning to the case law that followed *Google Spain*, it may be interesting to note some brief remarks, both positive and critical, from the academic commentary.[522]

The first aspect to note is that the judges and the advocate general of *Google Spain* came to different conclusions.[523] Hijmans suggests that this is the main cause of controversy surrounding the judgment.[524] Sartor refers to this difference as "striking".[525] Very briefly, the advocate general, Jääskinen, had argued that search engines should not be equated to data controllers as defined in Directive 95/46, as they merely disseminate data. In terms of the eCommerce Directive 2000/31,[526] search engines are only intermediaries between the websites

information in this instance was kept in a register – and like the internet – the register provides all the relevant information in one convenient spot. The CJEU acknowledged that information provided in a professional capacity, ie for the registration of a company in the relevant companies register, will over time become personal. The court did not lay out any specific guidelines in calculating the time period as such, but did conclude that the EU Member States' national courts, based on the relevant national as well as EU law, and depending on the facts before it, must decide what will be the best solution in each individual case, based on the relevant legislation and the protection of rights and freedoms for all involved. *Manni* was discussed in *LB v Hungary* [2023] ECHR 239 para 50. See *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 paras 57 – 71 where a data subject requested, in terms of Article 17(1)*(b)* of the GDPR, that their information be removed from directories that were made available by the telecommunications company Proximus. See also E Carava 'Personal data kept in companies registers: The denial of the right to be forgotten' (2017) 3 *European Data Protection Law Review* 287 – 292.

[521] *NT1 & another v Google LLC & another* [2018] 3 All ER 581 and BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

[522] For more detail see generally, B van Alsenoy, A Kuczerawy & J Ausloos 'Search engines after *Google Spain*: Internet@Liberty or Privacy@Peril?' (6 September 2013). ICRI Working Paper Series: ICRI Research Paper 15, O Lynskey 'Control over personal data in a digital age: G*oogle Spain v AEPD and Mano Costeja Gonzalez*' (2015) 78 (3) *The Modern Law Review* 522 – 534, A Kuczerawy & J Ausloos 'From notice-and-takedown to notice-and-delist: Implementing *Google Spain*' (2015) 14(2) *Colorado Technology Law Journal* 219 – 257, J Powles 'The case that won't be forgotten' (2015) 47 *Loyola University Chicago Law Journal* 583 – 615, and GF Frosio 'The right to be forgotten: Much ado about nothing' (2017) 15 *Colorado Technology Law Journal* 307 – 336.

[523] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 558 and G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 546.

[524] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 558, EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 2 *European R 246.eview of Private Law* 241 at 246.

[525] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 546.

[526] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic

that host the information and the internet user that is looking for the information. Jääskinen, therefore argued that search engines play a passive role within the information society.[527]

Sartor agreed with the advocate general in respect of the above argument.[528] He argued that the eCommerce Directive 2000/31 has a "stable framework" with which to hold intermediaries responsible for data protection violations.[529] Sartor maintains that the approach of the CJEU misses the mark of a "stable framework", and brings about legal uncertainty.[530] According to Sartor, the eCommerce Directive 2000/31 provides the best solution as it distinguishes between content providers that make information available on the internet for indexing, and the functions of intermediaries who index that information. Sartor's argument points out that search engines are not responsible for the indexing of information, as that is the responsibility of the media houses or companies. Media houses index their articles with the requisite keywords.[531] The function of these keywords or index tags is to provide a summary of the information contained within the article. Search engines will use these keywords to further index the information within their own systems, making it easier to locate,[532] irrespective of whether the information within the articles contains personal information.[533] Based hereon, Sartor suggests that aggrieved data subjects must apply with the original

commerce).

[527] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12) EU:C:2013:424, delivered on 25 June 2013 paras 84 – 90, Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 at 14, H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 558 and G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 546.

[528] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 – 575.

[529] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 564 – 565.

[530] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 564 – 565.

[531] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 565 – 566. See generally DH Lee & T Schleyer 'Social tagging is no substitute for controlled indexing: A comparison of medical subject headings and CiteULike tags assigned to 231,388 papers' (2012) 63(9) *Journal of the American Society for Information Science and Technology* 1747at 1747

[532] Lee and Schleyer describe index tags, or as it also referred to as indexing, is the controlled process to assign terms or keywords to content in order to summarise or outline what is contained therein. Another general reference for these terms is "descriptive metadata". Information retrieval systems, ie search engines, use the assigned index tags to locate and display in a list (or index) information or data, based on the search terms used by the internet user. See DH Lee & T Schleyer 'Social tagging is no substitute for controlled indexing: A comparison of medical subject headings and CiteULike tags assigned to 231,388 papers' (2012) 63(9) *Journal of the American Society for Information Science and Technology* 1747at 1747.

[533] DH Lee & T Schleyer 'Social tagging is no substitute for controlled indexing: A comparison of medical subject headings and CiteULike tags assigned to 231,388 papers' (2012) 63(9) *Journal of the American Society for Information Science and Technology* 1747at 1747, and G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 565 – 566 and 568 – 570.

publisher to have the information de-indexed.[534] Hence, search engines fulfill the intermediary role and can only index the information that content providers allow to be indexed. Sartor further argues that when search engines are aware that the content providers are engaged in prohibited processing activities, only then should they be liable, in terms of criminal, civil or administrative law.[535]

The problem is, Sartor acknowledged, what happens when the data subject is unable to locate the original publisher?[536] To whom can the data subject then turn to protect their rights and freedoms? The CJEU has managed to find a middle road. Therefore, requiring search engines to de-index or de-reference links, provides the data subject with the necessary protection of their personal data, albeit only upon receiving the requisite application.[537]

Van Oyen *et al* pointed out that search engines are not equipped to make the decision of whose information should be forgotten and whose should not. The persons ultimately responsible for these decisions, search engine operators, have not been trained in the complexities of the balancing of rights, freedoms, and interests for each country's legal system.[538]

Wolf was very critical of the judgement and pointed out a few technical difficulties in relation to the implementation of the CJEU's decision in *Google Spain*.[539] One of the difficulties of the judgment is that it requires a non-EU company, which operates through subsidiaries that merely promote and sell advertising space and tailor their services to the local markets of the EU Member States in which they trade, to apply EU data protection legislation.[540] Peguera, was also critical of this aspect, and stated that due to the inextricably

---

[534] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 566

[535] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 570 – 574, compare with P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 626 – 628.

[536] G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 566.

[537] *GC & others v CNIL* EU:C:2019:773 para 78 and J Globocnik 'The right to be forgotten is taking shape: CJEU judgments in *GC and others* (C-136/17) and *Google v CNIL* (C-507/17)' (2020) 69(4) *GRUR International* 380 at 384. Note, as Hijmans emphasised that media houses or companies may claim the journalistic exemptions when processing data, including personal data. See H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 – 563.

[538] JS Van Oyen, M Lange & S Kreinsen, 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 at 306 – 307.

[539] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 – 554.

[540] The adverts that are seen by internet users are often based on the searches that the users conduct with use of the search engines, hence, the CJEU argued that. See *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 55, C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines

linked operations of Google Inc and Google Spain, it creates a problem as to who should appear on the de-linking request.[541] However, the data processing functions (these include indexing, uploading and storing data) are often performed in a non-EU State.[542] EU based regulators now have more control over the activities of non-EU companies.[543] This may lead to an impact on services and revenue generated by these companies in the long term, as well as what information is available to internet users, even in non-EU countries.[544] This affects the right to freedom of expression, discussed later in the thesis.

By expanding the territorial reach of the data protection legislation to non-EU based-companies (especially to web-based service providers), Wolf argues that these companies will need to rework their operational structures.[545] Where this becomes too complicated, these companies may either leave the EU altogether or find a Member State where the data protection laws are not as strictly applied. This has the potential to generally lower the level of protection of EU citizens where they choose to use these services.[546] Wolf noted that search engines have been inundated with de-linking requests.[547] He was also critical of the CJEU for not providing

---

and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 548 – 549. P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627, here De Hert and Papakonstantinou pointed out that Google was the preferred search engine of most Europeans, this was due to the accuracy with which their algorithms correlated as well as found information, which were connected to their marketing strategy – the authors commented that Google's "efficiency in the market was its demise in court".

[541] M Peguera 'In the aftermath of *Google Spain*: How the right to be forgotten is being shaped in Spain by courts and the Data Protection Authority' (2015) 23 *International Journal of Law and Information Technology* 325 at 341 – 343.

[542] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on Search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 549, D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 764 and C Kuner '*Google Spain* in the EU and international context' (2015) 22(1) *Maastricht Journal of Comparative and European Law* 158 at 159 – 161.

[543] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 547.

[544] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 552 – 553 and D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 764.

[545] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 552, G Sartor 'Search engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 at 566 and C Kuner '*Google Spain* in the EU and international context' (2015) 22(1) *Maastricht Journal of Comparative and European Law* 158 at 159 – 161. Compare with P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 628 – 631.

[546] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 552.

[547] C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 552 – 553 and H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 556.

substance to who is a "public figure"[548] and what the phrase "no longer relevant" means.[549] Hijmans agrees that legal certainty needs to be given to certain phrases, such as those referred to by Wolf, either by way of legislation or legal decisions.[550] However, in order to provide some form of legal certainty the Article 29 Data Protection Working Party (Article 29 WP) drafted guidelines to assist in the implementation of *Google Spain*.[551] These guidelines provide assistance in interpreting the mentioned phrases as well as how certain terms should be applied.[552] The guidelines, presented in a question and answer style, detail the common criteria that data authorities (as well as courts) need to consider when a search engines refuses to implement the right to be forgotten.[553] The application of these guidelines by the courts will be discussed below.

De Andrade[554] and McGoldrick[555] argue that the right to be forgotten provides the legal framework that allows individuals to naturally reconceptualise themselves by regulating what personal information is available about them on the internet, as well as who holds such personal information. McGoldrick critically points out that data subjects who reconceptualise their image, may also cover-up past crimes, and this new image may not be a true reflection of who

---

[548] The CJEU in *Google Spain* referred to "the role played by the data subject in public life" – see *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 81.

[549] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 93 – 94. C Wolf 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 at 553 and H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 562.

[550] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 563.

[551] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014.

[552] S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 339 341. Note also *Google Netherlands B.V v Google Inc.* NL:HR:2017:316. For 'public figure' see Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 13 – 14. For whether the data is 'relevent' see Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 15 – 17.

[553] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 13 – 20, and *Hurbain v Belgium* [2023] ECHR 948 para 77ffg.

[554] NNG de Andrade 'Oblivion: The right to be different … from oneself: Reproposing the right to be forgotten' (February 2012) 13 *IDP. Revista de Internet, Derecho y Política* 122 at 124 and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 257 – 258.

[555] D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 765. See also E Frantziou 'Further developments in the right to be forgotten' (2014) 14 *Human Rights Law Review* 761 – 778.

the person really is.[556] Jones adds that this reconcetualisation is now much easier in light of the right to be forgotten.[557]

Hijmans is generally supportive of the CJEU's decision.[558] In his opinion, the CJEU convincingly argued that search engines play a decisive role in disseminating information, including personal information.[559] Hence, search engines cannot escape responsibility, based on the journalistic exemptions provided in Directive 95/46, because they do not engage in journalistic work.[560] He argues that their core function is to process large volumes of information for dissemination, which is inextricably connected to the search engine's economic activities (in the form of advertising space).[561] To clarify what the "inextricable link" test means, Article 29 WP, in their updated Opinion 8/2010, set out applicable guidelines to determine whether EU law is applicable to non-EU companies.[562] Hijmans pointed out that if search engines were to escape any form of responsibility, then "this would compromise the effective and complete protection of [the] fundamental rights" to privacy and data protection.[563] Esposito observed that data or information, including published information, is not always indexed in search results in accordance with the date of publication.[564] This is problematic, because older information, depending on its position on the results page, may be perceived as being the most current information about a data subject.[565] Although discussed later, the CJEU solved this issue by requiring that, instead of the information being forgotten, the algorithms

[556] D McGoldrick 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 at 765. Note also EP Maat '*Google v. CNIL*: A Commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 246 – 247 where Maat points out that academics have argued that the right to be forgotten operates to suppress freedom of expression as well as the truth, and that the EU places a greater value to privacy compared to the United States.
[557] ML Jones 'Forgetting made (too) easy' (2015) 58(6) *Communications of the ACM* 34 – 35.
[558] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 – 563.
[559] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 559.
[560] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 562.
[561] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 559.
[562] Article 29 Data Protection Working Party *Update of Opinion 8/2010 on applicable law in light of the Court of Justice judgment in Google Spain,* adopted 16 December 2015.
[563] H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 560.
[564] E Esposito 'Algorithmic memory and the right to be forgotten on the web' (2017) April 4(1) *Big Data & Society* 1 at 6.
[565] E Esposito 'Algorithmic memory and the right to be forgotten on the web' (2017) April 4(1) *Big Data & Society* 1 at 6 – 7, Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018), and R Seyfert 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1542 at 1550 – 1552.

be reworked to display the latest information first on the results page.[566]

The right to be forgotten is a statutory right, also referred to as a procedural right. It is, however, a part of the right to privacy and assists in protecting aspects of dignity.[567] However, the right to be forgotten is qualified, meaning that a request will not automatically result in a removal of the links from the data subject's name; this has received generally positive responses from academics.[568] The qualification is to encourage the balancing of the relevant rights, freedoms and interests at play, between the data subject, and internet users. Ultimately, the right to be forgotten impacts the right to freedom of expression and information.[569] Edros summed the balancing of the right to be forgotten with the right to freedom of expression and information in that the right to be forgotten[570]

> "recognises and seeks to integrate tensions with other rights including to freedom of expression but does not see these rights as inherently inconsistent with data protection playing a role in policing the dissemination of personal information online."

As succinctly noted by Peguera, each matter must be decided on its own facts.[571]

---

[566] *GC & others v CNIL* EU:C:2019:773 para 78. See also the discussion in R Seyfert 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1542 at 1550 – 1552 regarding the programming of algorithms. N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR Jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 – 1473 outlines the types of technical measures available to implement right to be forgotten requests.

[567] In some countries reference is also made to the right to identity, see NNG de Andrade 'Oblivion: The right to be different … from oneself: Reproposing the right to be forgotten' (February 2012) 13 *IDP. Revista de Internet, Derecho y Política* 122 at 125. Germany calls this a right to informational self-determination (it falls under the right to personality), see C Kodde 'Germany's 'right to be forgotten' – between the freedom of expression and the right to informational self-determination' (2016) *30 International Review of Law, Computer & Technology* 17 at 20, and see also BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 – *Volkszählungsurteil*.

[568] *NT1 and another v Google LLC and another* [2018] EWHC 799 (QB) para 13.9.

[569] ML Ambrose & J Ausloos 'The right to be forgotten across the pond' (2013) 3 *Journal of Information Policy* 1-23, M Fazlioglu 'Forget me not: The clash of the right to be forgotten and freedom of expression on the Internet' (2013) 3(3) *International Data Privacy Law* 149 – 157, L Jaume-Palasi '"*Google Spain* case": Court decision privatises the public sphere' Internet Policy Review 27 May 2014. *https://policyreview.info/articles/news/google-spain-case-court-decision-privatises-public-sphere/291* (Accessed: 22 February 2025), DC Nunziato 'The fourth year of forgetting: The troubling expansion of the right to be forgotten' (2018) 39(4) *University of Pennsylvania Journal of International Law* 1011 at 1020, D Clifford & J Ausloos 'Data protection and the role of fairness' (2018) 37(1) *Yearbook of European Law* 130 at 142 – 154, M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 – 212, and S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 323 – 324, 327 – 334 and 339 – 341.

[570] D Edros 'The "right to be forgotten" beyond the EU: An analysis of wider G20 regulatory action and potential next steps' (2021) 13(1) *Journal of Media Law* 1 at 8, see also D Edors 'European Union data protection law and media expression: Fundamentally off balance' (2016) 65 *International and Comparative Law Quarterly* 139 at 140, and D Erdos 'Statutory regulation of professional journalism under European data protection: Down but not out?' (2016) 8(2) *Journal of Media Law* 229 – 265.

[571] M Peguera 'In the aftermath of *Google Spain*: How the right to be forgotten is being shaped in Spain by courts and the Data Protection Authority' (2015) 23 *International Journal of Law and Information Technology* 325 at 331ffg.

Directive 95/46 provides an exemption for journalistic activities,[572] and thus recognised the important role that the press plays within a democratic society, in line with the right to freedom of expression as well as to information.[573] Ovčak Kos notes that public opinion is shaped not only through accessing the latest news, but also through archived articles.[574] As the case discussion below illustrates,[575] the right to be forgotten may be used as a form of censorship and may manipulate the record of contemporary historical events.[576] Ovčak Kos argues that the best way to solve the legal uncertainty left by *Google Spain* is not to establish precise criteria to deal with the conflict between the right to be forgotten and the right to freedom of expression, but rather to focus on the core considerations established by the courts when balancing the rights to privacy and freedom of expression.[577] These established considerations already protect and recognise the importance of the rights, freedoms and interests of all parties involved, and assist in finding the best solution in light of the unique circumstances of each case.[578]

Ground-breaking is that *Google Spain* presents a solution to cease the internet's eternal memory.[579] Ausloos, although dealing specifically with the GDPR's Article 17 "Right to erasure (right to be forgotten')" ultimately concluded that the right to be forgotten is a

[572] Article 9 of Directive 95/46. The right to freedom of expression and information is protected in Article 11 of the Charter and Article 10 Convention.
[573] M Ovčak Kos 'The Right to be Forgotten and the Media' (2019) 11(2) *LeXonomica* 195 at 204 – 205. See also M Peguera 'In the aftermath of *Google Spain*: How the right to be forgotten is being shaped in Spain by courts and the Data Protection Authority' (2015) 23 *International Journal of Law and Information Technology* 325 at 343 – 345.
[574] M Ovčak Kos 'The Right to be Forgotten and the Media' (2019) 11(2) *LeXonomica* 195 at 209.
[575] Compare the responses by the ECtHR in *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) and *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021).
[576] M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 209. See also F Zufall 'Challenging the EU's right to be forgotten: Society's right to know in Japan' (2019) 5 *European Data Protection Law Review* 17 at 19 – the Japanese Supreme Court held that search engines provide "titles and snippets as a preview" of each of the results listed, which contains enough personal information for the user to understand what the link contains, and hence this amounts to processing. The court held that it is important that the competing rights of right to personality and freedom of expression (which includes the right to know) are balanced in terms of each case before the court.
[577] M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 209 – 210.
[578] M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 210 – 211. See also S Singleton 'Balancing a right to be forgotten with a right to freedom of expression in the wake of *Google Spain v. AEPD*' (2015) 44 *Georgia Journal of International and Comparative Law* 165 – 194, F Zufall 'Challenging the EU's right to be forgotten: Society's right to know in Japan' (2019) 5 *European Data Protection Law Review* 17 at 19 and K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157.
[579] JS Van Oyen, M Lange & S Kreinsen, 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 at 307.

"powerful tool" to protect the fundamental rights to privacy and data.[580]

How the right to be forgotten has been balanced with the right to freedom of expression, as well as further defining the jurisdictional reach of Directive 95/46, and later the General Data Protection Regulation, are amongst some of the issues dealt with by the courts. The following discussion includes judgments from both the regional (ie Court of Justice of the European Union (CJEU) and the European Human Rights Court (ECtHR)) and the highest national courts of the European States.[581]

IV DEVELOPING GOOGLE SPAIN'S RIGHT TO BE FORGOTTEN THROUGH THE CASE LAW

(a) Introduction

The following will outline the development of the right to be forgotten, focussing on judgments from either the regional or highest national courts, in Europe. These cases have defined and discussed the right to be forgotten, providing the scope and considerations to keep in mind when balancing the right to be forgotten with the right to freedom of expression. The cases from the national high courts of each European State will be from their highest national appeal courts, or constitutional courts. The case discussions are not in chronological order, but categorised in broad topics, namely the territorial application of the right to be forgotten; the application of the right to be forgotten in criminal matters; statements, interviews, etc, made in a professional capacity; the processing of special categories of data; and the anonymisation of archives. Each topic will be discussed in turn.

(b) Territorial jurisdiction

The territorial or physical jurisdiction refers to how far the right to be forgotten must be applied, ie is the application limited to only within a single State or country or can it be expanded regionally, as in the EU? The leading case in this instance is *Google LLC v Commission*

[580] J Ausloos *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018 at 403.

[581] The United Kingdom whilst still a member of the European Union, applied the right to be forgotten within its own case law, following the judgment of the CJEU of the European Union. The European Union is made up of 27 Member States, which have signed Treaty on the Functioning of the European Union (Consolidated 2016) (TFEU), formerly Treaty Establishing the Economic Community, signed at Rome, on 25 March 1957 (the Treaty of Rome) – see Article 358 of the TFEU, which created the CJEU. The ECtHR emanated from the European Convention on Human Rights, which has been ratified by 47 States (including Member States of the European Union).

nationale de l'informatique et des libertés (CNIL) (*Google LLC v CNIL*).[582] This case, due to the far-reaching consequences it has globally, will be set out in some detail. Defining the physical or territorial jurisdictional application of the right to be forgotten is vital when balancing the rights, freedoms and interests of all the parties concerned, especially since the territorial application of the right to be forgotten has a tremendous impact on how personal information may be accessed.

(i) Background and issue

The Conseil d'État,[583] referred the territorial jurisdiction issue to the CJEU for a preliminary ruling.[584] The specific issue raised by the Conseil d'État was a general enquiry, namely, whethere a request for de-linking of personal data extends to all Google's extensions, ie does the request apply to all countries in which Google is active?[585] Briefly, the CNIL had served Google with a formal notice requesting the removal of personal data of a natural person in all its domains.[586] Put differently, must Google apply the right to be forgotten globally? Google refused and only applied the right to be forgotten in the EU member States. Google, where it operates, refers to each country as a domain, and each domain has a separate geographic extension. These extensions can be accessed, no matter in which domain/country an individual uses the Google search tool. Each search tool/domain is tailored to the specific country's market in which it operates, ie the language(s) spoken in each country, and provides advertising

---

[582] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772. See also *Hurbain v Belgium* [2023] ECHR 948 para 85.

[583] The Council of State, France.

[584] *Google LLC v CNIL* EU:C:2019:772. See also T Bertram, E Bursztein, S Caro *et al* 'Five years of the right to be forgotten' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*) (11 – 15 November 2019, London, United Kingdom) 959 at 961, E Flett & J Clover '*Google LLC v CNIL* – CJEU rules on the territorial scope of the "right to be forgotten"' (2020) 31(2) *Entertainment Law Review* 69 – 71, CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 261 – 262, J Globocnik 'The right to be forgotten is taking shape: CJEU judgments in *GC and others* (C-136/17) and *Google v CNIL* (C-507/17)' (2020) 69(4) *GRUR International* 380 – 388, and EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 – 261

[585] *Google LLC v CNIL* EU:C:2019:772 para 2. J Globocnik 'The right to be forgotten is taking shape: CJEU judgments in *GC and others* (C-136/17) and *Google v CNIL* (C-507/17)' (2020) 69(4) *GRUR International* 380 – 388. See also *Biancardi v Italy* [2021] ECHR 972 paras 25 – 26.

[586] According to *TechTerms.com*: a domain name

> "is a unique name that identifies a website. For example, the domain name of the TechTerms Computer Dictionary is "techterms.com." Each website has a domain name that serves as an address, which is used to access the website. . . The domain suffix helps identify the type of website the domain name represents. For example, ".com" domain names are typically used by commercial websites, while ".org" websites are often used by non-profit organizations. Some domain names end with a country code, such as ".dk" (Denmark) or ".se" (Sweden), which helps identify the location and audience of the website."

See P Christensson 'Domain name definition' *TechTerms.com*, 14 September 2012, h*ttps://techterms.com/definition/domain_name* (Accessed: 10 December 2022).

opportunities for the local businesses. Google in this matter argued that, beyond the domain or the region, ie the European Union, it should not have to remove the link to the data complained of in other extensions, as these are not, in terms of legal jurisdictions, affected by the request for de-linking.[587] In other words, the question before the CJEU relates to what the territorial scope of the right to be forgotten is.[588]

(ii) The territorial extent of the right to be forgotten

Before addressing the issue at hand, the CJEU used the terms "geo-location" and "geo-blocking". It is important to clarify and understand these terms, in relation to the territorial extent of the right to be forgotten. Geo-location simply refers to the actual location of the internet user, ie are internet users accessing the internet, via an internet capable device, from South Africa, Australia, France, etc.? The geo-location is ascertained with the use of the Internet Protocol Address (IP address).[589] Google uses geo-location to automatically re-direct an internet user from the Google generic search tool (ie google.com), to the local search tool of the domain/country applicable in which they are situated. The results displayed will be in accordance with the information for that domain.[590] Geo-blocking, on the other hand, uses the geo-location techniques to block access to information "regardless of the version of the search engine used".[591] Put differently, it is possible to limit access to the de-linked information in a specific domain or region, ie anyone trying to access the information from a domain within the EU will be blocked. However, it is still available to persons outside the EU.[592]

(iii) Application

The CJEU noted that the internet has become an international search tool, and that it is possible to obtain information from any domain within the world, especially since the start of globalisation and the ability of a person to access personal information about individuals that

[587] *Google LLC v CNIL* EU:C:2019:772 paras 36 – 39.
[588] *Google LLC v CNIL* EU:C:2019:772 para 53.
[589] Opinion of Advocate General Szpunar in *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) EU:C:2019:15, delivered 10 January 2019 para 71.
[590] *Google LLC v CNIL* EU:C:2019:772 para 42.
[591] *Google LLC v CNIL* EU:C:2019:772 para 43.
[592] Opinion of Advocate General Szpunar in *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) EU:C:2019:15, delivered 10 January 2019 para 71, E Flett & J Clover '*Google LLC v CNIL* – CJEU rules on the territorial scope of the "right to be forgotten"' (2020) 31(2) *Entertainment Law Review* 69 at 70, EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 249 – 250, N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 at 1673 – 1674.

are found in another domain.[593] Although the CJEU, confirmed *Google Spain* and the interpretation of the right to be forgotten,[594] it emphasised that the right is not absolute and must be proportionally balanced with fundamental human rights.[595] Importantly, and in terms of the GDPR, the EU has tried to strike a balance between the right to be forgotten and the right to privacy, along with the right to freedom of expression and information. However, the legislation is silent regarding how such a balance can be achieved with information found in a domain outside of the EU.[596] In other words, the right to be forgotten is specifically applicable in the EU and not globally, even if it is recognised in other legal jurisdictions. In other words, the CJEU held that there is a territorial limit to the right to be forgotten.

When information is obtained within the EU, the question that then arises is whether the de-linking applies to individual Member States only, or to the entire EU region. The CJEU pointed out that the Member States have signed the GDPR (as was the case with Directive 95/46) to ensure "a high level of protection [of personal data] throughout" the EU and remove "obstacles to flows of personal data within the" EU.[597] In Directive 95/46 there was no uniformity, within the EU, in how the proportionality test was applied among the Member States, leading to varying weight being given to the rights to privacy and being forgotten and the rights to freedom of expression and information.[598] The GDPR, however, indcludes a mechanism to provide consensus and consistency within the EU, where the affected rights are balanced against each other.[599]

---

[593] *Google LLC v CNIL* EU:C:2019:772 para 56 – 57.

[594] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 80; *Google LLC v CNIL* EU:C:2019:772 para 56.

[595] This balancing exercise is likely to occur in most countries around the world – *Google LLC v CNIL* EU:C:2019:772 para 60. See also *Volker und Markus Schecke GbR and Eifert v Land Hessen (Bundesanstalt für Landwirtschaft und Ernährung joined party)* EU:C:2010:662 para 48 and *Fuchsmann v Germany* [2017] ECHR 925 para 32ffg with regards to an example of the approach of the ECtHR. See also EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 257 – 258. *LB v Hungary* [2023] ECHR 239 paras 47 – 53 summarises the CJEU's cases that discussed the protection of personal data in light of the balancing of all the relevant rights.

[596] *GC & others v CNIL* EU:C:2019:773 para 59; *Google LLC v CNIL* EU:C:2019:772 para 61. See also EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 245 – 246 and 255 – 256. Note the CJEU confirmed that there is no global right to be forgotten – *Google LLC v CNIL* EU:C:2019:772 para 63.

[597] *Google LLC v CNIL* EU:C:2019:772 para 66. See also EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 249.

[598] *Google LLC v CNIL* EU:C:2019:772 para 67.

[599] The process is described in para 68 of *Google LLC v CNIL* EU:C:2019:772: In terms of the GDPR

> "Articles 56 and 60 [provide] for cross-border processing as defined in Article 4(23). . .subject to Article 56(2) thereof, the various national supervisory authorities concerned must cooperate, in accordance with the procedure laid down in those provisions, in order to reach a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union. Moreover, Article 61. . .obliges the supervisory authorities. . .to provide each other with relevant information and mutual assistance [to

In so far as the required legal measures to be taken were concerned, the CJEU pointed out that a data subject's fundamental rights and freedoms are to be protected throughout the EU. The requisite legal measures implemented must at least discourage, if not prevent, internet users within the EU from gaining access to the links that lead to personal information, when using the data subject's name as the search term.[600] The CJEU pointed out that, even though the GDPR contains a mechanism to provide consistency and uniformity with regard to the proportionality test, there is no provision that specifically states that when a person is granted a de-linking request in one domain (or country) within the EU region, the request must be applied automatically to all domains.[601] However, the relevant supervisory or judicial authority remains competent to decide whether the personal data should no longer be available throughout the EU.[602] The CJEU did encourage uniformity between Member States.[603]

(iv) Conclusion

In conclusion, the CJEU held, that "on a proper construction of" Article 12*(b)* and Article 14*(a)* of Directive 95/46 and Article 17(1) of the GDPR,[604] where a request for delinking has been granted in one EU domain, that decision does not automatically apply to all domains across the EU. However, in order to promote consistency throughout the EU and protect the fundamental right to privacy, the CJEU encouraged all domains within the EU to apply such requests in their own domains.[605] That means that the right to be forgotten is restricted, as in this case, to a region, ie access to the information is restricted to within the EU.[606]

---

apply the GDPR consistently throughout the EU in terms of the consistency mechanism in] Article 63 [and] Articles 64 and 65. . .[where a matter is urgent] Article 66. . .permits the immediate adoption, in exceptional circumstances, where. . .there is an urgent need to act in order to protect the rights and freedoms of data subjects, of provisional measures intended to produce legal effects on its own territory with a specified period of validity which is not to exceed three months."

[600] *Google LLC v CNIL* EU:C:2019:772 para 70; see also *Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH* EU:C:2014:192 para 62 and *McFadden v Sony Music Entertainment Germany GmbH* EU:C:2016:689 para 62. See also *Google LLC v CNIL* EU:C:2019:772 paras 42 – 43. A possible method is through geo-location and geo-blocking, although this was not specifically mentioned by the CJEU.

[601] *Google LLC v CNIL* EU:C:2019:772 paras 64 and 72.

[602] *Google LLC v CNIL* EU:C:2019:772 para 72. See also *Åklagaren v Åkerberg Fransson* EU:C:2013:105 para 29, *Melloni v Ministerio Fiscal* EU:C:2013:107:60 para 59 – 60 and *Spiegel Online GmbH v Volcker Beck* EU:C:2019:625 paras 19 – 21. For a detailed discussion of *Melloni v Ministerio Fiscal* see M Rodriguez-Izquierdo Serrano, 'The Spanish Constitutional Court and fundamental rights adjudication after the first preliminary reference' (2015) 16(6) *German Law Journal* 1509 – 1528. For a brief discussion of *Spiegel Online GmbH v Volcker Beck* see CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 259 – 261.

[603] *Google LLC v CNIL* EU:C:2019:772 para 66. See also EP Maat '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 at 258 – 260.

[604] *Google LLC v CNIL* EU:C:2019:772 para 73.

[605] E Flett & J Clover '*Google LLC v CNIL* – CJEU rules on the territorial scope of the "right to be forgotten"' (2020) 31(2) *Entertainment Law Review* 69 at 71.

[606] R Belbin 'When Google becomes the norm: The case for privacy and the right to be forgotten' (2018) 26

The next aspect tends to be a very sensitive one, namely criminal trials and convictions, especially where a former accused person is rehabilitated and wishes to integrate into society.

(c) The right to forget a crime and criminal trials

(i) Introduction

Generally, most persons, once their sentence has been served, wish to start on a clean slate and forget their criminal past. The problem faced by former offenders is that the information is still available to internet users and is often one of the top results, based on searches when their names are the search terms. The right to be forgotten may be used to assist with the complete integration of sentenced criminals within society, by restricting access to information regarding their criminal past. There are three cases that will be discussed under this topic. One point of reference is that some of the arguments are similar to those cases that deal with the anonymisation of information that is found in online archives. The reason is that particularly remarkable criminal cases form a part of the contemporary history of each State, and these are often found in media archives.[607] However, some of the considerations set out below are not exclusive to the application of the right to be forgotten in criminal matters, they are capable of universal application. This is not a comprehensive discussion on the topic, these cases are simply examples of how the right to be forgotten may apply in criminal matters.

The three cases originated from different countries, two were resolved at national level,[608] and one was referred for a preliminary hearing to the ECtHR.[609] The first case is from the Queen's Bench, United Kingdom (UK) and is *NT1 v Google LLC* (*NT1*).[610] The second

Dalhousie Journal of Legal Studies 17 at 21, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 261 – 262. See also *Google Inc. v Equustek Solutions Inc.* 2017 SCC 34, V Goswami 'Algorithms, expression and the Charter: A way forward for Canadian Courts' (2017) 7(1) *Western Journal of Legal Studies* Article 2 at 1 – 15, and R Diab 'Search engines and global takedown orders: *Google v Equustek* and the future of free speech online' (2020) 56(2) *Osgoode Hall Law Journal* 231 – 270.

[607] The reason for dealing with these three cases under one heading is because, they were matters dealing solely with past criminal convictions where the data subjects (ie the applicants or complainants in their respective matters) were not asking for the deletion of their personal data online, but for the de-linking or de-referencing thereof, ie they were requesting that their data be "forgotten". These requests were made with the relevant search engine. Later in this chapter, the data subjects, in their respective criminal matters, either approached the court for an order against the country's data protection authority in terms of Article 8 of Directive 95/46, which provides for the prohibition against processing sensitive data; or they were requesting for the anonymisation of their names within an article or deletion of their personal data directly from the publishers.

[608] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

[609] *GC AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773, and *ML v Slovakia* [2021] ECHR 821.

[610] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB).

case that will be discussed was delivered by the Bundesverfassungsgericht,[611] Germany, and is referred to as *Recht auf Vergessen 1*.[612] The third case originated in Slovakia, but was referred to the ECtHR, namely *ML v Slovakia*.[613] Common to all matters is that journalists reported on the criminal trial proceedings, and the subsequent convictions and sentences. Hence, the data of their criminal trials was available in the online media archives.[614]

In two of the three cases under this discussion, it was through the digitising of archives that the articles including the personal data became available on the internet. Wherein *NT1*[615] the conviction and sentence had been served and had been automatically expunged, in *Recht auf Vergessen I*,[616] despite the complainant having served his term of imprisonment for murder, and even though these articles were relatively old, his criminal record was not expunged due to the serious nature of the crime.[617] The complainant was seeking full re-integration and rehabilitation back into society. In the third case, *ML v Slovakia*,[618] it was the press, a year after the death of the accused, which brought up the criminal convictions, leading to a great deal of stress and heartache for the family, especially the mother of the deceased accused, who was the complainant in the matter.[619]

In terms of criminal convictions, the following three aspects will be discussed, in light of the right to be forgotten: forgetting expunged criminal convictions,[620] accessing contemporary historical events stored in unaltered media archives,[621] and where a family

[611] The Federal Constitutional Court, Germany.
[612] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.
[613] *ML v Slovakia* [2021] ECHR 821.
[614] Compare with the Californian State Laws, United States, see M Keiter 'Criminal law principles in California: Balancing a right to be forgotten with a right to remember' (2018) 13 *California Legal History* 421 – 472.
[615] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB). For a general discussion see P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 – 390.
[616] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*. For a short discussion of the case see CM Wulff 'The right to be forgotten in post-*Google Spain* Case Law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 263 – 268. For a detailed discussion, with a comparative to the EU law, especially with regards to the judgments of the CJEU, see R Hofmann, A Heger & T Gharibyan 'Die Wandlung des Grundrechtsschutzes durch das Bundesverfassungsgericht – *Recht auf Vergessen I* und *II* als "*Solange III*"?' (2019) 102(4) *KritV Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* 277 – 292 and M Wasser *You're Forgiven but not Forgotten: The coherence of the right "to be forgotten" in Germany and the EU* (unpublished bachelor thesis (partial-fulfilment), University of Twente, the Netherlands, 2 July 2020).
[617] In BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* – a period of 30 years had passed since the convictions and the uploading the articles online.
[618] *ML v Slovakia* [2021] ECHR 821.
[619] *ML v Slovakia* [2021] ECHR 821.
[620] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB).
[621] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

member of an accused applies for the information regarding a crime to be forgotten.[622]

(ii) Forgetting expunged criminal convictions

Although criminal records may be automatically expunged, depending on the nature of the crime, they do still come back to haunt those that committed the crime. The Queen's Bench in *NT1 v Google LLC*[623] (*NT1*) focused on criminal convictions that resurfaced after they had been automatically expunged. In *NT1*, briefly, two businessmen (the applicants in this matter) were convicted and sentenced for fraud or fraudulent behaviour. In terms of the provisions of the Rehabilitation of Offenders Act 1974 these convictions had been automatically expunged, after the lapse of the relevant time periods.[624] However, when the names of the applicants/businessmen were used as the keywords in the Google search tool, the expunged convictions appeared as a part of the top results returned in the list of links. The applicants applied for the links to be forgotten,[625] ie they applied for the links to be de-linked or de-referenced, on the grounds that they were seeking full rehabilitation into society, and thus no longer wished to be confronted by their past criminal misdemeanours.[626]

Although the Queen's Bench in *NTI* made numerous references to Directive 95/46 and *Google Spain* throughout its judgment, only those pertinent to the implementation of the right to be forgotten will be discussed in this section.[627]

The Queen's Bench started by clarifying a few points, namely: the label, ie the right to be forgotten, is somewhat of a misnomer, as individuals are not asking to be forgotten, but requesting that information about them, whether accurate or erroneous, no longer appears as a link on the results page of an internet search, when their name is used as the search term

---

[622] *ML v Slovakia* [2021] ECHR 821.
[623] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB). See also *Hurbain v Belgium* [2023] ECHR 948 paras 101 – 105.
[624] See s 4 of the Rehabilitation of Offenders Act 1974.
[625] The application was brought as a result of the outcome in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, where the CJEU used the right to be forgotten as the remedy to de-link or de-reference links that appear on the results page, based on the data subject's name as the search term. See *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 9, and P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388 – 390. Compare with Mauritius: JD Mujuzi 'Spent convictions in Mauritius: Analysing the Police and Criminal Evidence Bill, 2013' (2015) 3 *South African Journal of Criminal Justice* 284 – 302, and New Zealand: F Gollogly 'The blemish on the Clean Slate Act: Is there a right to be forgotten in New Zealand?' (2019) 25 *Auckland University Law Review* 129 – 154.
[626] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), see specifically paras 5 – 8 and 13. See P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 384 – 385.
[627] See generally, *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 13, 22, 27, 29, 31 – 37, 52, 82, 85, 95, 101, 103 – 105, 107, 110 – 115, 131 – 133, 145, 147, 150, 161 – 162, 166, 170, and 223.

keyword.[628] The information need not be removed by the original publisher thereof. In other words, "the de-listing request" is only when a search is done using the individual's name and the link to the information[629] may be returned when a search is done using other keywords, other than the individual's name.[630]

The Queen's Bench in *NT1*, in discussing Directive 95/46, emphasised that the right to be forgotten is a qualified right.[631] Summarising the salient features of *Google Spain*,[632] the Queen's Bench provided a non-exhaustive list of factors, to be considered when a person is requesting that data be forgotten or de-linked. Some of these factors find universal application, whereas a few are specific in relation to de-linking or de-referencing of expunged criminal matters. The considerations discussed by the court included the following:

1 The Queen's Bench held that "the sensitivity of the data in question is an important element" when striking the balance between the various competing rights and interests.[633] To this extent it is worth noting that the rights and freedoms in the Charter are of equal value.[634] Hence, specifically in light of expunged criminal convictions, the fact that the criminal record has been expunged will play an important role in granting the right to be forgotten. Even though this is an important factor, the rights of the data subject will still be balanced with those of the general internet users, as well as that of the publishers in appropriate instances.[635]

2 *NT1* clarified the role of search engines where they process personal information as discussed in *Google Spain* as follows: search engines have a far wider impact, than eg hard copy newspapers, journals, etc., on the distribution of information, including personal data, which has a greater impact on privacy and data protection.[636] Search

[628] The Queen's Bench pointed out that it is very likely that where a successful request has been made against Google, that other internet search engines or ISEs, such as Yahoo, Bing, etc. will merely de-list the information automatically, *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 38.
[629] Referred to as a URL or universal resource locator, *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 38.
[630] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 38.
[631] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 13(8) and 13(9). The court emphasised the importance, in para 13(8), of applying the Charter to the provisions of Directive 95/46. See also P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388.
[632] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 33.
[633] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 38. See also I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) 302 – 304.
[634] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 131 – 133.
[635] See also K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157.
[636] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 33(1), *eDate Advertising GmbH v X, Martinez & another v MGN Limited* EU:C:2011:685 para 45, and *Google Spain SL, Google Inc. v AEPD, Mario*

engines, due to the nature of their business, cannot claim that they are processing data "solely for journalistic purposes", because the nature of their business is to make a profit from the searches conducted by internet users.[637] Thus, Google in responding to a search "on an individual's name" facilitates "access to journalistic content about that individual" which is "purely accidental, and incidental to its larger purpose of providing automated access to third party content" irrespective of whether the content contains personal data or not. The data is identified on the tags provided by the content provider, and where these tags meet the search criteria of the internet user, a link is created to that information. The linking of information on a results page is for Google's own commercial exploits, no matter how profitable and are "not undertaken for any of the special purposes, or 'with a view to' the publication by others of journalistic material".[638]

3 The de-listing request is based on the data subject's circumstances at the time that the request is made.[639] Hence, a de-listing request made to a search engine, for data or information that was published in terms of a law or court order, and contains "true information" about the data subject, which are now "irrelevant or no longer relevant, or excessive in relation to" the original purpose for the publication thereof, is a suitable remedy.[640]

4 The right to rehabilitation, whether it be a criminal or a sequestrated individual, is an aspect of the law of privacy. Rights protected under this rubric include the right to reputation, the right to family life and the right to a private life, including the "unhindered social interaction with others." Although the right to privacy tends to support the rehabilitation of offenders back into society from a societal point of view, the right remains qualified and must be balanced against the conflicting "rights of others

Costeja González EU:C:2014:317 para 80.

[637] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 33(2) and 105 – 115, and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 85.

[638] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 100. Compare with *Google LLC v The Privacy Commissioner of Canada, & others* 2023 FCA 200 where the majority held that the collection of personal data for indexing and to subsequently display as a link on a results page for internet users does not amount to the collection of personal data for commercial purposes in terms of Canada's Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5 – see paras 88 – 91.

[639] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 33(4), and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 94 and 96.

[640] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 33(3), and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 94.

to freedom of information and freedom of expression".[641]

5 The court emphasised that legal proceedings are public proceedings – in this instance no individual will have a reasonable expectation of privacy during such hearings. However, at a later date, the information may become personal again. With regards to convictions, a formal statute will determine the date in time when the convict may expect that the "information about the crime, conviction, or sentence" will be private.[642] A starting point is that the conviction is "spent" adding more weight to the protection against further disclosure, and "in favour of that information being 'forgotten'". However, the right to the individual's privacy must still be balanced against the public's competing rights to receive and impart information and freedom of expression.[643] Earlier the court emphasised that where a person commits a crime, they should foresee that due to their own actions, they may suffer a loss of reputation, and that certain personal information will be made public during proceedings.[644]

6 Regarding the balancing exercise, the nature and extent of any actual or future harm will be assessed, and where disclosing the data will "or is likely to cause, serious or substantial interference with private or family life that will tend to add weight to the case for applying the general rule" of "forgetting".[645] This would include whether there may be substantial harm caused to the data subject, where the link is still available on a search done using their name as the search term.[646]

7 In terms of the proportionality assessment, an important question is what benefit, if any, the information will serve the public – factors include the nature and quality of, and how current, the information is – namely, latest news or is it older? Although freedom

---

[641] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 166.1. P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388, and K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157 at 3 – 5 and 8 – 11.
[642] P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388.
[643] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 166.2. See also the remarks of the ECtHR in *ML v Slovakia* [2021] ECHR 821 para 38.
[644] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 111 and 162. See also *Axel Springer AG v Germany* [2012] ECHR 227paras 79 and 83 – 84. P Kirkwood '*NT1 & NT2 v Google LLC* – the secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 387.
[645] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 166.3. See also P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 387 – 388. This is similar to the argument in *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67, where it was held that privacy exists on a continuum, the closer the data is to the core of privacy, the more likely that the right to be forgotten will be granted.
[646] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 147 – 155.

of expression is important – the court found that in some instances the right to privacy will be of greater importance than the right to free expression – but this will depend on the facts and circumstances of each case.[647]

8 Finally, in the UK, the courts will focus not only on the *Google Spain* balancing exercise, but will also look at the domestic legal principles, and it was ultimately noted that: "de-indexation does not per se remove the source websites containing the relevant data from the online environment. It merely makes that data harder for the public to find."[648]

Between the two businessmen/applicants, the first applicant was not successful in his bid for the de-linking request whereas the second applicant had more luck. This was mainly due to the differing personal circumstances. In terms of the first applicant, the Queen's Bench, apart from the balancing of competing rights (ie the first applicant's right to privacy and the public's right to information), found that the first applicant did not have a reasonable expectation of privacy, because the information mainly focussed on the first applicant's business undertakings.[649] Thus, the processing of the information was proportionate to the public's right to information.[650]

In relation to the second applicant, the Queen's Bench found that the information was inaccurate and no longer relevant in terms of the data protection principles. Hence, it was ordered that the information be de-listed, de-linked or de-referenced. The reasoning of the Queen's Bench was that due to the passage of time the information was now outdated and irrelevant and was no longer of use or interest to the public.[651]

---

[647] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 166.4, see also para 145 in respect of "sensitive" data also known as the "special categories" of data. K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157 at 2.

[648] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 166.5. The Queen's Bench used various aspects of domestic law to guide its decision, one of these being the law of defamation. In a claim for defamation the meaning of the offending text, as read by an "ordinary reader" is vital in deciding whether there has been an infringement committed on the rights to privacy and reputation – see generally paras 82 – 87.

[649] In terms of the arguments in *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67, this information would not be considered to be close to the inner core of sanctum of privacy.

[650] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 136 – 173, and 229, and P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388.

[651] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) para 174 – 228 and 230, and P Kirkwood '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 at 388.

(iii) Considerations of access to contemporary historical events in online archives

Recht auf Vegessen I was a challenge against the decision of the Bundesgerichtshof[652] where it held that the complainant was not entitled to have articles discussing his past conviction and sentence de-linked from a search done using his name. The Bundesgerichtshof reasoned that the public's accessibility to contemporary historical events was more important than the complainant's right to be forgotten. The crux of *Recht auf Vegessen I* discussed the limitless availability of information on the internet, and the implication or consequences on these rights.[653]

The dramatic facts of *Recht auf Vergessen I,*[654] briefly, are: the complainant shot two persons whilst on a yacht on the high seas during 1981. The complainant was convicted and sentenced to life imprisonment for murder in 1982. Subsequently, in 2002, he was released on parole. During 1982 and 1983, *Der SPIEGEL* magazine ran three print articles on the case, identifying the complainant by name. In 1999, Spiegel Online GmbH (Spiegel),[655] whilst

---

[652] The German Federal Court of Justice. The judgment of the Bundesverfassungsgericht (the Federal Constitutional Court, Germany) in BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* was quoted with approval in the dissenting judgment of Pavali J in *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021). See also *Hurbain v Belgium* [2023] ECHR 948 paras 113 – 121. Similar conclusions were reached by the ECtHR in *Mediengruppe Österreich GmbH v Austria* [2022] ECHR 316. See also R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 265 – 266.

[653] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 96, 101 – 103 – the ability for information to be taken out of context is vital. Note also BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and *Hurbain v Belgium* [2023] ECHR 948 paras 127 – 130.

[654] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* was quoted with approval in the dissenting judgment of Pavali J in *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021).

Compare with *Google Netherlands B.V v Google Inc*. NL:HR:2017:316 – a case from the Hoge Raad (the Dutch Supreme Court), the Netherlands – the complainant was convicted of a serious crime (murder). The Hoge Raad denied the complainant's request to de-link (ie forget) certain links on the results page, and referred the matter to "the Court of Appeal in Den Haag for further consideration and decision". In this case, the Hoge Raad actively balanced the rights of the complainant as well as of internet users, the balancing exercise being in line with *Google Spain*. For the history of the right to be forgotten in the Netherlands, see S Kulk & F Zuiderveen Borgesius, 'Freedom of expression and right to be forgotten cases in the Netherlands after *Google Spain*' (2015) 1 *European Data Protection Law Review* 113 – 124, and S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 – 348 (the second article discusses *Google Netherlands B.V v Google In*). Note also *Hurbain v Belgium* [2023] ECHR 948 para 111 where the seriousness of the offence may be a consideration as to whether the information will be de-linked or de-referenced (ie "forgotten") or not.

For a history of the right to be forgotten in Germany, see C Coors 'Headwind from Europe: The new position of the German courts on personality rights after the judgment of the European Court of Human Rights' (2010) 11(5) *German Law Journal* 527 – 537, C Kodde 'Germany's "right to be forgotten" – Between the freedom of expression and the right to informational self-determination' (2016) 30 *International Review of Law, Computer & Technology* 17 – 31, and JS Van Oyen, M Lange & S Kreinsen, 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 – 314. For a critical comment on this case see D Burchardt 'Backlash against the Court of Justice of the EU? The recent jurisprudence of the German Constitutional Court on EU fundamental rights as a standard of review' (2020) 21 *German Law Journal* 1 – 18.

[655] Spiegel Online GmbH is the internet offshoot from the magazine *Der SPIEGEL*, and is a part of the SPIEGEL-

digitizing the print magazine's archives, uploaded the articles onto the internet, making them freely accessible to the public. Thus, using the complainant's name in the search tool of an internet search engine, these articles appeared amongst the top results. During 2009, the complainant discovered the uploaded articles and that they appear among the top results in an internet search when his name is used as the search term. He lodged an action to halt Spiegel from disseminating the information any further. The Bundesgerichtshof[656] rejected the complaint, on the basis that information regarding contemporary historical events should be easily accessible to the public, which includes finding it with the most convenient, available search terms. The complainant appealed and the matter came before the Bundesverfassungsgericht.

The Bundesverssaungsgericht acknowledged that at the time the complaint was lodged Directive 95/46 was still operative.[657] Directive 95/46 requires, with a certain amount of freedom or autonomy[658] in its interpretation and implementation within each individual Member State,[659] that each Member State must "protect the right to privacy of natural persons with respect to the processing of personal data".[660] The Bundesverfassungsgericht held that such protection accords with the high standards as stipulated within Directive 95/46. The Bundesverfassungsgericht in coming to this conclusion stated that the Basic Law accords the same level of protection as that of the Charter. Directive 95/46 specifically provides Member States with some autonomy in the application of Article 9, which provides for the processing of personal data by the media, ie the "so-called media privilege".[661] Hence, the Bundesverssungsgericht focussed primarily on the rights of the data subject (referred to as the complainant), largely on the basis of applying the Basic Law, with the EU Law merely forming a backdrop to the discussion.[662]

Verlag Rudolf Augstein GmbH & Co. KG. The offices are situated in Hamburg, Germany. See generally, *https://www.spiegel.de/* (Accessed: 29 December 2022).

[656] The Federal Court of Justice, Germany.

[657] The GDPR repealed Directive 95/46 on 25 May 2018, but the original court proceedings began under Directive 95/46.

[658] The Bundesverfassungsgericht specifically uses the term "latitude", see BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 11 – 12.

[659] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 11 – 12, and generally see F Duina 'Explaining legal implementation in the European Union' (1997) 25 International Journal of the Sociology of Law 155 at 156.

[660] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 11.

[661] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 74. A similar "leeway" is provided in Article 85 of the GDPR.

[662] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 11 – 12, and 74, and see generally R Hofmann, A Heger, & T Gharibyan 'Die Wandlung des Grundrechtsschutzes durch das Bundesverfassungsgericht – *Recht auf Vergessen I* und *II* als "*Solange III*"?' (2019) 102(4) *KritV Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* 277 – 292, D Burchardt 'Backlash against the Court

The Bundesverfassungsgericht explained which rights needed to be balanced as follows:[663] first, Article 2(1), read with Article 1(1), of the Basic Law for the Federal Republic of Germany (Basic Law),[664] which together protect an individual's rights to personality (which includes the right to privacy) and generally against "statements affecting one's person".[665] Second, Article 5(1), which protects the right to freedom of expression and also guarantees

of Justice of the EU? The recent jurisprudence of the German Constitutional Court on EU fundamental rights as a standard of review' (2020) 21 *German Law Journal* 1 – 18, and Goldman, M 'As darkness deepens: The right to be forgotten in the context of authoritarian constitutionalism' (2020) 21 *German Law Journal* 45 – 54 for some of the criticisms and praise for the Bundesverfassungsgericht. In *Recht auf Vergessen I* the Bundesverfassungsgericht pointed out that each country within the EU is afforded a wide discretion, and even denying protection of certain rights conforms to the Convention and Charter see paras 42, 43, 49, 58, 62, 67 and 72 – 74. Germany is still an autonomous State within the EU, and the application of fundamental rights will be in terms of the German Basic Law and relevant legal principles, bearing in mind the protection of fundamental rights ensured in the Charter and relevant EU legislation, on a case-by-case basis. Hence, in some instances a combined approach of the Basic Law and Charter will ensure the best protection. See also Directive 95/46 and the GDPR, the German Civil Code (*Burgerliches Gesetzbuch* – BGB) and any further corresponding German or EU law. See also J Milker 'Karlsruhe im Luxemburger Gewand, aberdennoch eigenständig: Der Umgang mit Online-Archiven im Lichte der Beschlüsse des BVerfG vom 6.11.2019 (1 BvR 16/13 und 1 BvR 276/17)' *VerfBlog*, 29 November 2019, CM Wulff 'The right to be forgotten in Post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 264, and F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 933 – 934.

[663] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 96. Regarding the factors to be considered where rights are balanced, see *Von Hannover v Germany (no. 2)* [2012] ECHR 228 para 109 – 113, and *Fürst-Pfeifer v Austria* [2016] ECHR 431 para 12.

[664] *Grundgesetz für die Bundesrepublik Deutschland*.

[665] To clarify the formulation of the complainant's rights above: Article 1(1) of the Basic Law sets out that "human dignity shall be inviolable", and that it will be the duty of all State entities to respect and protect it. Article 1(1) of the Basic Law reads as follows: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority." Article 2(1) sets out the personal freedom to allow citizens to develop their personality insofar that it does not infringe the rights of others or offend the "constitutional order or moral law". Article 2(1) states: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." See the Basic Law and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 76 – 92. The rights to personality, include the protection of privacy and private life as well as includes the development of one's personality, affords protection from statements capable of damaging reputation, honour, public image and informational self-determination (para 90). Germany does not have a specific right to privacy set out in its Constitution, ie known as the Basic Law, but these two rights together form a base for the right to the protection of personal information in light of the right to privacy. See also BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 – *Volkszählungsurteil* para 42, and C DeSimone 'Pitting Karlsruhe against Luxembourg? German Data Protection and the contested implementation of the EU Data Retention Directive' (2010) 11(3) *German Law Journal* 291 at 292ffg.

freedom of the press.[666] The findings of the court in this matter were as follows:[667]

1 The Bundesverfassungsgericht found that the unaltered press reports on the crime formed a part of contemporary history. Access thereto was vital for research purposes. However, the crime was inextricably linked to the complainant's name. Furthermore, the public demand accurate and detailed reporting of criminal trials, and this includes identifying the persons involved, even where the personal details of the perpetrator and any true statements are incorporated, although they infringe on the rights of the person concerned.[668] The press plays a vital role in reporting accurately on contemporary events, especially since these reports will add to the historical collection of the courts and Germany. The court also acknowledged that truthful press reports may infringe on the personality rights of data subjects, however, access to events of contemporary history is vital.[669] In the present circumstances, the Bundeverfassungsgericht acknowledged that the press reports were all truthful and fact-based accounts of the extraordinary murders. In addition, the Bundesverfassungsgericht also acknowledged the seriousness of the crime. At the same time, however, it emphasised the plight of the complainant, ie the continued availability of information on the internet that was intricately linked to his name, which infringed his right to personality.[670]

2 The passage of time and the continued dissemination of the information can result in a burdensome infringement on the rights of the affected person:

---

[666] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 75, 78, 94 and 109 – 114. Article 5(1) of the Basic Law protects both freedom of expression and freedom of the press, securing the independence of the press to obtain information and disseminate articles and opinions covering private life. The court held that this includes the decision of the press to upload archived material making it permanently available to the public. It is the press' prerogative to decide what information is included and how to present it, including the presentation of archived information. See also *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) para 90 and *Times Newspapers Ltd v The United Kingdom (Nos. 1 & 2)* [2009] ECHR 451 para 27 and 45. Note also *Axel Springer AG v Germany* [2012] ECHR 227 para 83, where it was held that a person cannot use the Article 8 privacy rights in the Convention for protection of their rights, where their reputation was lost as a result of the individual's own actions, ie through the commission of a crime, etc. See A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 113.

[667] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 143.

[668] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 144.

[669] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 106 – 113, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 86 – 93.

[670] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 144. See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 263 – 265, the author does not even mention the crimes, and only deals with the how the court dealt with the plight of the complainant and the need to protect his rights to privacy and personality against the right of the general public to freedom of information.

(a) The passing of time is an important factor, because the crime and trial, in this instance, occurred 30 years ago.[671] Specifically with regards to the passage of time, the court considered the following: First, the frequency and ease of name-based searches, which are often conducted by acquaintances of the affected person. The results of name-based searches often provide a comprehensive overview of an individual. Where these results are dominated by a past crime and resultant conviction and sentence, it will be more difficult for the affected person to completely reintegrate into society.[672] Second, where name-based searches are carried out by acquaintances of the affected person, it may result in the affected person withdrawing from society, especially where the new acquaintances question them about the crime and subsequent conviction and sentence. Thus, the affected person is then constantly confronted with their past.[673] Third, the continued availability of the article could impede new beginnings and complete reintegration into society.[674] Fourth, if the information is at the top of the search results, it creates the impression that the press reports are the latest information on the applicant, despite the fact that they were published in 1982/1983.[675]

(b) Another important factor that needs to be considered was that after serving the sentence of imprisonment the complainant was released and did nothing to incite public interest in the matter. [676]

---

[671] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 146 – an important point to note is that the applicant had served his sentence.
[672] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 147 – 148.
[673] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 109 – 115, and 148. Compare with the remarks of Cameron J in *The Citizen 1978 (Pty) Ltd & others v McBride* 2011 (4) SA 191 (CC) paras 69 – 72 regarding crime and reconciliation, and the remarks of the main judgment (para 66) and dissenting opinion (para 14) in *LB v Hungary* [2021] ECHR 2 and the subsequent Grand Chamber judgment in *LB v Hungary* [2023] ECHR 239 regarding tax matters.
[674] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para1 101 – 109 and 148.
[675] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 115 – 142, and 149.
[676] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 150. The Bundesvervassungsgericht distinguished *Recht auf Vergessen I* from *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), which failed at both national and regional level. Although, similarly, the offenders sought protection from the publication of past crimes, they had committed, which were available in online media archives. Instead of merely obtaining the relief from the court they contacted the press, and used a public campaign to add weight to their plight. Furthermore, one of the defence lawyers had posted articles regarding the crime and predicament of the offenders on their website. However, the articles were only accessaible after a subscription was paid, ie a paywall. In *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) the court gave considerable weight to this aspect when it arrived at its decision. See *Recht auf Vergessen I* paras 151 – 152.

3 The Bundesverfassungsgericht held that a balanced approach needs to be used to protect the complainant from the general availability of the articles on the internet.[677] There are less restrictive methods,[678] other than the complete deletion or removal of the article, alternatively the redaction or alteration of the article, that could be considered in finding a solution that balances all rights involved. These methods may have an impact on how the articles are obtained, but there is no proof that they are unreasonable.[679]

The Bundesverfassungsgericht, unanimously, reversed the order granted by the Bundesgerichtshof and the matter was reverted back to the Bundesgerichtshof to consider a suitable order in light of their judgment.[680]

(iv) Family applying for the crime to be forgotten

In *ML v Slovakia*[681] the applicant was the son's mother. The son, whilst he was a Roman Catholic priest, was convicted of the sexual abuse of young children. The son subsequently, after his release from prison, committed suicide. The press, a year after his death, published

[677] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 112, 113 and 153.

[678] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 137, the Bundesverfassungsgericht held that it was not for it to decide on finding a suitable less restrictive, for that the lower courts are better equipped. In para 137 the court suggested that link to the text could appear further down on the results page of an internet search, and in para 153, the Bundesverfassungsgericht provided further ideas, such as digitally blacking out the name of the affected person. Although the court did not intend to provide any particular solutions, it did in both paras 137 and 153 (as well as throughout the judgment) stress that the solution must be reasonable (zumutbar) even if the solution is fairly technical, including where there are costs involved.

[679] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 153. Note: rights have direct vertical, and indirect (through respect, etc.) horizontal application: para 90ffg. Further the Bundesverfassungsgericht enjoined the ordinary courts to find innovative solutions to these technical issues – because situations and circumstances are constantly changing. Ordinary courts, during the balancing exercise, must remember that the solution must be both reasonable (zumutbar) and practical for the media houses and publishers to carry out (paras 136 – 142). This may include the development of suitable technology, depending on the circumstances of the matter.

[680] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 155 and 157. The Bundesverfassungsgericht, based on the approach and conclusions discussed above, found that it was unnecessary to deal with the applicability of the European Charter of Fundamental Rights (the Charter). The court noted that the German legislation under discussion was still to be harmonised with the relevant EU legislation. And there was nothing to suggest that the rights as balanced by the Bundesverfassungsgericht, discussed in light of the cases from the ECtHR, that suggested the Basic Law didn't provide the same level of protection, within Germany, as that of the Charter and the European Convention of Human Rights (the Convention). The court concluded that "the Basic Law does not call into question the level of protection of the Charter". See *Recht auf Vergessen I* para 154. See Article 52(3) of the Charter and the guarantees of the Convention. Article 52(3) provides for interpretation mechanisms for the Charter and how to deal with the Convention – see specifically Articles 7, 8 and 11 of the Charter. See also *Google LLC v CNIL* EU:C:2019:772.

The Bundesgerichtshof in BGH, Urteil vom 22. September 2020 - VI ZR 476/19, reverted the matter back to the Oberlandesgericht, Hamburg (Higher Regional Court, Hamburg) to decide what would be a reasonable solution in these circumstances. See also M Dollmann 'Streit um Nennung des Täters der Apollonia – Morde muss nochmal vor das OLG', dated 3. Nov 2020; available at *https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-streit-um-nennung-des-taeters-der-apollonia-morde-muss-nochmal-vor-das-olg*, (Accessed: 22 August 2022).

[681] *ML v Slovakia* [2021] ECHR 821.

articles containing scandalous information, and connecting the suicide of the son with the confessed sexual abuse.

The salient factors considered by the ECtHR were: the son was a priest, and a public figure. Hence, he should be more resilient to public criticism. However, that does not preclude him (or in this case his mother, the applicant) from successfully applying for the articles to be de-linked from his name when it is used as the search term.[682] Specifically, the son had been given a suspended sentence, which included a probationary programme, with which he had complied. Furthermore, the conviction was automatically expunged or "spent", based on the relevant laws of Slovakia.[683]

The ECtHR focused on the rights and freedoms as provided in the Convention in formulating its solution.[684] The ECtHR held that although convicted persons must take into account the loss of reputation, based on their own behaviour, they are not prevented from applying for their past criminal convictions to be de-linked/de-referenced, ie forgotten, especially when these are spent.[685] The ECtHR examined the speculative comments made by the press in relation to the son's death, and the adverse impact these had on the applicant's life as a mother, specifically her right to privacy.[686] The articles targeted the son's reputation, the ECtHR held, and this directly impacted her feelings as a mother, hence the conclusion that these comments affected her privacy. Furthermore, the ECtHR held that the articles did not add to the public debate.[687] The articles amounted to idle gossip rather than actual news. Furthermore, although the articles cited, amongst other sources, the bishop's office, the bishop's office denied ever having been approached on the matter.[688] Furthermore, the ECtHR

[682] *ML v Slovakia* [2021] ECHR 821 paras 37 – 39.
[683] *ML v Slovakia* [2021] ECHR 821 para 39.
[684] J Kokott & C Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) *International Data and Privacy Law* 222 at 222. Initially, and before the enactment of the Charter, the CJEU originally proclaimed on human rights in general terms, closely following the formulations in the Convention (J Kokott & C Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) *International Data and Privacy Law* 222 at 223), and has admitted that the Convention is a significant source of international human rights (S O'Leary 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 at 4). Furthermore, the ECtHR has discussed principles from the CJEU cases in its judgments (See generally *Big Brother Watch & others v The United Kingdom* [2021] ECHR 439. See also S O'Leary 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 at 5 – 6.
[685] *ML v Slovakia* [2021] ECHR 821 para 38. See also *Axel Springer AG v Germany* [2012] ECHR 227 para 83, and *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 87 – 88 and 100.
[686] *ML v Slovakia* [2021] ECHR 821 paras 40 – 48.
[687] *ML v Slovakia* [2021] ECHR 821 para 45, and 49 – 53.
[688] *ML v Slovakia* [2021] ECHR 821 para 47.

emphasised that the press's right to freedom of expression is there for the press to fulfil its democratic function to inform the public of news and events, whether in politics, sports, and court proceedings. The press cannot exploit the right to freedom of expression to release flamboyant claims about persons, which impact on their reputation, but most importantly on their right to privacy.[689] The ECtHR in this instance granted the request of the mother to have the information forgotten (ie de-linked) from the internet.

(v) Conclusion

The above cases illustrate that it will depend on the overall picture whether the information should be de-linked, or displayed in chronological order, on the results page of an internet search. The considerations are not always specific to criminal matters and may be applied to purely civil proceedings. It is useful to note that all the cases emphasised the passage of time, even if using a different viewpoint, as the main ground for granting the application. The seriousness of the crimes was merely one of the considerations. The courts focussed, not on victims or the family of the criminals,[690] but on the criminal's rights to privacy (including the personality rights of the criminal)[691] against the right of the general public to access the information.[692] Only in *ML v Slovakia*[693] did the court consider the right to be forgotten from the viewpoint of the family of the criminal. Whether victims, or family of criminals will be involved when criminals are applying for links to be removed from results pages, where their names are the search terms will, it is submitted, most likely depend on the circumstances of each individual case. Furthermore, victims who have enjoyed their anonymity may not now break their silence openly, and come to the fore to challenge the application, they simply wish to remain anonymous and thereby will remain silent.

The next topic deals with whether individuals that are confronted with information arising out of past or present actions that arise out of their professional duties, ie interviews, statements, etc. that are made on behalf of their employers, may have such information forgotten.

[689] *ML v Slovakia* [2021] ECHR 821 para 53.
[690] In *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) the family life in terms of privacy of the second applicant was mentioned, but from the view of the applicant and not a direct request from the family.
[691] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 144.
[692] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 20.
[693] *ML v Slovakia* [2021] ECHR 821.

(d) Statements, interviews, etc, made in a professional capacity

There are instances where data subjects, in line with their professional duties to their employer, will be required to make certain statements in defence of the employer, during interviews and press releases. Where the name of the data subject is typed into the search engine tool, the links displayed on the results page will include links to these interviews or press releases, etc. Data subjects may find this damaging to their reputation, especially where the employer's reputation has fallen into disrepute with the general public.

In *Recht auf Vergessen II* the issue was whether a person giving an interview in their professional capacity could ask that it be forgotten.[694] The facts, briefly, were as follows. The complainant, in her capacity as managing director of a company, gave an interview for the NDR[695] broadcasting corporation's *Panorama* show, titled "Dismissal: the dirty tricks of employers". Towards the end of the segment, a former employee is interviewed accusing the complainant of unfair dismissal based on the establishment of an employee work council (Betriebsrat).[696] A transcript of the broadcast was uploaded on the NDR website. This link appears first on the list of the search results where the complainant's name is typed into the search tool. The complainant claimed that her general rights of personality and self-determination had been violated. The linked transcript set out false assertions, was misleading and she claimed that she had never played 'dirty tricks' to unfairly dismiss employees. The

[694] Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*. For a brief overview of the judgment see *Hurbain v Belgium* [2023] ECHR 948 paras 122 – 126, J Milker 'Karlsruhe im Luxemburger Gewand, aberdennoch eigenständig: Der Umgang mit Online-Archiven im Lichte der Beschlüsse des BVerfG vom 6.11.2019 (1 BvR 16/13 und 1 BvR 276/17)' *VerfBlog*, 29 November 2019. Note: An employee council or work council is an employee organised council that is directly involved in the company's decisions that affect the working conditions of the employees, eg, working hours, etc. and they also present to management the employees' concerns – see generally 'Der Betriebsrat: Was Beschäftigte und Betriebsräte wissen müssen', dated 23 September 2021. *https://www.verdi.de/themen/arbeit/der-betriebsrat* (Accessed: 28 September 2021) and PA Willers 'Betriebsrat – einfach erklärt!' *https://www.betriebsrat.com/wissen/betriebsrat* (Accessed: 28 September 2021). For a detailed discussion, with a comparison with the EU law, especially with regards to the judgments of the CJEU, see R Hofmann, A Heger & T Gharibyan 'Die Wandlung des Grundrechtsschutzes durch das Bundesverfassungsgericht – *Recht auf Vergessen I* und *II* als "*Solange III*"?' (2019) 102(4) *KritV Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* 277 – 292, D Burchardt 'Backlash against the Court of Justice of the EU? The recent jurisprudence of the German Constitutional Court on EU fundamental rights as a standard of review' (2020) 21 *German Law Journal* 1 – 18, M Wasser *You're Forgiven but not Forgotten: The coherence of the right "to be forgotten" in Germany and the EU* (unpublished bachelor thesis (partial-fulfilment)), University of Twente, the Netherlands, 2 July 2020), CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 265 – 268, A Bobić 'Developments in the EU-German judicial love story: The *Right to Be Forgotten II*' (2020) 21(Special Issue) *German Law Journal* 31 – 39, and F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 933 – 934.

[695] Norddeutscher Rundfunk (NDR) – a broadcasting service in Germany, with a focus on the northern German states, see generally *https://www.ndr.de/* (Accessed: 23 August 2022).

[696] 'Der Betriebsrat: Was Beschäftigte und Betriebsräte wissen müssen', dated 23 September 2021. *https://www.verdi.de/themen/arbeit/der-betriebsrat* (Accessed: 28 September 2021) and PA Willers 'Betriebsrat – einfach erklärt!' *https://www.betriebsrat.com/wissen/betriebsrat* (Accessed: 28 September 2021).

information vilified her and violated her private life.

The complainant, in her application to the Bundesverfassungsgericht included a request for a preliminary ruling from the CJEU in terms of Article 267(3) of the Treaty on the Functioning of the European Union.

The Bundesverfassungsgericht held that there was no need to refer the matter to the CJEU, as the issues didn't require an interpretation of the relevant EU legislation, and argued that the issues had been sufficiently clarified within CJEU judgments.[697] The Bundesvervassungsgericht unanimously dismissed the constitutional complaint for the following reasons:

1 The Bundesverfassungsgericht confirmed that the interests and business activities of search engines must be balanced against the complainant's rights in terms of Articles 7 and 8 of the Charter.[698] Furthermore, the complainant need not first approach the content provider to remove the information.[699] Each matter will be decided on its own facts. The Bundesverfassungsgericht referred to the judgments of the CJEU in *Google*

[697] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 32 – 84 and 137. See also Article 52(3) of the Charter – which requires that the judgments of the CJEU are read in light of those from the ECtHR (European Court of Human Rights) judgments. See also *A v B and others* EU:C:2014:2195 from para 39. See *Recht auf Vergessen II* para 67, where the Bundesvervassungsgericht held the first sentence of Article 23(1) of the Basic Law permits the Bundesverfassungsgericht to apply "EU law within the framework of its responsibility with regard to European integration." The relevant part of Article 23(1) of the Basic Law reads:

> "With a view to establishing a united Europe, the Federal Republic of Germany shall participate in the development of the European Union that is committed to democratic, social and federal principles, to the rule of law, and to the principle of subsidiarity, and that guarantees a level of protection of basic rights essentially comparable to that afforded by this Basic Law."

Thus, the Bundesverfassungsgericht is able, due to its close cooperation with the CJEU, to review matters in terms of the Basic Law as well as the Charter. For a short discussion see CM Wulff 'The right to be forgotten in Post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 263 – 268, and A Bobić 'Developments in the EU-German judicial love story: The *Right to Be Forgotten II*' (2020) 21(Special Issue) *German Law Journal* 31 at 34 – 37, where the relationship between the Bundesverfassungsgericht and the CJEU is detailed. A similar approach was discussed, although the facts and issues are distinguishable, in BVerfG, Urteil des Zweiten Senats vom 5. Mai 2020 – 2 BvR 859/15, 2 BvR 980/16, 2 BvR 2006/15, 2 BvR 1651/15, see also I Feichtner 'The German Constitutional Court's PSPP judgment: Impediment and impetus for the democratization of Europe' (2020) 21 *German Law Journal* 1090 – 1103.

[698] Search engines are able in terms of Article 16 of the Charter to protect their interests, which provides for the freedom to conduct a business, and not in terms of the Article 11, which provides for freedom of the press. It will be their interests under Article 16 that will be balanced against the data subject's rights in terms of Article 7 (privacy) and Article 8 (data protection). See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267.

[699] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 111 – 122, and 138, and *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 from para 34ffg; *GC & others v CNIL* EU:C:2019:773 paras 68 and 77; and *Google LLC v CNIL* EU:C:2019:772 para 44.

Spain,[700] *GC & others*,[701] and *Google LLC v CNIL*,[702] where this approach was confirmed, ie that the data subject may first approach the operator of the search engine to de-link the articles from the results page where a search is done using the data subject's name. The data subject need not first approach the content provider to have the information removed. As confirmed in the three CJEU cases, the information is still available but only more difficult to locate.[703]

2 All fundamental rights in a matter must be taken into account, that includes the fundamental rights of the content providers, all fundamental rights outlined in the Charter, as well as the decisions and findings from the CJEU and ECtHR.[704] This follows from the decision of *Google Spain* and subsequent decisions.[705] The CJEU held that the freedom of expression of the public must be included in the balancing exercise. If it is possible to deal with a non-specific public and their interests, then the matter before the court must all the more consider the rights or interests of content providers. It is the content providers' freedom of expression that is directly and indirectly affected. The balancing exercise will also include the Charter rights that are applicable to search engines, keeping in mind the data processing principles as provided in Directive 95/46.[706] The de-linking of information has a direct impact on the content provider's rights, as certain platforms for the dissemination of information are no longer available.[707]

The Bundesverfassungsgericht distinguished the present matter from those of the CJEU,[708] and

[700] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 from para 34ffg.
[701] *GC & others v CNIL* EU:C:2019:773 paras 68 and 77.
[702] *Google LLC v CNIL* EU:C:2019:772 para 44.
[703] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 138, see also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267.
[704] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 114 – 122, and 139. See also *Promusicae v Telefónica de España SAU* EU:C:2008:54 para 65ffg; *Land Nordrhein-Westfalen v Renckhoff* EU:C:2018:634 paras 41 and 42 and *Von Hannover v Germany (no. 2)* [2012] ECHR 228 para 106.
[705] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para140, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 from para 21ffg; *GC & others v CNIL* EU:C:2019:773 para 57ffg; and *Google LLC v CNIL* EU:C:2019:772 para 40ffg.
[706] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 120ffg and 140, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 74, 75 and 76. See also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 114.
[707] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 120 and 140. See also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 114. See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 266 – 267.
[708] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras

held that the current constellation of facts did not call for an interpretative clarification from the CJEU, as they did not give precedence to the complainant's right of personality. The facts, before a court, are the determining factor in deciding whose rights have precedence. The Bundesverfassungsgericht pointed out that in *Google Spain* the right of freedom of expression was not given much consideration as the problematic publication was a legal publication.[709] In *GC & others* the rights of the complainants were given a special preference because they fell under the special categories of data that may negatively impact the personality of the complainants.[710] Before weighing up the respective rights within *Recht auf Vergessen II*, the Bundesverfassungsgericht emphasised that all rights within the Charter are accorded equal weight.[711] In this matter, the complainant's rights in Articles 7 (privacy) and 8 (data protection), were weighed against the search engine's rights in terms of Article 16 of the Charter, which provides for the freedom to conduct a business and pursue economic interests, as well as the rights of an unspecified public to information and the freedom of expression of the content providers.[712] Also, the complainant has the right to freedom of expression to make certain statements.[713] Search engines, do not operate in the same was as publishers. They simply use the information to further their business interests which, as held in *Google Spain*, means that they are not entitled to the protections of a free press.[714] The court acknowledged that the right to de-link outweighed the search engine's right to pursue economic interests.[715] The Bundesverfassungsgericht concluded that although the interview was consented to as a part of

123 – 136 and 141, see generally *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *GC & others v CNIL* EU:C:2019:773; and *Google LLC v CNIL* EU:C:2019:772.

[709] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141, see *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[710] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141, *GC & others v CNIL* EU:C:2019:773. See Articles 8(1) and (5) of Directive 95/46.

[711] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141, note also the discussion in para 63ffg and later summarised in para 121. See also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 170. *Von Hannover v Germany (no. 2)* [2012] ECHR 228 para 106, *Węgrzynowski and Smolczewski v Poland* (European Court of Human Rights) application no. 33846/07 (16 July 2013) para 56, *Delfi AS v Estonia* [2015] ECHR 586 (for a comment on *Delfi AS v Estonia* see N Cox, '*Delfi v. Estonia*: Privacy protection and chilling effect', *VerfBlog*, 19 June 2015, and. *Fürst-Pfeifer v Austria* [2016] ECHR 431 para 38.

[712] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 120 – 122 and 141. See also *Fuchsmann v Germany* [2017] ECHR 925 para 32ffg. See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 266 – 267.

[713] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141.

[714] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 105, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *GC & others v CNIL* EU:C:2019:773 para 85, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.

[715] CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.

her professional capacity, the contents would impact on the complainant's social sphere. However, the complainant had consented to the interview, which at the date of judgment was seven years previously, and that was not considered a long enough timespan, and the topic was still relevant within German society.[716] The Bundesverfassungsgericht thus refused the application.

(e) Processing special categories of data

(i) Introduction

Special categories of data, or sensitive data/information,[717] are data that most people want to keep out of the public eye, due to the nature of the data. Special categories of data include information about medical records, sexual orientation and sex life, religious and philosophical beliefs, opinions and political views, racial and/or ethnic background as well as trade-union

[716] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 134, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268. *Hurbain v Belgium* [2023] ECHR 948 para 11 confirmed that where a discussion is likely to add to the public debate, the data will not be de-linked or de-referenced, ie "forgotten".

[717] The Protection of Personal Information Act 4 of 2013 refers to sensitive data, and these have the same or similar description as special categories of data in Article 8 of Directive 95/46. In light of the matters before the CJEU, the relevant parts of Article 8 of Directive 95/46 read as follows:

> "1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
>
> 2. Paragraph 1 shall not apply where:
>
> *(a)* the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
>
> *(b)* processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
>
> *(c)* processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
>
> *(d)* processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
>
> *(e)* the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
>
> . . .
>
> 5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
>
> Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority."

membership. Also included are criminal records, and civil cases, such as sequestrations.[718] The CJEU dealt with this issue extensively in *GC, AF, BH, ED v CNIL* (*GC & others*).[719]

The facts of this case were as follows. Each of the four applicants, GC, AF, BH and ED, filed a separate request with Google to de-list links to articles, videos, etc. that appeared on the results page where their respective names were used as the search terms. Google rejected the requests.[720] The CJEU took the opportunity, not only to deal with the issues in terms of Directive 95/46 (under which the application was launched), but also to pronounce and provide guidance on the newly promulgated GDPR.[721]

The facts of the each individual case are as follows: GC requested the de-linking of a satirical photomontage that was uploaded on YouTube in 2011. The montage depicted her with a mayor, under whom she had served as his head of the cabinet. The montage portrayed them as having had an affair, and had been uploaded during an election, for which GC was a candidate. She claimed that the montage negatively impacted on her political career. At the time of the request, GC was no longer serving as the head of the cabinet, and neither was she a candidate in an upcoming election.[722]

AF applied for links to an article, dated 2008, in a daily newspaper to be de-listed. The article referred to the suicide of a member of the Church of Scientology, for which AF had worked as their public relations officer. The suicide was a result of the mental manipulation of

[718] It is submitted that other civil cases that should be considered as special categories of data include divorce proceedings, family matters, personal injury claims, retrenchment, tax matters, etc. This is not a closed list. These matters have not appeared in the cases that are under discussion in this chapter. However, the considerations would equally apply where a person is applying for the information to be forgotten. The ECtHR dealt with an issue concerning the display of the personal tax information of the spouse of a high-ranking official implicated in a corruption charge in the case of *Samoylova v Russia* [2021] ECHR 1067. The court in *Samoylova v Russia* held that although corruption, especially the corruption charges and trials of high-ranking officials, is a matter of public interest, only the actual official's details may be displayed, not those of the spouse if they are not directly implicated by the authorities. See R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 268 – 270. Note that in *GC & others v CNIL* EU:C:2019:773, three of the four applicants all had a matter involving their past employment and the further development of their careers.

[719] *GC AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773. See *Hurbain v Belgium* [2023] ECHR 948 paras 81 – 84, and N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 at 1674.

[720] *GC & others v CNIL* EU:C:2019:773 para 24.

[721] *GC & others v CNIL* EU:C:2019:773 para 13. General Data Protection Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 repealed Directive 95/46, and came into effect on 25 May 2018. The judgment in *GC & others v CNIL* EU:C:2019:773 and *Google LLC v CNIL* EU:C:2019:772 are dated 24 September 2019 – after the promulgation of the GDPR. See also Y Miadzvetskaya & G van Calster G 'Google at the Kirchberg Dock. On delisting requests, and on the territorial reach of the EU's GDPR.' (2020) 6(1) *European Data Protection Law Review* 143 – 151.

[722] *GC & others v CNIL* EU:C:2019:773 para 25.

the member. In the article, AF had given the author of the article the Church of Scientology's version of events and provided various comments. AF no longer worked in that position.[723]

BH requested the de-referencing of articles referring to court proceedings against him that had been opened after an investigation implicated him alongside other political personalities and businessmen with regard to anomalies in political party funding. BH was discharged at the close of the proceedings, however, the links that appeared were related to the opening of the investigation and the court proceedings, and not to the outcome.[724]

Lastly, ED[725] requested the de-referencing of links "leading to two articles published in" two periodicals which reported on a criminal trial in which he was convicted of sexually assaulting children younger than 15 years old and sentenced to seven years imprisonment plus a 10-year rehabilitative programme. One article contained "several intimate details relating to ED that were revealed at the hearing."[726]

The issues in *GC & others* that will be discussed in light of these facts pertain, first, to the duties imposed on search engine operators and/or controllers by Directive 95/46 and the GDPR; second, to de-linking/de-referencing/de-listing in light of the legislative exceptions; and third, to the order in which results must be displayed on the results page.[727]

(ii) Duties imposed on search engine operators and/or controllers

The CJEU, once again emphasised that search engine operators are controllers of personal data because they process personal data (which includes indexing and storing), even where this occurs automatically, as discussed in *Google Spain*.[728] In terms of Article 8(1) of Directive 95/46, it is prohibited to process data that reveals the "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of data concerning health or sex life."[729] Article 8(2) provides for exceptions to the prohibition.[730] It is clear from the wording of Directive 95/46 that the provisions will apply, subject to the

[723] *GC & others v CNIL* EU:C:2019:773 para 26.
[724] *GC & others v CNIL* EU:C:2019:773 para 27.
[725] Ie the fourth applicant in the combined case.
[726] *GC & others v CNIL* EU:C:2019:773, the facts relevant to this discussion appear at para 28.
[727] *GC & others v CNIL* EU:C:2019:773.
[728] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 35 – 38, and 41.
[729] *GC & others v CNIL* EU:C:2019:773 para 39. Article 9 of the GDPR is worded as follows:

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[730] *GC & others v CNIL* EU:C:2019:773 para 41. Note Article 8 was incorporated into the GDPR, with some variations as Articles 9 and 10.

exceptions, with respect to special categories of data.[731] This is important to note, as one of the issues[732] from the Conseil d'État, was concerned with the compliance of a search engine operator with the requisites of Article 8, where data was uploaded on the internet by third parties, and is processed by the operator of the search engine.[733]

The CJEU held that both Directive 95/46 and the GDPR apply to operators of search engines. In *Google Spain* it was held that data that is or has become incompatible with Directive 95/46 (this would apply to the GDPR) must be de-listed from the search results, where the data subject's name has been used as the search terms. This is based on the protection of the data subject's fundamental rights to privacy and personal data. The responsibilities that search engine operators have, in terms of Article 8 of Directive 95/46,[734] mean that sensitive data, even on a third party's webpage, and may not be processed further than necessary.[735] What is important to note is that the prohibitions and restrictions on the processing of personal data, in both Directive 95/46 and the GDPR, must be adhered to by those carrying out the processing (ie the controllers and/or the operators of search engines).[736]

(iii) De-linking and exceptions

The issue under this heading,[737] and in light of the question answered above, from the Conseil

---

[731] *GC & others v CNIL* EU:C:2019:773 para 42.

[732] *GC & others v CNIL* EU:C:2019:773 para 31. Incidentally, this was the first question from the Conseil d'Etat, and it reads as follows:

> "Having regard to the specific responsibilities, powers and capabilities of the operator of a search engine, does the prohibition imposed on other controllers of processing data caught by Article 8(1) and (5) of Directive 95/46, subject to the exceptions laid down there, also apply to this operator as the controller of processing by means of that search engine?"

[733] *GC & others v CNIL* EU:C:2019:773 paras 34 and 38.

[734] And Articles 9 and 10 of the GDPR.

[735] *GC & others v CNIL* EU:C:2019:773 paras 46 – 47.

[736] *GC & others v CNIL* EU:C:2019:773 para 42. See the remarks by the CJEU in *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833 para 95.

[737] *GC & others v CNIL* EU:C:2019:773 para 31. This was the second question from the Conseil d'État, and was worded as follows:

> "If Question 1 should be answered in the affirmative:
>
> [(a)] Must Article 8(1) and (5) of Directive 95/46 be interpreted as meaning that the prohibition so imposed on the operator of a search engine of processing data covered by those provisions, subject to the exceptions laid down by that directive, would require the operator to grant as a matter of course the requests for de-referencing in relation to links to web pages concerning such data?
>
> [(b)] From that perspective, how must the exceptions laid down in Article 8(2)*(a)* and *(e)* of Directive 95/46 be interpreted, when they apply to the operator of a search engine, in the light of its specific responsibilities, powers and capabilities? In particular, may such an operator refuse a request for de-referencing, if it establishes that the links at issue lead to content which, although comprising data falling within the categories listed in Article 8(1), is also covered by the exceptions laid down by Article 8(2) of the directive, in particular points *(a)* and *(e)*?
>
> [(c)] Similarly, when the links subject to the request for de-referencing lead to processing of personal data carried out solely for journalistic purposes or for those of artistic or literary expression, on

d'État, contained three parts. Essentially, they were asking: (a) Would an operator of a search engine, as a matter of recourse, have to grant the request to de-link web pages, where they process personal data, covered by the provisions of Article 8(1) and (5) (noting the exceptions)? (b) This question, relating to the operator's responsibilities and exceptions, has two parts: first, how is Article 8(2)*(a)* and *(e)* to be interpreted in light of the responsibilities, powers and capabilities of an operator? Secondly, may the operator refuse to accede to a de-linking request where the data on the third-party website falls into Article 8(1), but is included in the exceptions specified in Article 8(2)*(a)* and *(e)*? (c) Lastly, where the personal information was originally published in terms of the journalistic or artistic freedom, provided in Article 9 of Directive 95/46, would the operator be able to refuse a de-linking request, based on Article 9?[738]

The CJEU summarised its approach in *Google Spain* and stated that operators are obliged, in terms of Articles 12*(b)* and 14*(a)* of Directive 95/46, to comply with the requests to de-reference links to personal data on third party websites, even if the data is not, later or simultaneously, removed by the third party.[739] This includes information that was lawfully published.[740] Further, the economic interests of the search engine and the public's right to information cannot exceed the protected Charter rights of privacy and data protection.[741] Directive 95/46 requires that data be published only for as long as it is absolutely necessary,[742] and thereafter it must be removed by the controller, without undue delay.[743]

The data subject's explicit consent is an important factor, unless it is prohibited to process the data.[744] Strictly speaking, the search engine should obtain the consent of the data

---

> which basis, in accordance with Article 9 of Directive 95/46, data within the categories mentioned in Article 8(1) and (5) of the directive may be collected and processed, must the provisions of Directive 95/46 be interpreted as allowing the operator of a search engine, on that ground, to refuse a request for de-referencing?"

There was a third question, however, that was dependent on the first question, being answered in the negative. As the first question received a positive answer, there will be no need to deal with the third question of the Conseil d'État – see *GC & others v CNIL* EU:C:2019:773 paras 31 and 70.

[738] *GC & others v CNIL* EU:C:2019:773 paras 31 and 49.

[739] *GC & others v CNIL* EU:C:2019:773 para 52; *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88. *GC v CNIL* para 54 – 55 sets out the following: Article 17 of the GDPR, which is titled the "Right to erasure (right to be forgotten)", similarly to Articles 12*(b)* and 14*(a)* of Directive 95/46, requires that data only be published for as long as it is absolutely necessary, and thereafter must be removed by the controller, without undue delay.

[740] *GC & others v CNIL* EU:C:2019:773 para 52; *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88.

[741] *GC & others v CNIL* EU:C:2019:773 para 53; *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317para 99.

[742] *GC & others v CNIL* EU:C:2019:773 para 54.

[743] *GC & others v CNIL* EU:C:2019:773 para 55.

[744] *GC & others v CNIL* EU:C:2019:773 para 61. Compare with *CN v European Parliament* EU:T:2015:926 para 94.

subject, where, in terms of their business operations, they process the data subject's personal data. However as correctly accepted by the CJEU, that would be impossible.[745] Merely based on the fact that the data subject is making the de-linking/de-referencing request means that the data subject indicates that they have withdrawn their consent.[746] Where the information is made public, in terms of Article 8(2)*(e)*,[747] the data subject will need to apply to both the search engine as well as the publisher of the website for its removal.[748]

Data processing by a search engine must be lawful, in terms of the relevant legislation, if not the data subject may request the de-linking of the information.[749] Essentially, an operator of a search engine will need to balance, based on the relevant facts of each matter, the conflicting rights between the public and the data subject.[750] Important factors to be taken into account include the special categories of data,[751] and how the links on the results page impact the fundamental rights protected in the Charter.[752] This is problematic as the court placed the responsibility for balancing competing rights on the search engines, which is the work of legal experts. In other words, non-legally trained persons, must now decide how best to balance the competing rights and interests between individuals and groups. Generally, the staff employed specialise in the services provided by search engines, and they are now required to decide on legal issues without the requisite training.[753]

The CJEU answered the questions from the Conseil d'État as follows: (a) generally in terms of Article 8 of Directive 95/46, and in light of the exceptions provided in the legislation, an operator must accede to a request to de-link.[754] (b) Where the data to be de-linked falls into the special categories of data set out in Article 8(2), the operator may refuse the de-link request, "provided that it satisfies all the other conditions of lawfulness" in terms of the legislation. However, the data subject has the right to object, in terms of Article 14, but these objections are dependent on the individual circumstances of the data subject.[755] And, (c) the court held,

[745] *GC & others v CNIL* EU:C:2019:773 para 62.
[746] *GC & others v CNIL* EU:C:2019:773 para 62.
[747] Note in terms of Article 8(2)*(e)* of Directive 95/46, and Article 9(2)*(e)* of the GDPR.
[748] *GC & others v CNIL* EU:C:2019:773 para 63.
[749] *GC & others v CNIL* EU:C:2019:773 paras 64 – 65.
[750] *GC & others v CNIL* EU:C:2019:773 para 66.
[751] *GC & others v CNIL* EU:C:2019:773 paras 64 – 65. The special categories are an important aspect of the enquiry.
[752] *GC & others v CNIL* EU:C:2019:773 para 68.
[753] See the comments made by S De Conca '*GC et al v CNIL*: Balancing the right to be forgotten with the freedom of information, the duties of a search engine operator' (2019) 5 *European Data Protection Law Review* 561 at 563, and JS Van Oyen, M Lange & S Kreinsen, 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 at 306 – 307.
[754] *GC & others v CNIL* EU:C:2019:773 para 69.
[755] *GC & others v CNIL* EU:C:2019:773 para 69.

depending on the circumstances of each matter, that the operator of the search engine must, in a de-linking/de-referencing application, consider the impact of the link on the data subject's rights to privacy and data protection.[756] However, the data subject's rights must be balanced against the public's right to information and expression.[757] Based on the outcome of the balancing exercise the operator must conclude whether the link is strictly essential on the results page, where the data subject's name is the keyword used in the search.[758]

(iv) Operators of search engines to set out the current position

In *GC & others,*[759] this last issue was specifically in regard to how information is displayed on a results page, specifically, for both BH and ED, the acquittal or conviction, were displayed further down on the results page and the criminal investigations at the top, which, made it seem as though the investigations were current. Put differently, the information at the top of the results page does not set out the actual current circumstances of the accused.[760]

Articles 8 and 9 of Directive 95/46 relate to the processing of special categories of data. Criminal matters are set in Article 8(5) of Directive 95/46, which states that data in relation "to offences, criminal convictions and security measures" may be processed in terms of suitable safeguards, by the national authority, with certain exceptions.[761]

The Conseil d'État wanted guidance where the information displayed relates to the pending proceedings and subsequent conviction, however, the information is no longer current, and the articles contain intimate details of the former accused.[762]

---

[756] Ie Articles 7 and 8 of the Charter.
[757] Protected by Article 11 of the Charter.
[758] *GC & others v CNIL* EU:C:2019:773 para 69.
[759] *GC & others v CNIL* EU:C:2019:773. There were ultimately four questions referred to the CJEU for a preliminary hearing, by the Conseil d'État (Council of State, France). Only the question relevant to this topic will be discussed here. It happened to be the fourth question which related to the consequences of publishing about a criminal trial and subsequent conviction. The other three questions will be set out below in their respective topic, namely the processing of sensitive personal data will be set out below. See also S De Conca, '*GC et al v CNIL*: Balancing the right to be forgotten with the freedom of information, the duties of a search engine operator' (2019) 5 *European Data Protection Law Review* 561 at 564, and 566 – 567.
[760] In *GC & others v CNIL* EU:C:2019:773.
[761] Article 8(5) of Directive 95/46 reads as follows (quoted here again for convenience):

> "Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
> Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority."

[762] *GC & others v CNIL* EU:C:2019:773 paras 31 and 71. This was the fourth question that was referred to the CJEU by the Conseil d'État, and it reads as follows:

> "Irrespective of the answer to be given to Question 1:

The CJEU in considering this issue, set out that there are special restrictions regarding the display of information in relation to convictions and court proceedings. *Google Spain* was an example of once lawfully published information later becoming unlawful with the lapse of time.[763] The CJEU made specific reference to the importance of striking the balance between the rights of the individual to data protection and privacy and the public's right to receive information, which is a part of the essential functions played by the press in a democratic society.[764] The balancing exercise is the responsibility of the operator of the search engine,[765] in light of the circumstances before it.[766] Even where the operator decides that the link must still be included in the list of search results, the data subject is not without a remedy, on a de-linking request, the operator of a search engine is required, where the information in question is regarding past court proceedings, to display the latest information first, and the information complained of must appear later in the chronological list of results.[767]

In conclusion, the CJEU held that, although the rights of the data subject in terms of Articles 7 and 8 of the Charter[768] override the general public's right in Article 11,[769] the operator, must accede to the de-linking request.[770] Alternatively, depending on the circumstances, the operator must ensure that the information regarding the past or current legal proceedings, must be displayed in chronological order, ie the current position first and older or outdated information later on the results page.[771] This includes data that relates to "offences"

> [(a)] whether or not publication of the personal data on the web page at the end of the link at issue is lawful, must the provisions of Directive 95/46 be interpreted as:
>
> – requiring the operator of a search engine, when the person making the request establishes that the data in question have become incomplete or inaccurate, or are no longer up to date, to grant the corresponding request for de-referencing;
>
> – more specifically, requiring the operator of a search engine, when the person making the request shows that, having regard to the conduct of the legal proceedings, the information relating to an earlier stage of those proceedings is no longer consistent with the current reality of his situation, to de-reference the links to web pages comprising such information?
>
> [(b)] Must Article 8(5) of Directive 95/46 be interpreted as meaning that information relating to the investigation of an individual or reporting a trial and the resulting conviction and sentencing constitutes data relating to offences and to criminal convictions? More generally, does a web page comprising data referring to the convictions of or legal proceedings involving a natural person fall within the ambit of those provisions?"

[763] *GC & others v CNIL* EU:C:2019:773 paras 71 – 74. See also J Globocnik 'The right to be forgotten is taking shape: CJEU judgments in *GC and others* (C-136/17) and *Google v CNIL* (C-507/17)' (2020) *GRUR International* 1 at 5 – 6.

[764] *GC & others v CNIL* EU:C:2019:773 para 76.

[765] See the answers provided to question 2, set out later in the judgment.

[766] *GC & others v CNIL* EU:C:2019:773 para 77.

[767] *GC & others v CNIL* EU:C:2019:773 para 78.

[768] Article 7 is the right to privacy and Article 8 is the right to the protection of personal data.

[769] Article 11 provides for the right to freedom of expression and information.

[770] *GC & others v CNIL* EU:C:2019:773 para 79.

[771] *GC & others v CNIL* EU:C:2019:773 para 79. See also S De Conca '*GC et al v CNIL*: Balancing the right to be forgotten with the freedom of information, the duties of a search engine operator' (2019) 5 *European Data*

and "criminal convictions" in terms of the requirements of Article 8(5) of Directive 95/46.[772]

(v) Conclusion

To conclude this case discussion, the CJEU concluded that the provisions of Article 8 of Directive 95/46 apply to search engine operators, subject to the exceptions provided within the directive. In light of their responsibilities when they process the personal data, including sensitive data, of data subjects, irrespective of whether this occurs automatically or not. They must comply with a request to de-link/de-reference, when requested by the national data protection authority. Furthermore, the operator of a search engine may refuse to comply with the de-linking/de-referencing request if the data subject has disclosed the sensitive information or has consented to its processing. However, the data subject may still have the right to object, as provided in Article 14 of Directive 95/46, where they have compelling personal reasons.

The operator of a search engine must balance the data subject's fundamental rights to privacy and data protection with the general public's right to know when there is a request to de-link/de-reference sensitive information. Lastly, if the operator of a search engine, does not comply with a de-linking/de-referencing request, they must ensure that the links on a results page are displayed in chronological order, ie the latest information should appear on the first page of the results with older information further down the first page or on subsequent pages. This is to ensure that the most current position of the data subject is accessed first.[773]

(f) Anonymisation and deletion of archives, and the right to be forgotten

(i) Introduction

There is some overlap with the discussion relating to criminal matters, because the three cases discussed here all originate out of criminal investigations and proceedings. The reason for this separate discussion is that the direct anonymization or deletion of archives is a far more drastic step than merely de-linking/de-referencing links. The anonymisation of the archives, specifically online media archives, means an alteration in the original text and may include replacing the data subject's name with an "X", if the data subject's initials aren't used. The cases set out below highlight a different consideration where courts are not merely applying

Protection Law Review 561 at 564 and 566 – 567.

[772] *GC & others v CNIL* EU:C:2019:773 para 79. See also S De Conca '*GC et al v CNIL*: Balancing the right to be forgotten with the freedom of information, the duties of a search engine operator' (2019) 5 *European Data Protection Law Review* 561 at 564 and 566 – 567.

[773] See generally the order at the end of *GC & others v CNIL* EU:C:2019:773.

the right to be forgotten in light of de-linking links on a results page, but requiring that the protection of privacy includes the anonymisation of the data subject.[774] Another option that was considered in respect of archives was the deletion of the information, this would mean that the information would no longer be available online, even in altered form.

Three cases will be discussed in this section. Two cases discussed anonymizing the data subject's details, and both originated from the ECtHR, namely *ML & WW v Germany* (*ML & WW*),[775] and *Hurbain v Belgium* (*Hurbain*).[776] The third case, also from the ECtHR, considered deletion of the information, namely *Biancardi v Italy* (*Biancardi*).[777]

(ii) Anonymisation

The facts in *ML & WW v Germany*,[778] were as follows: the applicants in this matter are half-brothers, who were convicted and sentenced for murder in 1993. They were released on parole

[774] S Schweda 'Right to be forgotten also applies to online news archive, Supreme Court Rules' (2015) 1 *European Data Protection Law Review* 301 – 304, AN Vavra 'The right to be forgotten: An archival perspective' (2018) 81(1) *The American Archivist* 100 – 111, M Elliot *et al* 'Functional anonymisation: Personal data and the data environment' (2018) 34 *Computer Law & Security Review* 204 – 221, E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 – 265, L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808 1 at 2, and EM Weitzenboeck, P Lison, M Cyndecka & M Langford 'The GDPR and unstructured data: Is anonymization possible' (2022) 12(3) *International Data Privacy Law* 184 at 191 – 196. Regarding the benefits of anonymising and pseudomysing personal data see SY Esayas 'The role of anonymisation and pseudonymisation under the EU data privacy rules: Beyond the "all or nothing" approach' (2015) 6(2) *European Journal of Law and Technology* 1 – 28.

[775] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).

[776] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), this is a judgment from the ECtHR's Third Chamber, which was upheld by the Grand Chamber in *Hurbain v Belgium* [2023] ECHR 948. The Grand Chamber in *Hurbain v Belgium* [2023] ECHR 948 in paras 94 – 132 provides an overview of how the national high courts (from the contracting states to the ECtHR) regarding anonymisation or deletion of information made available in online archives, and how the national courts balanced the right to be forgotten with freedom of expression.

[777] *Biancardi v Italy* [2021] ECHR 972.

[778] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018). For a comment in this case see E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 – 265. Compare with *IVT v Romania* [2022] ECHR 189 where a minor child gave an unaccompanied interview, without the necessary consent from the parents or school, regarding the accidental death of a schoolmate. The interview was in front of the school. The court applied and adapted the criteria from *Axel Springer AG v Germany* [2012] ECHR 227 paras 89 – 95 where the minor child's right to a private life is at issue, and held when information regarding a child's identity is disclosed, this has the potential to risk their well-being and dignity more severely than in comparison to adults, "given their greater vulnerability, which attracts special legal safeguards" (see R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 271). The court found that due to the young age and lack of infamy of the child, and that the interview added little or nothing to the public debate on the issue, and further that courts, parents, teachers, authorities, etc. all have an active responsibility to protect a minor child's private life (in terms of Article 8 of the Convention). See also R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 270 – 271.

in 2007 and 2008, respectively.[779] During their time in prison as well as after their release on parole and throughout the proceedings, they contacted the press to draw attention to their case, by sending them papers. As a result, their matter remained in the public domain. When internet searches were conducting using their names as keywords, both the newer and older articles appeared in the search results.[780] The applicants requested that their names be anonymised in articles published by the press reporting on their case.

The ECtHR conducted a comprehensive balancing exercise between the rights of privacy and freedom of expression, protected in Article 8 and 10 of the European Convention on Human Rights (Convention), respectively.[781] The court detailed the "relevant criteria" that must be considered where competing, yet equal, rights of Articles 8 and 10, must be balanced, and these are as follows:[782]

> "contribution to a debate of public interest, the degree to which the person concerned is well known, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and, where it arises, the circumstances in which photographs were taken".

Furthermore, the court highlighted that, generally, individuals cannot claim that their reputation has been damaged and thus also their personality rights (which is a part of the right to privacy) has been infringed where this is a result of their own behaviour.[783]

---

[779] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 6 – 9. The applicants appealed their convictions, including a constitutional appeal against the criminal proceedings/convictions to the Bundesverfassungsgericht, all of which were dismissed.

[780] E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 262.

[781] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 86 – 113. In para 86, the ECtHR in *ML & WW v Germany* explained "private life" as follows:

> "the concept of "private life" is a broad term not susceptible to exhaustive definition, which covers the physical and psychological integrity of a person and can therefore embrace multiple aspects of a person's identity, such as gender identification and sexual orientation, name or elements relating to a person's right to their image. The concept covers personal information which individuals can legitimately expect should not be published without their consent."

See also *Flinkkila & others v Finland* [2010] ECHR 446 para 75, and *Saaristo & others v Finland* [2010] ECHR 1497 para 61.

[782] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) para 95, these principles were summarised in *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 para 165, see also *Axel Springer SE and RTL Television GmbH v Germany* [2017] ECHR 793 para 42, *Falzon v Malta* (European Court of Human Rights) application no 45791/13 (20 March 2018) para 55, and *Hurbain v Belgium* [2023] ECHR 948 para 98. The court also applied *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 263.

[783] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 87 – 88, see also *Axel Springer AG v Germany* [2012] ECHR 227 para 83, and *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 para 163. Article 8 of the Convention is

The ECtHR applied the above criteria, coupled with *Google Spain*,[784] (ie the consideration of the permanency of the internet)[785] and came to the following conclusions:[786] access to reports which were lawful at the time of publication, coupled with the current behaviour of the applicants, who were in constant contact with the press before and throughout the proceedings, will mean that the applicants will not succeed in having the links "forgotten", ie de-referenced. Similarly, the court argued that there was no violation of the right to privacy.[787]

In *Hurbain v Belgium*,[788] the facts before the ECtHR, briefly, were as follows: The applicant, was the publisher of a popular Belgian newspaper, which had reported on a motor vehicle accident caused by Dr G.[789] Dr G, a medical practitioner, caused a fatal accident in

---

worded 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 well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Hurbain v Belgium [2023] ECHR 948 para 96 pointed out that even if the information is already in the public domain, does not mean that it is precluded from being protected under Article 8 of the Convention, the "interest in publishing that information had to be weighed against considerations relating to private life." See also *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 paras 134 – 136.

[784] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[785] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) para 114, see also *Pihl v Sweden* (European Court of Human Rights) application no 74742/14 (7 February 2017) para 33, and *Fuchsmann v Germany* [2017] ECHR 925 para 53. Note in *Pihl*, the ECtHR applied *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

[786] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 97 – 116.

[787] See generally *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), as this point was something that the ECtHR kept on coming back to. See also E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 263 – 26, and A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 121 – 122.

[788] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), and *Hurbain v Belgium* [2023] ECHR 948, as set out above, this is a judgment from the ECtHR's Third Section, which was upheld by the Grand Chamber in *Hurbain v Belgium* [2023] ECHR 948. The facts are largely discussed in a similar manner by both the Third Section and the Grand Chamber. See the approaches of *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, as well as, as described above the Grand Chamber's discussion in *Hurbain v Belgium* [2023] ECHR 948 paras 94 – 132 which summarises the approaches of the national high courts (from the contacting states to the ECtHR) on the anonymisation or deletion of information made available in online archives, and how the national courts balanced the right to be forgotten (ie privacy) with freedom of expression. See also the discussion in A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 122 – 123, R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 266 – 268, N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 at 1675 – 1676, and H Tomlinson '*Hurbain v Belgium*: The Grand Chamber of the European Court of Human Rights upholds decision that order anonymising newspaper archive did not violate article 10' (2024) 35(1) *Entertainment Law Review* 30 – 35,

[789] Mr Hurbain represented the Belgian publisher that owned the popular newspaper, *Le Soir*, in the proceedings at the ECtHR.

which two persons died and three were injured. He was subsequently convicted in 2000 and served his sentence, and was rehabilitated during 2006. The criminal proceedings of Dr G were published by the publisher. The articles included the full name of Dr G. The print articles mentioning the criminal proceedings against Dr G were originally published during 1994, and uploaded onto the newspaper's online archive during 2008. Dr G used the publisher's own search tool, and thereby found the articles reporting on the criminal trial on the publisher's website. Dr G also used various internet search engines, and the link to the 1994 article appeared on the results pages of these search engines. Thereafter, Dr G directly approached the publisher for the removal of the link to the article, since the link to it appeared on the results pages of several internet search engines, as well as on the results page of the publisher's website. Both the majority in the third section and the Grand Chamber of the ECtHR expanded the right to be forgotten to, not merely de-linking/de-referencing the links from a search engine's results page, or the publisher's website search tool, or that a "no-index tag" is added to the article, but that the digitally archived article or articles in question, must be anonymised and that the data subject's name be replaced with an "X".[790] Both courts applied similar criteria. For this discussion, only those of the Grand Chamber are quoted, however, reference is made to the reasons provided by the Third Section. The Grand Chamber, before applying the criteria (which will be listed hereafter), stated that the two rights to be balanced are the right to freedom of expression, specifically the rights of the free press, publishers, and Dr G's right to a private life. Both of these rights are of equal value.[791] The right of the public to the information contained in these archives needs to also be kept in mind, especially since digital archives are a source of contemporary history.[792] The court also pointed out that there is need to preserve the integrity of digital archives, and the possible chilling effect that an anonymization order may have on freedom of the press in general.[793] The right to maintain archives, including online

[790] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021). In para 81, the issue was stated as follows:

> "The question raised by the applicant before the domestic courts was whether G. satisfied the relevant criteria in order to claim the right to be forgotten, in so far as, in the applicant's view, the article in question was not newly published material but an archived version of an old article. In this regard the Court of Cassation upheld the interpretation of the Court of Appeal, which had found that the online publication of the archived version of the article amounted to 'fresh disclosure' of G's previous conviction."

Mr Hurbain, on behalf of the publisher, has appealed the decision of the Third Section and the application will be argued before the Grand Chamber of the ECtHR on 9 March 2022 (see C Docksey, 'Journalism on trial and the right to be forgotten', *VerfBlog*, 9 March 2022).

[791] *Hurbain v Belgium* [2023] ECHR 948 para 211, see also *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 93, 98 and 101. Compare with *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).

[792] *Hurbain v Belgium* [2023] ECHR 948 paras 182 and 212.

[793] *Hurbain v Belgium* [2023] ECHR 948 paras 209 and 211, see also *Hurbain v Belgium* (European Court of

archives, is not absolute.[794] Hence, it is important for courts to undertake the balancing exercise, in order to find the best possible solution in light of the facts.[795]

The Grand Chamber applied the following criteria, whilst balancing the right to a private life (ie privacy) with freedom of expression, the court noted that there is some overlap between the application of the criteria to the facts, and it is important that the criteria be taken as a whole, in order to weigh up the competing rights of the parties:[796]

1 In terms of the first criteria, namely the "nature of the archived information", the Grand Chamber held that the article was factually correct, and therefore there was no need for corrections, furthermore, it was presented in an objective manner. It is the only article, although related to the events that led up to the criminal trial, did not deal with the trial per se, but rather was based on the tragedy that often accompanies road traffic accidents, which includes deaths. The article did not, at the time of the original publication, nor when it was placed into the digital archives, attract widespread publicity.[797]

2 The second criteria that the Grand Chamber considered was the passage of time. The incidents dealt with in the article occurred some 20 years ago, and the Dr G had been rehabilitated since 2006, and the request for anonymization came 16 years after the initial publication of the article. Hence, Dr G had a legitimate interest to be re-integrated into society, without being reminded of his past.[798]

Human Rights) application no 57292/16 (22 June 2021) paras 102 – 103.

[794] *Hurbain v Belgium* [2023] ECHR 948 para 22 of the concurring opinion of Judge Krenc, see also *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 104.

[795] *Hurbain v Belgium* [2023] ECHR 948 para 211.

[796] *Hurbain v Belgium* [2023] ECHR 948 para 205:

> "the Court considers that the balancing of these various rights of equal value to be carried out in the context of a request to alter journalistic content that is archived online should take into account the following criteria: (i) the nature of the archived information; (ii) the time that has elapsed since the events and since the initial and online publication; (iii) the contemporary interest of the information; (iv) whether the person claiming entitlement to be forgotten is well known and his or her conduct since the events; (v) the negative repercussions of the continued availability of the information online; (vi) the degree of accessibility of the information in the digital archives; and (vii) the impact of the measure on freedom of expression and more specifically on freedom of the press."

See *Guardian News & Media Ltd & others Re: HM Treasury v Ahmed & others* [2010] UKSC 1, F Aldhouse 'Anonymisation of personal data – A missed opportunity for the European Commission' (2014) 30 *Computer Law & Security Review* 403 at 405 – 414 for a discussion of the English cases and the considerations taken into account by the court in deciding whether the personal data should be anonymized or not.

[797] *Hurbain v Belgium* [2023] ECHR 948 para 219. Compare with *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).

[798] *Hurbain v Belgium* [2023] ECHR 948 para 221, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 108 – 109 and 113 – 122. See also *Österreichischer Rundfunk v Austria* [2006] ECHR 1043 para 68, *Węgrzynowski and Smolczewski v Poland* [2013] ECHR 690 para 58, *Delfi AS v Estonia* [2015] ECHR 586 para 133, and *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) para 91ffg. The Third Section re-iterated that applicants cannot rely on the protection afforded by Article 8 of the Convention where the loss of reputation is a result from

3 The third criteria dealt with the contemporary interest in the events. The Grand Chamber found that although the events were tragic, they carried no significant historical value, other than amounting to a statistic in light of the number lives lost in road traffic accidents. For this Dr G's name was not necessary, he was not a public figure, and did not add to the publicity of the article. There was no reason as to why his name still needed to be associated therewith.[799]

4 The fourth criteria was specifically whether the applicant attracted attention to their plight or the events (it over laps a bit with the third criteria, as set out above). Here the court once again re-iterated that Dr G was not a public figure, and was generally an unknown applicant. The matter, as it came before the courts, did not attract widespread publicity. Dr G did not attract any publicity, nor court the media, he specifically wanted to remain unnoticed.[800]

5 The fifth criteria looked into the "negative repercussions" where the information remains available online. Dr G had served his sentence, and he was rehabilitated, and that the article or information should not serve as a "virtual criminal record". The unhindered availability of the article will mean that it is accessible to a widespread audience, including Dr G's colleagues, patients, new acquittances, etc., and due to this availability has the potential to cause Dr G psychological harm.[801]

6 The sixth criteria focused on how easily accessible the information is when stored in

---

their own actions. That does not mean that Dr G was left without a remedy. The right to be forgotten aids in the rehabilitation of applicants – provided that they have served their sentence and that a reasonable amount of time has passed – see paras 108 – 109.

[799] *Hurbain v Belgium* [2023] ECHR 948 para 225, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 105 – 107, and 112. The Third Section in para 110 pointed out that during the trial the applicant would have gained a certain amount of notoriety, after the trial has ended and with the passage of time the applicant slips back into oblivion:

> "Although, after the commission of a criminal offence and while the trial is ongoing, a hitherto unknown person may acquire a degree of notoriety, that notoriety may also decline with the passage of time (see *M.L. and W.W. v Germany*, cited above, § 106). Indeed, the public's interest as regards criminal proceedings will vary in degree (ibid., § 100). Thus, in some cases, the right to be forgotten may confer on the person concerned the right to revert to being simply an individual unknown to the public. *Again, time is a very important factor in this regard*." (my emphasis)

Compare with *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

[800] *Hurbain v Belgium* [2023] ECHR 948 paras 229 – 230, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 108 – 109 and 113 – 122, see specifically 112. Compare with *M.L. & W.W. v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 106 - 109 and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

[801] *Hurbain v Belgium* [2023] ECHR 948 paras 239 and 252, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 113 – 122 and 132.

digital archives (this has some overlap with the fifth criteria discussed). Online digitised archives are far more easily accessible than print archives, especially where these are not blocked with a paywall, ie the information is available free of charge, means that it is accessible to a widespread audience – as detailed above. The Grand Chamber noted that the information found in court proceedings continually remained available free of charge. It is this widespread continued availability of the information that causes Dr G harm.[802] Both the Grand Chamber and the Third Section emphasised that the anonymisation request would only affect the digital version of the article, the print (original) version would be left intact.[803]

7 The seventh criteria discussed by the Grand Chamber was the impact that the proposed order may have on freedom of expression, but more specifically freedom of the press. The court highlighted that there the technical measures that may be ordered against the operator of a search engine as well as against publishers, where it has been established that there is a need to protect the private life (ie privacy) of an applicant. Those that are applicable to search engine operators include (a) the ordering of results so that the latest information always appears first on a results page,[804] or (b) the de-listing/de-referencing of links to the applicant's name.[805] The measures that may be required of a publisher include: (a) complete or full deletion of the digitally archived article/information; (b) anonymising the text by removing specifically the first and surname, and any further identifying feature, of the applicant; (c) update the digital archived text (where this is necessary), and add a note that the information in the text has been updated on the digital platform; (d) remove the information from the website's internal search engine index; (e) ensure that the article/information is not indexed/referenced by search engine web crawlers (through the use of no-index tags and similar codes) thereby preventing the information from being indexed by search engines to appear on a results page, where a search is conducted using the applicant's name.[806] During the balancing exercise, the

[802] *Hurbain v Belgium* [2023] ECHR 948 para 234, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 126 – 128 and 132.
[803] *Hurbain v Belgium* [2023] ECHR 948 para 253, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 128 and 132.
[804] See *GC et al v CNIL* EU:C:2019:773, *Hurbain v Belgium* [2023] ECHR 948 para 241.
[805] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *Hurbain v Belgium* [2023] ECHR 948 para 241.
[806] *Hurbain v Belgium* [2023] ECHR 948 para 241, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 132. In *Standard Verlagsgesellschaft mbH v Austria (No. 3)* [2021] ECHR 1029 the court found that uplifting the anonymization granted forum users that comment on articles published on a newspaper's website, to allow persons, against whom those comments are aimed, to pursue defamation actions, infringes on the newspaper's right to freedom of the press (as a part of the right to freedom

Grand Chamber held that courts must consider the aim that the applicant wishes to achieve in protecting their privacy (ie private life) and determine the least restrictive method of achieving that aim for the publisher.[807] Each case must be gauged on its own facts and circumstances, and in some instances a less restrictive limitation on freedom of expression may suffice.[808] The factors that were taken into account in terms of this criteria included the possible stigmatism that would result if the article remained "as is" online, and whether Dr G was rehabilitated.[809] Further, in terms of the circumstances of a matters it may be more prudent to direct an anonymisation request to the publisher, instead of approaching the search engine operator to de-index/de-reference.[810] As regards to the possible "chilling effect" that an anonymisation order may have on press freedom, the Grand Chamber noted that even though the publication of the article was lawful, an anonymisation order may form a part of the "duties and responsibilities" of the press, where a limit is imposed to curb any harm that be caused to the person who is the subject of the article.[811]

In summary, the Grand Chamber found that it would be best to order the publisher to anonymise the article. Amongst the reasons provided, summarising some points mentioned earlier, was that the article created a "virtual criminal record", even though Dr G had been rehabilitated. The continued availability of the unaltered digital version of the article was a cause of harm to Dr G. Also, a significant amount of time has passed, since the article was first published. Anonymising the article is in these instances, in light of the press freedoms granted in terms of

---

of expression). Newspapers may protect the sources from which they receive, not only information, but also comments from. Disclosing the authors of comments would deter forum users from making comments online, in fear of drawing unwanted attention themselves. The anonymity of the forum users would come to nought were the newspaper not able to defend itself in its own right. The newspaper had in place a notice and take down policy for particularly offence comments, and was generally active in reviewing and removing offensive comments. The court also concluded that the comments did not amount to hate speech, although they were defamatory. The court, in coming to its conclusions, balanced the respective rights of the parties involved, there were the forum users' right to anonymity, the newspapers freedom of the press and the injured parties' right to protect their reputation. See also *Axel Springer AG v Germany* [2012] ECHR 227 pars 89 - 95 for the criteria the court followed in coming to its conclusions, and *Delfi AS v Estonia* [2015] ECHR 586 paras 136, 140, and 157 – 159 in light of the allegations of hate speech. See also R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 266 – 268.

[807] *Hurbain v Belgium* [2023] ECHR 948 para 242, the court once again pointed out that courts must not lose site of the integrity of digital archives during the balancing exercise when justifying the method chosen to achieve the aim of the individual. See also *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 127 and 132, where the Third Section pointed out that it could only make a decision on the facts before it. It was not a search engine that was before the court, but the publisher, and hence the court had to find a solution based on the facts and the parties before them.

[808] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 134.

[809] *Hurbain v Belgium* [2023] ECHR 948 para 245.

[810] *Hurbain v Belgium* [2023] ECHR 948 paras 246 – 247.

[811] *Hurbain v Belgium* [2023] ECHR 948 paras 177 and 254.

the right to freedom of expression, is the best possible means of protecting Dr G's right to a private life (ie privacy).[812]

There was one concurring opinion by Krenc J and a dissenting opinion by Ranzoni J. Kūris, Grozev, Eicke and Schembri Orland JJ concurred in Ranzoni J's dissenting opinion. Interestingly, even in the Third Section there was a dissenting opinion written by Pavali J.

Krenc J concurred and added that the specific case that the Grand Chamber was required to deal with the specific case brought by Dr G, and does not expect that publishers must systematically begin to anonymise their archives. Put differently, a request for the anonymisation of archives must be expressed in specific terms, and provide how "severely" the right to privacy is impacted. Only where there is a need, due to the possible "severe" impact on the right to privacy, will it then be necessary to conduct a balancing exercise, based on the criteria discussed in the majority judgment.[813]

Ranzoni J's (with Kūris, Grozev, Eicke and Schembri Orland JJ concurring) dissenting opinion focused, as similarly discussed in the Third Section's dissent by Pavali J, on the debate of the right to be forgotten and search engines. The dissenting opinion pointed out that executing the right to be forgotten is primarily the function of search engines, as they primarily have the tools that make information available to a wider audience.[814] Hence, Ranzoni J was of the opinion that, in order to preserve press freedom, search engines should be the "first port of call" where an applicant is wishing to claim the right to be forgotten, especially since they have a far wider reach than publishers. The publishing of lawful and accurate journalistic articles is at the heart of what freedom of expression aims to protect.[815] The dissenting opinion also detailed the importance that digital press archives have, since the original press are becoming more infrequent, especially in light of the fact that more and more journalistic publications are exclusively found online and no longer have a "print version" of their publications.[816] Press archives take on the role of preserving information, and their function is to "remember" and not "forget". Archived material provides a source for historical research, irrespective of the interest that it may generate within the public domain.[817] The dissenting opinion suggested that as a general "guiding principle" in light of the press digital archives

[812] *Hurbain v Belgium* [2023] ECHR 948 paras 255 – 257.
[813] *Hurbain v Belgium* [2023] ECHR 948 para 33 of Krenc J's concurring opinion.
[814] *Hurbain v Belgium* [2023] ECHR 948 para 7 of Ranzoni J's dissenting opinion.
[815] *Hurbain v Belgium* [2023] ECHR 948 para 7 of Ranzoni J's dissenting opinion. See also *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 89, 97 and 102.
[816] *Hurbain v Belgium* [2023] ECHR 948 paras 8 – 9 of Ranzoni J's dissenting opinion.
[817] *Hurbain v Belgium* [2023] ECHR 948 paras 10 – 11 of Ranzoni J's dissenting opinion.

where the "lawfulness of the original article" is not being questioned, that these archives "must retain their authenticity and integrity".[818] The dissenting opinion suggested that where there is a request to alter existing information within press archives, it "should not entail a balancing exercise between two rights of equal standing."[819] Hence, the dissenting opinion suggested the following criteria where such a request is made:[820]

(a) In an application where an applicant claims the protection under Article 8 of the Convention (ie the right to a private life/privacy) they must provide compelling reasons as to the seriousness of the harm suffered (or would be suffered) and why freedom of expression should be limited. The reasons must include the degree of accessibility of the article, and how the accessibility impacts on the rights of the applicant, as well as the sensitive nature of the personal information, and the vulnerability of the applicant or any person's affected by the publication thereof, ie the nature of the archived material should be considered.[821]

(b) Where the seriousness of the harm has been established, and based on the facts, including the protection of the reputation of the applicant and anyone else's rights that are affected, an option that limits access to the information, and has the least impact on freedom of expression should be explored. Ranzoni J emphasised that press archives are a vital source of remembrance, and hence, options that involve de-indexing/de-referencing (ie the right to be forgotten) via search engines should be the first option considered, as this is a well-established remedy.[822]

---

[818] *Hurbain v Belgium* [2023] ECHR 948 para 13 of Ranzoni J's dissenting opinion.
[819] *Hurbain v Belgium* [2023] ECHR 948 para 13 of Ranzoni J's dissenting opinion.
[820] *Hurbain v Belgium* [2023] ECHR 948 para 14 of Ranzoni J's dissenting opinion.
[821] *Hurbain v Belgium* [2023] ECHR 948 para 14(a) of Ranzoni J's dissenting opinion.
[822] *Hurbain v Belgium* [2023] ECHR 948 para 14(b) of Ranzoni J's dissenting opinion. See also the separate dissenting opinion of Pavali J *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021). Pavali J noted the following (para 19):

> "It is clear from the above that the plaintiff's root concern was with the online search results, not the article itself. With this in mind, his legitimate interest in not being confronted with the article in question in his daily personal and professional life could have been adequately protected by removing the article from name-based search results on general search engines (according to current statistics, more than 90 percent of Belgian Internet users tend to use one of two major search engines). Such a measure would have prevented the article from becoming easily accessible through curiosity-driven or other random search queries. At the same time, it would have preserved the integrity of the press archives and allowed full access to the unaltered original source to those persons – journalists, researchers or others – who might become specifically interested in the past events covered in the article. While delisting remains a significant interference with the freedom to receive and impart information and ideas, it is still less onerous for the applicant and less detrimental to his Article 10 rights."

The judgment agreed with the discussions and findings in *Jankauskas v Lithuania (No. 2)* [2017] ECHR 593 and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*. Compare with *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).

(c) If the circumstances justify such a measure, the applicant may approach the publishers and request that the archived material be altered, ie anonymised, etc. and in the extreme cases, deleted. Ranzoni J stated that the courts should not be too quick to grant an order that requires press archives to be permanently altered, especially articles that were lawfully published. Hence, the least restrictive option in light of all the circumstances should be implemented, so as to lessen the impact on freedom of expression.[823]

Ranzoni J came to the conclusion, based on the facts, as outlined by the Grand Chamber, that de-indexing/de-referencing the article with the search engine and the internal publisher's search tool would be enough. Dr G was not a vulnerable individual, the report did not solely deal with the accident caused by Dr G, he was one of many mentioned in the article, Dr G did not provide any evidence that he had suffered harm, furthermore, the article had been available one the internet for over 2 years, and there was no evidence that Dr G would suffer any harm if it were still available. Ranzoni J stressed that with the increased migration of press archives to digital platforms, the anonymization of digitally archived material will have a chilling effect on freedom of expression, as this may result in the press and/or publishers refraining from keeping lawfully published articles on their websites, and this will impact on the "right to remember".[824] Hence, Ranzoni J supported the de-indexing/de-referencing of articles with search engines and not directly with the publishers.[825]

---

[823] *Hurbain v Belgium* [2023] ECHR 948 para 14(c) of Ranzoni J's dissenting opinion.

[824] *Hurbain v Belgium* [2023] ECHR 948 paras 16 – 29 of Ranzoni J's dissenting opinion. M Ctvrtník *Archives and Records: Privacy, Personality Rights, and Access* (2023) at 122 – 123 describes the "right to remember" as follows:

> "one may ask why the right to be remembered could not equally be created, written down, and codified? Why should not citizens be able to claim that a certain imprint should be left in reality and in history? Such a right, however, need not be formulated merely as a person's right to preserve the memory of their own actions. It can also be defined in the sense that society as a whole also has the right to be remembered for the deeds and actions as members of that society, whether for their positive contribution or, conversely, their negative impact. At this point, the right that comes into play is the right of a society to hold its individual members accountable for their actions, the pursuit of justice, but also to enable the creation of a historical memory of the society, its historical consciousness, including coming to terms with its own past."

[825] *Hurbain v Belgium* [2023] ECHR 948 paras 16 – 29 of Ranzoni J's dissenting opinion. See also *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) – see the separate dissenting opinion of Pavali J. Pavali J noted the following (para 19):

> "It is clear from the above that the plaintiff's root concern was with the online search results, not the article itself. With this in mind, his legitimate interest in not being confronted with the article in question in his daily personal and professional life could have been adequately protected by removing the article from name-based search results on general search engines (according to current statistics, more than 90 percent of Belgian Internet users tend to use one of two major search engines). Such a measure would have prevented the article from becoming easily accessible through curiosity-driven or other random search queries. At the same time, it would have preserved the integrity of the press archives and allowed full access to the unaltered original source to those persons – journalists, researchers or others – who might become specifically interested in the past events covered in the article. While delisting remains a significant interference with the freedom to receive and impart information and ideas, it is still less

Considering the above, it is evident that the anonymisation of archives will be ordered when there is a clear need to protect the individual's identity in order to allow them to develop and interact with society without the past hanging over them. This is reliant on a few factors, such as the type of work the data subject seeks to do, as well as if their sentence is served or the fine is paid, as well as the newsworthiness of the article. As illustrated above, all the relevant rights and freedoms must be considered where such a request is made. If the data subject's draw attention to their own plight, then the court is likely to refuse a request, because the data subject's behaviour does not show that they wish to live in relative anonymity.

(iii) Deletion

The ECtHR a few months later unanimously confirmed the approach of *Hurbain v Belgium*[826] in *Biancardi v Italy*.[827] In *Biancardi*, the facts are as follows: the applicant, as the editor-in-chief of a privately owned online newspaper, had received a request to remove an article from the newspaper's website. The article concerned a stabbing that had occurred in a restaurant, the police questioning of the perpetrators, and subsequent actions of the police.[828] The request was made, by the restaurant as well as one of the perpetrators, for the de-linking/de-referencing of the article and was sent to both Google Italy S.r.l. and the applicant during September 2010.

---

onerous for the applicant and less detrimental to his Article 10 rights."

[826] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021).

[827] *Biancardi v Italy* [2021] ECHR 972. The facts in this matter are best summed up in para 1:

> "The applicant, the editor-in-chief of an online newspaper, was held liable under civil law for having kept on his newspaper's website and not having de-indexed an article reporting the facts of a criminal case instituted against private individuals. The applicant alleged the violation of his freedom of expression under Article 10 of the Convention."

This case related to a criminal matter in which, after the fight, the restaurant owner suffered reputational damage. The article detailed the police investigation. The continued availability of the factually incomplete article meant that the reputation of the restaurant owner was still negatively impacted when persons searched for information regarding the restaurant and the article was amongst the top links displayed on the results page. See also R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 263 – 265, and N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 at 1674 – 1675. See R Craig & G Phillipson 'Privacy, reputation and anonymity until charge: ZXC goes to the Supreme Court' (2021) 13(2) *Journal of Media Law* 153 – 185 for a proposal that the names of those that are suspected of a crime are anonymized until the start of the trial. The idea would be to avoid unnecessary attention where the person suspected may not turn out to be the person who goes on trial. Compare with PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 – 18 on possible exceptions, but also the benefits as well as the implications of deleting personal data. Bernal at 10 – 11, suggested that one of the exceptions is for archives to ensure "a good, accurate and useful historical record of events." This would include newspaper archives, blogs, or any repository (including online) that is archival in nature or governed by archival procedures. The author uses the following example: the "British Library . . . has campaigned for a 'right to archive', effectively asking for the right to archive web pages without needing to get permission from the website owners . . . The British Library could be included on a 'register of archivists' that are permitted to keep such an archive - but required to control and report on that archive."

[828] The facts only indicate that the criminal proceedings were pending against the perpetrator, see *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 32.

The applicant, at the court hearing based on the original request, during May 2011, acceded to this request, hoping that the matter would end. In the judgment, during March 2012, the court of first instance excluded an order against Google Italy S.r.l. due to a withdrawal of the complaint against them. The applicant was ordered to pay damages for the reputational damages caused, specifically referring to the applicant's failure to de-link the information within a reasonable time, and the further processing thereof after the de-linking request was unlawful. The applicant lodged an appeal on various points of law. The Supreme Court confirmed the judgment of the court of first instance, basing its reasons on the ease with which articles are accessed via an internet search.[829] The applicant subsequently approached the ECtHR, wherein he claimed that his rights to freedom of expression had been violated through the court proceedings. The criminal proceedings were pending against the perpetrator, and hence, the period between the request and the actual de-linking of the information could not be considered as excessive. Also, according to the applicant, in similar cases, the courts had required that the publishing houses add "supplementary information of clarifications to the articles" where this was necessary.[830]

The ECtHR, discussing various cases (including cases from the CJEU), once again emphasised that the various rights, freedoms and interests need to be balanced in order to find a fair solution in the circumstances.[831] The ECtHR focused on the following aspects in reaching its decision to remove the online article, instead of the standard criteria, as set out in *Hurbain v Belgium*:[832]

1 The passage of time between the initial publication of the article (2008, and the request to remove (2010). Also, the court found that the article had not been updated since the initial publication to date.[833]

[829] *Biancardi v Italy* [2021] ECHR 972 paras 2 – 14.
[830] *Biancardi v Italy* [2021] ECHR 972 paras 1, and 32 – 35.
[831] *Biancardi v Italy* [2021] ECHR 972 para 19ffg, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), *GC et al v CNIL* EU:C:2019:773, *Google LLC v CNIL* EU:C:2019:772, Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014, and European Data Protection Board *Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1)* adopted 7 July 2020.
[832] *Biancardi v Italy* [2021] ECHR 972 paras 57 – 69. See also C Docksey, 'Journalism on trial and the right to be forgotten', *VerfBlog*, 9 March 2022, and R Stancescu-Cojocaru 'Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression' (2023) 24 *ERA Forum* 261 at 263 – 265.
[833] *Biancardi v Italy* [2021] ECHR 972 para 65. Compare with *G.I.E.M. S.r.l. & others v Italy* [2018] ECHR 564 paras 21 – 24, where the ECtHR held that the applicability of the "right to be forgotten" increases in matters where the accused has not been convicted (ie no verdict as to their guilt has been pronounced) and the time frame in

2 The sensitivity of the information, which is an important factor to consider where the respective rights and interests of all parties involved are balanced, presently it was only a criminal investigation which had an impact on the reputational existence of individuals. The continued processing or dissemination of the article severely infringed on the individual's right to a private life. The individuals were not public figures from politics or the entertainment industry – hence the effect on their reputation was severe.[834]

3 The applicant had not been held criminally liable. The civil sanction awarded by the national courts for the reputational damages of the individuals, although not insignificant (ie €5 000 per affected data subject). The individuals or data subjects were yet to be convicted or acquitted in the criminal proceedings and this was not reflected in the articles on the applicant's website. Hence the civil sanction was not excessive in the overall circumstances of the case.[835]

Hence the ECtHR concluded that the data subjects' reputational rights had been infringed and they continued to be infringed as long as the article was available on the publisher's website. Apart from the pecuniary payment, the order included a complete removal the article.[836]

Once again, the ECtHR took the right to be forgotten a step further – the criminal

which the crime may be prosecuted has lapsed.

[834] *Biancardi v Italy* [2021] ECHR 972 paras 67 – 68.

[835] *Biancardi v Italy* [2021] ECHR 972 para 69.

[836] *Biancardi v Italy* [2021] ECHR 972 para 70:

> "The foregoing considerations are sufficient to enable the Court to conclude that the finding by the domestic jurisdictions that the applicant had breached V.X.'s right to respect for his reputation by virtue of the continued presence on the Internet of the impugned article and by his failure to deindex it constituted a justifiable restriction of his freedom of expression (see, mutatis mutandis, *Times Newspapers Ltd*, cited above, § 47) – all the more so given the fact that no requirement was imposed on the applicant to permanently remove the article from the Internet."

See also *Times Newspapers Ltd v The United Kingdom* [2009] ECHR 451 para 47, *Axel Springer AG v Germany* [2012] ECHR 227 para 78, and *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 89 – 94. Compare with the decision in *LB v Hungary* [2021] ECHR 2 where the tax authority published the data subject's name and home address on a list of tax defaulters – here the main judgment concluded that the information appears in Hungarian, it will only attract a small group of interested readers and not a global audience, and it will only attract and be available to those readers that are genuinely interested in the information, and was thus reasonable in the circumstances (para 68). In their dissenting opinion of Judges Ravarani and Schukking found that the publication of the home address is unnecessary to achieve the aim of the legislation, further coupled that information published on the internet is never truly private, is easily replicated by third persons and distributed, the possible consequences may amount to the data subject becoming a victim of crime, eg theft. The majority in the Grand Chamber in *LB v Hungary* [2023] ECHR 298, agreed with the dissenting opinion. The Grand Chamber reasoned that the publishing the data subject's home address had the potential to be misused, and was not needed in light of the aims that the legislature wished to achieve, ie publicly implicate tax defaulters as a means of deterrence from evading tax and/or committing tax fraud (see chapter 2, at the discussion of *Deutsche Post AG v Hauptzollamt Köln* EU:C:2019:26, specifically in the footnotes for a summary of *LB v Hungary* judgments).

investigation and report were as a result of the data subject's own actions – a proper application of the principles in *Google Spain* would have amounted to a de-indexing/de-listing/de-referencing, rather than a complete removal – this would have sufficed in light of the facts.[837] Another point to make is that the ECtHR acknowledges that the interchangeable terms "de-indexing", "de-linking", and "de-referencing", as used in the EU and in international law, require that search engines to remove "from the list of results displayed (following a search made on the basis of a person's name) Internet pages published by third parties that contain information relating to that person",[838] but the court does not necessarily refer to this as the "right to be forgotten". The possible reason for this is that the right to be forgotten is found in the EU legislative instruments as applied by the CJEU. Although the ECtHR may refer to these instruments, especially where the Member State before the court is a part of the EU as well as the Council of Europe. Generally, the ECtHR will not apply the EU legislation, as not all members of the Council of Europe are a part of the EU. Furthermore, the ECtHR's jurisdiction is limited to the Convention, protocols and treaties that are promulgated by the Council of Europe. The ECtHR expects those Member States that are a part of the EU, to implement and interpret the domestic (ie national) and EU legislative instruments in light of the rights and freedoms provided in the Convention. The ECtHR is thus confined to ascertain "whether the effects of such adjudication [and implementation] are compatible with the Convention."[839]

---

[837] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*. See also C Docksey, 'Journalism on trial and the right to be forgotten', *VerfBlog*, 9 March 2022. Compare with BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and the summary of this case in *Hurbain v Belgium* [2023] ECHR 948 paras 127 – 130, especially para 129:

> "The interests of the data subject had to be weighed against the interests of the press and the public at large in the continued accessibility of an initially lawful article, in view of the changed circumstances. In that connection the courts had to take into consideration, in particular, the following factors: the seriousness of the breach of personality rights resulting from the continued availability of the information despite the passage of time; the length of time since the article had been archived; the conduct of the data subject in the meantime, including any updates; the actual continuing or diminishing impact of publication of the article on a large scale; the ranking of the information in the list of results following a name-based Internet search; the public interest in the continued availability of information whose initial publication had been lawful; and the interests of the content providers, based on fundamental rights, in having their content archived and made available in essentially unaltered form. Measures placing restrictions on the free availability in the online archives, in unaltered form, of initially lawful press articles were reasonable only if the consequences for the data subject were particularly serious and the measures therefore did not fundamentally call into question the principle that such material should be made available other than in a few isolated cases."

[838] *Biancardi v Italy* [2021] ECHR 972 paras 53 – 54.

[839] *Jeunesse v The Netherlands* [2014] ECHR 1036 para 110, Articles 19 and 32(1) of the Convention, and S O'Leary 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 at 5.

(g) Conclusion

To provide a short summary of what has been held to be important factors where a request has been made to de-index or de-link or de-reference data, in light of the right to be forgotten. The factors are loosely grouped into specific categories, for ease of reference, however, this is not cast in stone, as certain factors may need, depending on the circumstances, to be considered in terms of another category. The factors are divided into general, those specific to the data subject, those specific to the availability of the information, those regarding the search engines' duties, those in light of the content provider/publisher, and lastly what are the available remedies in light of de-linking or de-referencing request:[840]

1 The general factors that were considered by the courts, included:

(a) The right to be forgotten is not absolute, and must be balanced with the rights, interests and freedoms of the internet users, operators and publishers. The rights included in the balancing exercise will be the data subject's right to privacy, the search engine operators' right to generate an income, the internet users' and the publishers'/media's/content providers' rights to freedom of expression and to impart or receive information, or specifically press freedom. Balancing these, in terms of the facts of each matter, will guide the courts in coming to a fair outcome.[841]

(i) Generally, the right to privacy will override the search engine's or publisher's right to generate an income (ie right to economic gain).

(ii) However, the following should be noted in this regard: the data subject's right to privacy may be overridden by the right to generate an income where the data subject is a famous personality, ie a celebrity or politician, or where the notice must be published in terms of a legal obligation as required by law.[842]

[840] These criteria mirror those of the Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014 at 13 – 20, however, the courts expanded on the criteria and what each may further include, in addition to what was provided by Article 29 WP, or merely clarified what Article 29 WP was detailing in their list.

[841] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, *LB v Hungary* [2023] ECHR 239 para 47, BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, *Standard Verlagsgesellschaft mbH v Austria (No. 3)* [2021] ECHR 1029 and *Hurbain v Belgium* [2023] ECHR 948.

[842] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See also *Meta Platforms Inc.*

(b) The request will be limited to the regional (ie the European Union or Europe) or national (ie an individual State) borders. [843]

(c) Each case must be dealt with in light of the facts therein – it may mean that on a proper consideration of all the legal principles the request to de-link or de-reference may be unsuccessful.[844]

(d) The courts have stated that the balancing of the right to be forgotten with the relevant rights, interests and freedoms of internet users, operators and publishers is not limited to internet search engines, and the relevant information regulator. Governments, especially the legislature during the drafting and implementation of relevant laws, directives and/or regulations in light of data protection and access to personal data, as well as private companies, in the drafting and implementation of policies, etc. dealing with the processing of personal data, will be expected to carry out such a balancing exercise.[845]

2 Specifically with respect to the data subject:

(a) The passage of time is an important aspect to consider, between the initial publication and when the request is made – all the cases highlight this point!

(b) Did the data subject attract attention to the information?[846]

(c) How sensitive is the personal data or information?[847] Will the availability of the information have an adverse impact on the data subject, the data subject's personal or family life, or will it have no or little impact?[848] In other words, the more sensitive the information is or the closer the information is to the heart of the right to privacy, the more likely that the right to privacy will outweigh the

& others v Bundeskartellamt EU:C:2023:537, *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:276, and *Meta Platforms Ireland Ltd v European Commission* EU:T:2023:277.

[843] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *Google LLC v CNIL* EU:C:2019:772.

[844] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *TU, RE v Google LLC* EU:C:2022:962, BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and *Hurbain v Belgium* [2023] ECHR 948. See also F Lazzarelli 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 at 936 – 937.

[845] *LB v Hungary* [2023] ECHR 239.

[846] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and *Hurbain v Belgium* [2023] ECHR 948.

[847] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), and *Hurbain v Belgium* [2023] ECHR 948.

[848] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), *ML v Slovakia* [2021] ECHR 821, and *Hurbain v Belgium* [2023] ECHR 948. Note the privacy continuum in *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67.

other rights.

(d) Specifically in light of criminal cases: the sentence must have been served and/or the criminal record expunged to support the re-integration of the data subject into society, and the fact that convicted persons no longer wish to be confronted with their past criminal act.[849] In certain instances, the seriousness of the crime and the impact it had on society may be an important factor to consider.[850]

(e) The prominence of the data subject in public life also plays an important role – especially since most of the individuals mentioned are often not politicians or work in the entertainment industry. These so-called "average Joes or Janes" deserve that their privacy be protected as far as is possible within the legal limits.[851]

(f) In respect of de-linking or de-referencing inaccurate information, the data subject must provide the search engine operators (as well as the courts) with all the relevant information in order for them to reach a decision.[852]

3 Availability of the information:

(a) Where the information is kept in a register, directory or archive, and depending on the specific circumstances of the matter before the courts, taking into account, amongst other factors the reasons provided by the data subject whether the personal data should be erased, access blocked or restricted, and the possible need for certain third parties to gain access thereto in future, noting the lapse of relevant time periods and that personal data should only be processed for as long as necessary.[853] Furthermore, to access the personal data, the person requesting

[849] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), *Biancardi v Italy* [2021] ECHR 972, and *Mediengruppe Österreich GmbH v Austria* [2022] ECHR 316.
[850] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and *Hurbain v Belgium* [2023] ECHR 948 para 111.
[851] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, *TU, RE v Google LLC* EU:C:2022:962, and *Hurbain v Belgium* [2023] ECHR 948.
[852] *TU, RE v Google LLC* EU:C:2022:962.
[853] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197, *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833, *LB v Hungary* [2023] ECHR 239, and *Hurbain v Belgium* [2023] ECHR 948.

must have a legitimate interest to obtain same.[854]

(b) Regarding the availability of personal data on the internet: Government organisations and/or private companies will be required to restrict access thereto:[855]

(i) Where this infringes the data subject's rights to privacy and protection of personal data;

(ii) The reason for this is that even internet users who do not have a legitimate interest, eg where police are investigating a crime, are able to obtain the information, and process same without the knowledge of the data subject, as well as without having a legitimate interest. The processing of personal data by an internet user without a legitimate interest may have adverse consequences for the data subject;

(iii) Investigating authorities and/or the police can request the information from the relevant authorities, in terms of the data protection and/or access to information laws, by filing the required application.

(c) A further point to consider is whether the information forms a part of the contemporary public debate, and should remain available.[856]

(d) With regards to de-linking and exceptions:

(i) Generally, search engine operators must accede to the request to de-link, taking into account the exceptions listed in Directive 95/46 or the GDPR;[857]

(ii) Where the data falls into the special categories of data listed within the legislation, the operator may refuse to de-link, provided that the refusal is lawful, bearing in mind that the data subject may still be able to object, in light of their circumstances,[858] and

[854] *WM & Sovim SA v Luxembourg Business Registers* EU:C:2022:912. – an example provided is where the police request personal data from a government agency in order to carry out their investigations – this is a legitimate interest, and the request should then be made to the agency directly, and not obtained freely over the internet.
[855] *WM & Sovim SA v Luxembourg Business Registers* EU:C:2022:912, and *LB v Hungary* [2023] ECHR 239.
[856] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*, and *Hurbain v Belgium* [2023] ECHR 948.
[857] *GC & others v CNIL* EU:C:2019:773.
[858] See Article 14*(a)* of Directive 95/46 or Article 17 of the GDPR, *GC & others v CNIL* EU:C:2019:773, and BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*.

(iii) Apart from the special conditions with respect to the special categories of data to be considered, the de-linking process must also bear in mind the relevant Charter rights of all parties concerned to reach a fair outcome.[859]

4 In respect of search engines:

(a) Search engines must comply with the provisions of Directive 95/46, and importantly, as the Directive 95/46 was repealed, also with the provisions of the current GDPR.[860]

(b) Search engines must comply with the orders to de-link issued by the relevant data authority and the courts.[861]

(c) Where there is a request to de-link or de-reference information the data subject's privacy will most likely take precedence over the right to information of the internet users, ie the general public.[862]

(d) The data subject may approach the search engine directly to de-link or de-reference, irrespective of whether the data subject has approached the relevant content provider to remove the information.[863] However, where the data subject has revealed the personal information themselves, then the data subject must approach both the search engine and content provider to have the information removed, and/or de-linked or de-referenced.

(e) The operator of a search engine must, at the very least, when a de-linking/de-referencing/de-indexing request is made, reconcile the links leading to the personal information in such a way that the data subject's current legal position is first reflected on the results page.[864]

5 Publishers and/or content providers:

(a) The ECtHR has included that de-indexing requests may now be directed at

[859] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *GC & others v CNIL* EU:C:2019:773.
[860] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *GC & others v CNIL* EU:C:2019:773, and *TU, RE v Google LLC* EU:C:2022:962.
[861] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *GC & others v CNIL* EU:C:2019:773, *TU, RE v Google LLC* EU:C:2022:962.
[862] *TU, RE v Google LLC* EU:C:2022:962.
[863] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *TU, RE v Google LLC* EU:C:2022:962.
[864] *GC & others v CNIL* EU:C:2019:773.

publishers of news articles, including the anonymisation of data subjects, and replacing these with a letter, within the digital archives.[865]

(b) It may be required that the content be completely removed from the internet platform of the content provider/publisher, in certain instances. These are appropriate where the continued dissemination of the article(s) in question will further damage the reputations of those reported therein.[866]

6 The last consideration are the remedies available where a request to de-link or de-reference, has been made, including the deletion or destruction of the data:

(a) Are there less restrictive methods to deletion and destruction that will achieve a similar outcome, ie de-linking/de-referencing?[867]

(b) Similarly, to the above, is there a less restrictive method instead of anonymising the information? This will depend on the sensitivity of the information as well as the actions of the data subject (as discussed above).[868]

(c) Setting the results to show the current position of the data subject. This means that current legal proceedings must be displayed on the results, but where the outcome of those proceedings no longer correlate to the present circumstances of the data subject, these should either be displayed later in the list or de-linked – depending on the circumstance of each individual matter.[869]

(d) Will digitally blacking out the data subject's name assist in keeping the information available for public access?[870]

(e) Ultimately, what is reasonable under the present circumstance in terms of a suitable technological solution, even if there is some cost involved?[871]

---

[865] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), and *Hurbain v Belgium* [2023] ECHR 948.
[866] *Biancardi v Italy* [2021] ECHR 972, and *Hurbain v Belgium* [2023] ECHR 948.
[867] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) – see the separate dissenting opinion of Pavali J, BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, and *Hurbain v Belgium* [2023] ECHR 948.
[868] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), and *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021).
[869] *GC & others v CNIL* EU:C:2019:773, BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I, Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) – see the separate dissenting opinion of Pavali J, and *Hurbain v Belgium* [2023] ECHR 948 – see the dissenting opinion of Ranzoni J.
[870] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.
[871] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and *Proximus NV v Gegevensbeschermingsautoriteit* EU:C:2022:833.

(f) The courts have held that legislatures must provide alternative remedies that may be considered in relevant cases, instead of merely de-linking, de-indexing or de-referencing the information.[872]

V CONCLUSION

The cases set out above show that both national and regional courts have reflected, debated and interpreted the best application for the right to be forgotten in each and every circumstance before it. The applicant's request may not have always been granted, depending on the circumstances and facts of the specific case before the court. The standard principles of *Google Spain* have not consistently been followed. This is problematic because of the effect it has on the right to freedom of expression and information.

The courts have consistently pointed out that the right to be forgotten is not absolute, same as the rights of privacy and freedom of expression,[873] and that it is important that the interests and rights of all parties concerned are taken into account. The right to be forgotten, and this point is more directly formulated in certain instances than in others, has been developed to provide a suitable remedy for persons to have inaccurate or incorrect information de-linked or de-indexed from their name when that is the search term used. This information in at least two instances outlined above would hinder the data subjects' full reintegration within society. The aim in all instances is to merely make the information more difficult to find, however, this has also amounted to the complete removal thereof.

[872] *B v Latvijas Republikas Saeima* EU:C:2021:504, see also *LB v Hungary* [2023] ECHR 239 paras 47 – 53.
[873] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *La Quadrature du Net & others v Premier minister & others*; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* EU:C:2020:791 para 120 – 122, and *GD v Commissioner of An Garda Síochána & others* EU:C:2022:258 para 48.

CHAPTER 4

SOUTH AFRICAN LAW: PRIVACY AND EXPRESSION

I INTRODUCTION

Technology is a platform through which human beings may express themselves; through debate, comments, sharing of information, whether personal or not, and communicate with others, no matter where they are in the world.[874] Since the advent of mobile internet compatible devices, joining in debates, commenting on posts on social media and sharing information have never been more convenient.[875] This leads to a few issues: what happens when information is shared that should have been kept private? What happens when the right to freedom of expression and the right to privacy find themselves at odds with one another?[876] These imbalances, with the convenience, brought about by mobile technologies have started to become commonplace.[877]

Human rights are an integral part of every person and are the foundation that holds democratic societies together.[878] The rights to privacy and freedom of expression are guaranteed in the Constitution,[879] and both have a long history.[880] A central value of the South African State is human dignity, this "born out of the history of Apartheid".[881] Often the protection of the right to human dignity requires a balancing of the right to privacy against the right to freedom of expression. Not infrequently when persons are disrespectful towards one another, human dignity is sacrificed. Although not always recorded in the case law, disrespect

---

[874] S Shapiro 'Places and spaces: The historical interaction of technology, home, and privacy' (1998) 14(4) *The Information Society: An International Journal* 275 at 282 – 283.
[875] J Bohn *et al* 'Living in a world of smart everyday objects—Social, economic, and ethical implications' (2004) 10(5) *Human and Ecological Risk Assessment* 763 at 779 – 780.
[876] PM Schwartz 'Free speech vs. information privacy: Eugene Volokh's first amendment jurisprudence' (1999 – 2000) 52 *Stanford Law Review* 1559 at 1559.
[877] J Bohn *et al* 'Living in a world of smart everyday objects—Social, economic, and ethical implications' (2004) 10(5) *Human and Ecological Risk Assessment* 763 at 779 – 780, and M Friedewald & RJ Pohoryles 'Technology and privacy' (2013) 26(1-2) *Innovation: The European Journal of Social Science Research* 1 at 1.
[878] JP Rascão 'Freedom of expression, privacy, and ethical and social responsibility in democracy in the digital age' (2020) 1(3) *International Journal of Business Strategy and Automation* 1 at 1.
[879] Constitution of the Republic of South Africa, 1996 (the Constitution).
[880] See generally MH Cheadle, DM Davis & NRL Haysom *South African Constitutional Law: The Bill of Rights* (May 2020 – Service Issue 28). See also the remarks of Ledwaba DJP, Pretorius J and Molefe J in *EFF & another v Minister of Justice and Constitutional Development & another* 2019 (2) SACR 297 (GP) para 1.
[881] Section 1 of the Constitution; MH Cheadle, DM Davis & NRL Haysom *South African Constitutional Law: The Bill of Rights* (May 2020 – Service Issue 28) at 11-5. Section 10 of the Constitution provides for the right to human dignity. See also *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 68, and *The Citizen 1978 (Pty) Ltd & others v McBride* 2011 (4) SA 191 (CC) paras 143 – 147. See also the comments by JC Buiterlaar 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 at 182 – 184.

due to the behaviour of the parties, often results in a loss of human dignity. Although the right to human dignity is not the main focus in this discussion, it is closely linked to both the rights to privacy and freedom of expression. It is worth mentioning that the Constitution "knows no hierarchy of rights", each is to be treated with equal respect.[882]

The focus of this chapter will be on the rights to privacy and freedom of expression in terms of the Constitution as well as case law. Both rights will be described and set out in some detail. Much of the conflict surrounding the right to be forgotten may be attributed to the conflict between the rights to privacy and freedom of expression. The tension is particularly poignant when the information, even of a private nature, may serve the public's interest; however, the subject of that information is otherwise inclined.[883] The discussions will focus on the rights irrespective of whether being applied to a natural or juristic person, because constitutional rights apply equally to natural and juristic persons.[884] The focus is on how a delicate balance can be achieved between these rights.

The chapter is divided as follows, first, there is a discussion on the right to privacy, second, the right of freedom of expression will be discussed, and, last, how these two rights have been balanced within the case law. The historical context of each right will be discussed in brief, just as a background, the focus is not on how the final form of the rights came into being, but rather on the scope of protection and later how the balance between the two is achieved.[885] The focus of the case discussions will be on Constitutional Court and Supreme Court of Appeal (SCA) judgments, although in certain instances, high court judgments will be discussed when dealing with a specific aspect, such as the information having been expressed via an internet blog.[886]

---

[882] *The Citizen 1978 (Pty) Ltd & others v McBride* 2011 (4) SA 191 (CC) para 148.

[883] See generally also *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC); *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC); *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD). This was a vital discussion in the debate between granting the right to be forgotten, ie privacy, and whether the information should remain available as is in terms of the right to freedom of expression and information in *Google Spain SL, Google Inc. and Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317.

[884] Section 8(2) of the Constitution and *Investigating Directorate: Serious Economic Offences & others v Hyundai Motor Distributors (Pty) Ltd & others: In re Hyundai Motor Distributors (Pty) Ltd & others v Smit NO & others* 2001 (1) SA 545 (CC) para 17. It is important to note that juristic persons are only "entitled to the right in the Bill of Rights to the extent required by the nature of the rights and the nature of the juristic person", see s 8(4) of the Constitution, and P De Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 403-406.

[885] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 22 points out that the final as well as interim Constitutions are incredibly similar and that their approaches remain the same.

[886] For example, *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).

II THE RIGHT TO PRIVACY

(a) Introduction and historical context

There is not much recorded in the case law regarding the history of the right to privacy. During apartheid persons were generally not "left alone" especially, within their own homes. Being "left alone" is one of the central aspects of privacy, as will be explained later.[887] In the past telephones were tapped and homes were unlawfully or unjustifiably searched. This has significantly added value to, as well as compelled the need to protect, the right to privacy.[888] Briefly and historically, the protection often finds its greatest thrust in search and seizure matters.[889] The opening paragraph of *Gaertner v Minister of Finance* dramatically describes how the search and seizure procedures were used during apartheid as a painful tool to suppress, degrade and intimidate the majority of the population or those who were considered "enemies of the state".[890] Most of these searches took place during the dead of night, where no warning could be sounded, it was "a time of relaxation; sleep; intimacy; reckless abandon even; and when some, if not most, would be flimsily dressed".[891]

Sachs J in *Mistry v Interim Medical and Dental Council* pointed out that the existence of safeguards to stop police and other officials from merely entering a person's home is the hallmark of a democratic society and not that of a police state.[892] South Africa's right to privacy

---

[887] Note SD Warren & LD Brandeis 'Right to privacy' (1890-1891) 4 *Harvard Law Review* 193, and A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Review* 62 at 65 – 66. See also A Roos 'Data Protection Law in South Africa' In A Makulilo (ed) *African Data Privacy Laws* (2016) at 195 – 195.

[888] *Gaertner & others v Minister of Finance & others* 2014 (1) SA 442 (CC), *Residents of: Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others* [2020] 3 All SA 902 (GJ) para 28. See also UNCHR (Sub-commission) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40 para 25.

[889] *Gaertner & others v Minister of Finance & others* 2014 (1) SA 442 (CC). See also *Gigaba v Minister of Police & others* [2021] ZAGPPHC 55 paras 38 – 49, and *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others* [2021] ZACC 37.

[890] *Gaertner & others v Minister of Finance & others* 2014 (1) SA 442 (CC) para 1, the court dealing with a matter in terms of customs and excise and searches without warrants stated: "It is with this painful history in mind that we consider the constitutional validity of statutory provisions that authorise searches without warrants."

[891] *Gaertner & others v Minister of Finance & others* 2014 (1) SA 442 (CC) para 1; *Residents of: Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others* [2020] 3 All SA 902 (GJ) para 28, and *Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others* [2021] ZACC 37 para 1, where Mhlantla J (for the majority) stated 'A home is more than brick and mortar, it is often a place of comfort, safety, and the keystone of a functional society.' Generally, for most individuals on a more personal note, privacy means that one has found a place where one can close themselves from the outside world, and not be affected by its moral, political and economic demands. See M Steinbeis 'Was hilft mir das Recht auf Vergessen, wenn ich nicht für mich sein kann?' *VerfBlog*, 31 May 2014, *https://verfassungsblog.de/hilft-mir-das-recht-auf-vergessen-wenn-ich-nicht-fuer-mich-sein-kann/* (Accessed: 14 January 2023).

[892] *Mistry v Interim Medical and Dental Council of South Africa & others* 1998 (4) SA 1127 (CC) para 25 and *Residents of: Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police &*

was drafted to counter the past injustices of apartheid. The current right to privacy repudiates "past practices" that offend constitutional values, whilst affirming those values that are consistent with South Africa's constitutional democracy.[893] This includes decriminalising as well as destigmatising sexual conduct, which Sachs J described as deviating "from the official norm", and allowing gays, lesbians, etc. to become visible members of society and not remain an invisible community.[894]

The right to privacy, as contained in s 14 of the Constitution, which addresses the concept of being "left alone", reads as follows:[895]

> "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."

It is a highly valued right. However, there is much debate as to what it actually entails.[896] The academic literature, and that of the case law set out below, agrees that "it appears common cause in many jurisdictions that the nature and the scope of the right envisages a concept of the right to be left alone."[897] Although there is this "agreement", the controversy relates to "the

others [2020] 3 All SA 902 (GJ) para 29.

[893] *Mistry v Interim Medical and Dental Council of South Africa & others* 1998 (4) SA 1127 (CC) para 25. See also *De Lange v Methodist Church & another* 2016 (2) SA 1 (CC) para 76.

[894] *National Coalition for Gay and Lesbian Equality & another v Minister of Justice & others* 1998 (12) BCLR 1517 (CC) paras 124 – 129. Note also, the Immorality Act 23 of 1957 (renamed the Sexual Offences Act; now repealed) and other similar laws from the apartheid era that banned sexual relations as well as marriages between races and of the same sex. It is beyond the scope of the thesis to go into too much detail, see the discussion in P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 586 – 587 and 589 – 590.

[895] Note that privacy has been enshrined in various international legislative instruments, see UNCHR (Sub-commission) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40 para 20. See a short overview in A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 at 55 – 56. In terms of the common law, privacy formed a part of a group of rights often referred to as "personality rights" – see C Maimela 'The reasonable accommodation of employees with cancer and their right to privacy in the workplace' (2018) 21 *Potchefstroom Electronic Law Journal* 1 at 15 – 19, where the common right to privacy is defined and compared with the Constitutional right.

[896] *NM &others v Smith & others* 2007 (5) SA 250 (CC) para 32; see also SD Warren & LD Brandeis 'Right to privacy' (1890-1891) 4 *Harvard Law Review* 193, MH Cheadle, DM Davis & NRL Haysom *South African Constitutional Law: The Bill of Rights* (May 2020 – Service Issue 28) at 9-1, and G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 468 – 470. For the history of the development of the right to privacy, see O Diggelmann & MN Cleis 'How the right to privacy became a human right' (2014) 14 *Human Rights Law Review* 441 – 458.

[897] *NM &others v Smith & others* 2007 (5) SA 250 (CC) para 32.

definitional nature and the scope of the right."[898]

The Constitutional Court has described privacy, as well as the idea of being left alone, as the protection of an individual's highly "intimate personal sphere".[899] It has specifically held that "the very high level of protection" of the right to privacy is to protect "a final untouchable sphere of human freedom that is beyond interference from any public authority."[900] Ackermann J describes this as an "intimate" or "inviolable core" that cannot be justifiably limited.[901] It is only when an individual "enters into relationships with persons" beyond this core that an individual's actions "acquire a social dimension" which, depending on the overall context, may be justifiably limited.[902] It is often for this reason that the home is afforded special protection within the right to privacy, especially against unlawful search and seizures.[903] Privacy in one's home has often been associated with the inner sanctum.

The majority in *Bernstein v Bester* further described privacy as "amorphous and elusive" and that its scope is "closely related to the concept of identity", where a right such as privacy is "not based on a notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity".[904] Furthermore, that privacy is important for an individual in finding their place within a community and therefore within society as a whole.[905] Privacy "cannot be confined to any one sphere, and specifically not to an abstract individualistic approach."[906]Although, the right to privacy includes "the inner sanctum of a person, such as his or her family life, sexual preference and home environment, which is

---

[898] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 32.

[899] I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) 298 fn 29, here the court was referring to Germany's jurisprudence in *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC) para 77, see *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 33.

[900] *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC) para 77. In *Smuts & another v Botha* [2022] ZASCA 3 para 9, the Supreme Court of Appeal aptly described this as:

> "Privacy enables individuals to create barriers and boundaries to protect themselves from unwarranted interference in their lives. It helps to establish boundaries to limit who has access to their space, possessions, as well as their commercial and other information. It affords persons the ability to assert their rights in the face of significant imbalances. It is an essential way to protect individuals and society against arbitrary and unjustified use of power by reducing what can be known about, and done to them. The right to privacy is not sacrosanct, it must be balanced with the rights of other citizens."

[901] *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC) para 77.

[902] *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC) para 77.

[903] *Ravin v State of Alaska* 537 P.2d 494 (1975).

[904] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 65, see also the minority judgment of Kriegler J at para 130. See also JC Buiterlaar 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 at 182 – 186, where the importance of a private space for an individual to define their own autonomous identity is discussed; F Cassim 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18(2) *Potchefstroom Electronic Law Journal* 69 – 110 in a comparative study discusses the importance of privacy protection in the age of identity theft.

[905] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67.

[906] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67.

shielded from erosion by [the] conflicting rights of the community",[907] however, the more a person interacts with those around them, the more they move away from the inner sanctum, the right to privacy is balanced against the rights and freedoms of others.[908] *Bernstein v Bester* will be referred to in some detail as it is the leading authority on the scope of the right to privacy.

The discussion on privacy that follows will focus on the scope of privacy in *Bernstein v Bester* and its application and the State's interests in protecting rights and freedoms, within the inner sanctum.

(b) The scope of privacy in Bernstein v Bester and its application

Three key principles regarding the right to privacy emerge from Ackermann J's judgment in *Bernstein v Bester*. The three key principles are the legitimate expectation of privacy, privacy exists along a continuum and the inner sanctum. Each aspect was substantiated with a considerable amount of international and foreign case law and legal principles. Each will be discussed in light of Ackermann J's judgment as well as later South African Constitutional Court judgments.

(i) Legitimate expectation of privacy

The first of these principles regarding the scope of the right to privacy encompasses a "legitimate expectation" regarding an individual's private life. The analysis of what this entails consists of two components, namely an individual's "subjective expectation" as well as what society considers an "objective expectation". In each instance, the circumstances of the particular case before the court will be the guide in determining the expectations. Ackermann J referred extensively to the United States, where the courts have created a two-part test based on these two expectations.[909] The inquiry, although having a two-part approach, is dealt with in a singular stage. Ackermann J remarked that the approach of the United States courts seems sensible and that the "scope of a person's privacy extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured."[910]

It should be noted that Canada and the United States do not specifically provide

[907] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 67.
[908] See generally J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18 – 28, and N Shaik-Peremanov 'Basel II - The right to privacy: A South African perspective' (2009) 21 *South African Mercantile Law Journal* 546 at 550 – 552.
[909] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 75.
[910] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 75.

protection for the right to privacy in their respective constitutional charters.[911] The right, in both jurisdictions, is connected to the right against unlawful search and seizure of an individual's home.[912] The Canadian courts have stressed that protection from unlawful or "unreasonable" search and seizures is designed to protect only a reasonable expectation of privacy.[913] Similarly to the United States, the Canadian approach also has the same two parts described above in the form of a reasonable expectation of privacy, namely, the first is the "subjective expectation of privacy", and the second is the "objective expectation of privacy", described by Ackermann J as what "must be recognised as reasonable by society".[914]

(ii) Privacy exists along a continuum

The second of the key principles is that privacy exists along a continuum. There are aspects of an individual's life that are truly intimate and should therefore remain private, namely, the inner sanctum. On the opposite end of the scale is a person's interactions within the public or social sphere, and in certain instances, these interactions, due to their public nature, will carry implications where privacy will not apply. Locating privacy on the continuum is not always that straightforward, as illustrated by the cases that follow. Ackermann J substantiated this point by quoting from English and German company law practice, specifically with regard to insolvency law. After setting out extensively the European Court of Human Rights judgment in *Fayed v The United Kingdom*,[915] and a judgment of the Bundesverfassungsgericht,[916] descriptively referred to as *Tonband*,[917] Ackermann J concluded, and with this, all the justices in *Bernstein v Bester* agreed,[918] that privacy may be justifiably infringed for the sake of an inquiry in insolvency proceedings where responsible individuals are questioned. This is deemed necessary, at the very least, for the responsible parties to be held accountable through civil proceedings only, by those who have lost money, etc. on account of their

[911] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) paras 74 – 75.
[912] Article 8 of the Canadian Charter of Rights and Freedoms; Amendment IV of the Bill of Rights to the United States Constitution.
[913] *R v McKinlay Transport Ltd*. [1990] 1 SCR 627 at 641; *Hunter et al. v. Southam Inc*. 1984 CanLII 33 (SCC).
[914] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 76. See also *Smuts & another v Botha* [2022] ZASCA 3 para 9. See also C Maimela 'The reasonable accommodation of employees with cancer and their right to privacy in the workplace' (2018) 21 *Potchefstroom Electronic Law Journal* 1 – 31, G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 445 – 456.
[915] *Fayed v The United Kingdom* Series A No 294B; Application No 17101/90; (1994) 18 EHRR 393.
[916] Federal Constitutional Court, Germany.
[917] 34 *BVerfGE* 238 – *Tonband*. 'Tonband' is the German word for tape or cassette because the questioning of the errant insolvent was recorded and stored on tape to be transcribed and used as evidence. *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 78.
[918] The majority of the justices concurred with Ackermann J, however, Kriegler J and O'Regan J each wrote a minority judgment, concurring in part with Ackermann J.

mismanagement.[919]

In *Tonband,* the Bundesverfassungsgericht limited the requirement for the reposnsible errant insolvent to fully disclose their actions that caused the company to go insolvent, to civil proceedings only, in order to meet their responsibility towards creditors, who have suffered harm by their actions. The reason for the limitation is that the use of the information in criminal proceedings would be unfair,[920] because an accused is not forced, during criminal proceedings, to incriminate themselves. Put differently, insolvents, or potential witnesses, must answer all questions honestly, despite there being the possibility of self-incrimination.[921]

In *Fayed v The UK*,[922] the court similarly found that the primary aim of the English Company Laws System was to further the public interest with regards to the affairs of public companies where the owners benefit from limited liability, and is designed to protect the interests of the parties that are directly involved in the business of or have a direct relationship with the public company, such as "investors, shareholders, especially small shareholders, creditors, customers, trading partners and employees".[923]

In both cases, the protection of affected parties was more important than the privacy of the errant directors or insolvents, even where their reputations were damaged. Based on the continuum, and in light of reputational rights, which are often also protected under the guise of privacy, such protection of a person's privacy and reputation will vary in terms of their standing within the community, whether the individual has a public role within society, coupled with the type of work that they perform will determine how much interest there is generally in that person.[924] Hence, "businessmen actively involved in the affairs of large public companies"

---

[919] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC), see also *President of the Republic of South Africa & others v South African Rugby Football Union & others* 1999 (10) BCLR 1059 (CC) para 186.

[920] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 78. The Bundesverfassungsgericht based its arguments on Article 2(1) of the Basic Law, which provides as follows: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." (Official English translation). See also OLG Stuttgart, Urt. vom 08.10.2015 - 2 U 25/15.

[921] 34 *BVerfGE* 238 – *Tonband* Part B II para 3, the specific part is translated in para 78 of *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC), reads as follows:

> "because in these cases it is the general consensus that the right to one's own words no longer enters the question. For example, insofar as it has become common practice in commercial dealings to keep a record of telephone messages, orders or stock-exchange reports by means of a tape recording, the right of the speaker to the unfettered development of the personality will, generally speaking, not be affected. In communications of this sort the objective content of the statement is so much in the foreground that the personality of the speaker is almost completely obscured by it and the spoken word thereby loses its private character."

[922] *Fayed v The United Kingdom* Series A No 294B; Application No 17101/90; (1994) 18 EHRR 393.

[923] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 74.

[924] *Tshabalala-Msimang & another v Makhanya & others* 2008 (6) SA 102 (W).

must be prepared to accept criticism and scrutiny for their actions from the press and the relevant representative public organisations that would not be levelled at private individuals.[925] These considerations echoed the Canadian and United States approach of a "reasonable expectation of privacy" and that such limits are justified. [926] In South Africa, the sentiments equally apply to politicians and public officials, as the information allows a democratic electorate to make suitable judgment calls regarding the political leadership, even where the information has been illegally obtained.[927]

In later constitutional judgments, famed for the prohibition of prostitution and the private use of cannabis, the Constitutional Court grappled with the principle that privacy exists along this continuum. In each of these cases, the placing of privacy along this continuum, whether the act belonged more in the "inner sanctum" or whether the activity was completely of a public nature, was certainly more difficult to pin point.

In *S v Jordan,*[928] the Constitutional Court had to decide whether the commercial exploitation of sex, which is a crime that can only be committed within the private sphere, can find protection under the right to privacy. The complexity of the issue is that prostitutes invite the public "to come and engage in the unlawful conduct in private".[929] The majority held that the State, and thereby the law, must be interested in dealing with crimes that are committed in both public and private.[930] The majority held that even where the right to privacy is infringed, the infringement is at the periphery of the scope and not in the private sphere. The prohibition against prostitution is directed at the sale of sex, money being the sole reason for acting out the trade.[931] Prostitutes, like other members of society, may use their bodies however, they please, as long as it does not break a valid South African law, such as the sale of sexual services. The State has a legitimate interest in prohibiting the commercialised sale of sex as well as brothel-keeping.[932] There are other commercial pursuits that prostitutes and brothel-owners may pursue to earn money. The majority concluded that the limitation to the right to privacy was justified.[933] The Constitutional Court, thus, supports the notion that in democratic societies the

[925] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 74.
[926] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 74.
[927] *Tshabalala-Msimang & another v Makhanya & others* 2008 (6) SA 102 (W) para 39.
[928] *S v Jordan & others* 2002 (6) SA 642 (CC).
[929] *S v Jordan & others* 2002 (6) SA 642 (CC) para 28.
[930] *S v Jordan & others* 2002 (6) SA 642 (CC) para 28.
[931] *S v Jordan & others* 2002 (6) SA 642 (CC) para 29.
[932] *S v Jordan & others* 2002 (6) SA 642 (CC) para 29.
[933] *S v Jordan & others* 2002 (6) SA 642 (CC) para 29. See also P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 586 – 587.

State has the power, as well as a moral duty, to prohibit antisocial conduct, through the use of criminal sanctions, where necessary. However, if the State does enact legislation to prohibit antisocial conduct, the legislation must be consistent with the Constitution.[934]

Minister of Justice and Constitutional Development v Prince (*Prince III*) seems to have struggled in finding a neat place for the personal possession of cannabis on the continuum.[935] The court, although not explicitly stated in the judgment, seems to have placed the cultivation and possession of cannabis, and other recreational drugs, towards the inner core of the continuum.[936] The court substantiated its conclusions by summarising previous Constitutional Court decisions, for example *Bernstein v Bester*, including foreign law jurisdictions, as well as referring specifically to the arguments in *Case v Minister of Safety and Security*.[937] In summary, *Prince III* concluded that the criminalisation to possess, cultivate and use "cannabis by an adult in private for his or her personal consumption in private and in the absence of children" unjustifiably infringed the right to privacy.[938] Part of the emphasis was specifically placed on the ideas surrounding the "right to be let alone".[939]

Prince III acknowledged the medical evidence that supports the prohibition of the

---

[934] *Prince v President, Cape Law Society, & others* 2002 (2) SA 794 (CC) para 108 (the thrust of *Prince II* was freedom of religion, and not privacy, however, these comments are apt in describing the State's duty to society); *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division & others* 2004 (1) SA 406 (CC). See also *Minister of Justice and Constitutional Development & others v Prince; National Director of Public Prosecutions & others v Rubin; National Director of Public Prosecutions & others v Acton & others* 2018 (6) SA 393 (CC) paras 71 – 75 (*Prince III*). Note also, *Stanley v Georgia* 394 US Reports 557 (1969), *Olmstead v United States* 277 US 438 (1928), *Ravin v State of Alaska* 537 P.2d 494 (1975) and *S v Motloutsi* 1996 (1) SA 584 (C).

[935] *Minister of Justice and Constitutional Development & others v Prince; National Director of Public Prosecutions & others v Rubin; National Director of Public Prosecutions and others v Acton & others* 2018 (6) SA 393 (CC) (*Prince III*). The issue was whether sections of the Drugs and Drug Trafficking Act 140 of 1992 and Medicines and Related Substances Control Act 101 of 1965 justifiably limited the rights set out in the Constitution, based on the values of an open and democratic society, in light of the factors listed in s 36 of the Constitution, with regards to the personal possession of cannabis. See para 40 of *Prince III*.

[936] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) paras 58 and 101. See also P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 590.

[937] *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC). Useful for the purposes of the thesis is the following from *Case*: Didcott J (the majority judgment) concluded that the prohibited possession of "indecent or obscene material" as defined in the repealed Indecent or Obscene Photographic Matter Act 37 of 1967, and the subsequent criminal sanctions, unjustifiably infringed the right to privacy defined in the Interim Constitution (ie Constitution of the Republic of South Africa Act 200 of 1993). Didcott J reasoned in *Case* that it was no business of the State nor of any other person with regards to what erotic material any person keeps in the privacy of their own home. Note, Langa J qualified his concurrence with the majority. He emphasised that the right to privacy is not absolute, but the court was not called on to decide the scope of the limitation. Langa J stated that an intrusion on the right to privacy, as was carried out in the past, cannot be permissible, unless it is sufficiently justified in terms of the limitation clause.

[938] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) (*Prince III*) paras 58, and 94 – 97.

[939] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) paras 71 – 75 (*Prince III*). This ties into the conclusion at the end of the discussion of *S v Jordan & others* 2002 (6) SA 642 (CC) above.

personal use of cannabis, due to the long-term harmful effects of prolonged use, and reinforced the notion that the State has a legitimate interest in prohibiting certain activities, even where these are pursued in the private sphere.[940] However, in its opinion, *Prince III* found that the medical evidence presented regarding the harmful effects of prolonged use as well as the healing effects of cannabis, which may outweigh the harm, was not necessarily conclusive.[941]

The court considered the arguments of Ngcobo J in *Prince II*[942] and concluded that the net cast by the legislation was far too wide in prohibiting the private use of cannabis, hence these restrictions were unreasonable and unjustifiable. The Constitutional Court sadly missed the opportunity to conclusively decide on whether the criminal sanctions on the private use of cannabis by an adult amounted to an unjustifiable infringement of the right to freedom of religion, belief or opinion. The focus was on the right to privacy.[943]

In *Prince III* the court focused on the essence of the right to privacy and did not clearly answer the question of how, in terms of the scope, the infringement amounted to an unjustifiable and irrational limitation of the right to privacy.[944] The arguments were to some extent circular, the crux being that the place where the cannabis is cultivated and/or consumed,

---

[940] See *Prince v President, Cape Law Society, & others* 2002 (2) SA 794 (CC) (ie *Prince II*) for a complete discussion of the medical evidence. Compare with the following cases that were discussed in *Prince III*: *Stanley v Georgia* 394 US Reports 557 (1969): dealt with the possession of indecent and obscene material. *Olmstead v United States* 277 US 438 (1928): was concerned with the unlawful sale, transportation etc. of intoxicating liquor between the individual states and that the covert operation was discovered by illegally tapping into a telephone conversation. Holmes J, in a separate judgment summarised this as follows (at 470) that "evidence obtained and only obtainable by a criminal act" cannot be used against the accused in a criminal trial, and that the "right to privacy had been unjustifiably infringed." See also *S v Motloutsi* 1996 (1) SA 584 (C). *Ravin v State of Alaska* 537 P.2d 494 (1975): similarly, to the *Prince*-applications, the prohibition against the private buying, selling and subsequent possession and use of cannabis. *Mistry v Interim Medical and Dental Council of South Africa & others* 1998 (4) SA 1127 (CC), and *Magajane v Chairperson, North West Gambling Board & others* 2006 (5) SA 250 (CC) held that warrantless inspections by professional boards or councils, and even in certain instances the police, when these have been informed of nefarious activity by fellow colleagues or from the public, may justifiably limit the right to privacy where the empowering legislation provides a comprehensive set of procedures and remedies. Note also, *Tap Wine Trading CC & another v Cape Classic Wines (Western Cape) CC & another* 1999 (4) SA 194 (C) held that information obtained illegally or unconstitutionally, may still be used where it furthers the administration of justice, taking into account the limitations placed on such evidence in terms of s 35 and s 36 of the Constitution, and, *S v Dube* 2000 (2) SA 583 (N) pointed out that the right to privacy will also not be infringed unjustifiably when a police trap is used to obtain evidence, however, all safeguards and applicable empowering provisions must have been followed.

[941] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) paras 63 – 82 (*Prince III*); P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 591.

[942] *Prince v President, Cape Law Society, & others* 2002 (2) SA 794 (CC) (ie *Prince II*).

[943] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) para 101 (*Prince III*). See also Section 15 of the Constitution and *Prince v President, Cape Law Society, & others* 2002 (2) SA 794 (CC) (ie *Prince II*).

[944] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) paras 83 – 86 (*Prince III*). See also *Centre for Child Law v DPP, Johannesburg & others* [2022] ZACC 35 paras 23 – 30.

by an adult, must be a private place, such as a garden or another place considered to be private.[945] But the court failed to provide a conclusive answer as to how the scope of privacy is infringed by the prohibition, especially in terms of the fact that the State has the power and moral duty to prohibit anti-social behaviour with criminal sanctions. It, like the court of first instance, merely turned to foreign legal jurisdictions and listed the dates when these jurisdictions had decided to enact laws that allowed for the personal consumption of cannabis.[946] The Constitutional Court did agree that purchasing and selling cannabis, especially since this may involve approaching a dealer, remains criminal behaviour – mainly due to the fact that "[d]ealing in cannabis is a serious problem in this country and the prohibition of dealing in cannabis is a justifiable limitation of the right to privacy."[947]

Another case in which the Constitutional Court found it difficult to place the infringement to privacy on the continuum was *Centre for Child Law v Media 24 Ltd*.[948] Here the issue was specifically justifying the anonymization of the identity of a minor child who has been involved in criminal matters, whether as a victim, accused or witness. The court itself admitted that anonymizing the identity of a child victim in a criminal matter "blurs the line between personal and communal interests", but in terms of the right to privacy, allows for the reasonable protection of identity, and thereby secures the autonomous growth and development of the victim's identity.[949] The court justified this approach by highlighting the distinction between the concepts of "public interest", which is a fact-based approach founded on a

[945] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) para 85 (*Prince III*). See also P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 591. See *NUMSA obo Nhlabathi & 1 other v PFG Building Glass (Pty) Ltd* [2022] ZALCJHB 292 where the court dismissed an application for review of the dismissal of two employees based on the consumption of cannabis. The court, based its findings on *Prince III*, stating that the Constitutional Court decriminalised the use of cannabis, in a private space by an adult, but did not re-classify cannabis as a plant. *Prince III* did not affect the Occupational Health and Safety Act 85 of 1993, which requires employers to provide a safe working environment for all employees, and to achieve that end, set out the requisite policies. These policies may include a zero tolerance for drug and alcohol consumption, and thereby include that employees be tested to ensure that they are not intoxicated or using a narcotic substance. *Prince III* did not prohibit employers from requiring that employees must be "drug-free" due to the nature and dangers of the working environment, alternatively they will be dismissed.

[946] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) para 79 (*Prince III*).

[947] *Minister of Justice and Constitutional Development & others v Prince; NDPP & others v Rubin; NDPP & others v Acton & others* 2018 (6) SA 393 (CC) para 88 (*Prince III*), see also P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 591. But that begs the question, although it is not linked to the topic of the thesis: how does one obtain the necessary seeds, etc, to start one's own private cultivation and production of cannabis for personal use, without some form of purchase?

[948] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC); see also *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 42, and G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 456 – 468.

[949] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC) para 48.

legitimate and genuine interest and where the information is beneficial to the public; and "what is of interest to the public", which amounts to mere curiosity and serves no real benefit.[950] In other words, the public's right to information regarding a criminal trial is by no means hampered when the names of child victims, accused or witnesses are anonymized.[951]

Mhlantla J reiterated the arguments from *Bernstein v Bester* which provides that there is a legitimate expectation for the protection of privacy in what is termed the "inner sanctum" or "truly personal realm", but this protection erodes away the more an individual inter-relates with the world around them, thereby diminishing the expectation of protection from the right to privacy. She conceded that finding a way to balance the right to privacy on the continuum is not always easy and neither is it always possible,[952] eg protection of a child's identity, which seems to have been placed closer to the inner sanctum, than in the public sphere. These circumstances, in her opinion, called for a hybrid solution.[953]

Similarly, Jaftha AJ in *Johncom Media v M*[954] held that the complete prohibition on publishing the identities of the parties and children in a divorce proceeding was an unjustifiable restriction placed on expression and was not catered for in terms of s 16, and could neither find justification in terms of s 36. The court, unanimously held that only in exceptional circumstances, and in terms of a court order, prohibiting the publication of the identities of the parties, including "any evidence that would tend to reveal the identity of any of the parties or any of the children", is less restrictive and more suitable, than a complete ban.[955] Jaftha AJ reiterated the point that the superior courts, as upper guardians of all minor children, have a "particular responsibility" in protecting their best interests.[956]

---

[950] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC) para 100. The court made reference to the following authorities in footnote 103 in this regard, these cases deal with defamation, however, specifically dealt with the point regarding what the public will find interesting and what is of public interest or what the public needs to know: *Financial Mail (Pty) Ltd & others v Sage Holdings Ltd & another* 1993 (2) SA 451 (A) at 464A – C; *National Media Ltd & others v Bogoshi* 1998 (4) SA 1196 (SCA) at 1212J; and *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 27.

[951] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC) para 100.

[952] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC) para 45.

[953] *Centre for Child Law & others v Media 24 Ltd* 2020 (3) BCLR 245 (CC) para 46. Note, the Criminal Procedure Amendment Act 16 of 2021, which came into operation on 9 February 2022, provides that the identity of a child who was either an accused, victim, or witness, may not be revealed at any stage before or after the trial, unless authorised in certain instances, as per the amendment. See *Government Gazette* 45893, of 9 February 2022.

[954] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 30 see also *Mail & Guardian Media Ltd & others v Chipu NO* 2013 (6) SA 367 (CC) paras 90 – 91.

[955] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 30 see also *Mail & Guardian Media Ltd & others v Chipu NO* 2013 (6) SA 367 (CC) paras 90 – 91.

[956] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 43. Note also, this article: P Gabriel 'The Protection of Personal Information Act 4 of 2013 and children's right to privacy in the context of social media' (2019) 82 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 605 at 611 – 612, although in the context of social media, children have a legitimate expectation that their privacy (including their personal information) will

Note also *Arena Holdings (Pty) Ltd t/a Financial Mail v South African Revenue Services*[957] where the former president, Mr Zuma and the South African Revenue Services (SARS) opposed the application and the appeal of Arena Holdings (Pty) Ltd and Amabhungane Centre for Investigative Journalism NPC for insight into Mr Zuma's tax records. The Constitutional Court confirmed the high court's order and findings, using s 36 of the Constitution (ie the limitation clause) to balance the rights of the respective parties, and held that there are instances where the public's interest in the tax affairs of statespersons (whether former or present), will override the individual tax payer's (ie state person's) privacy.[958] Put differently, where the disclosure of the information (ie tax records) "clearly outweighs the harm" that may be caused to the individual's privacy.[959] Quoting from *Johncom*[960] and *Mail & Guardian Media Ltd v Chipu*,[961] the court concluded that "absolute taxpayer secrecy" cannot exist to the detriment of freedom of expression. Although tax documents are sensitive in nature, those that have or hold executive State positions cannot hide from their responsibility towards the public merely under the guise of absolute confidentiality.[962]

The Supreme Court of Appeal held in *Smuts v Botha*[963] that where an individual[964] releases their personal information into the public domain, such as via a social media webpage, and the personal information is readily available in a public record, such as the Deeds Registry, and another publicises the personal information, then the individual can no longer claim that

be protected.

[957] *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13, and *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2021] ZAGPPHC 779.

[958] *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13 paras 124, and 129 – 146, and *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2021] ZAGPPHC 779 paras 8.9 – 8.10.

[959] *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13 para 143.

[960] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC), *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13 para 164, and *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2021] ZAGPPHC 779 para 8.12.

[961] *Mail & Guardian Media Ltd & others v Chipu NO* 2013 (6) SA 367 (CC) para2 92 – 93, *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13 para 166, and *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2021] ZAGPPHC 779 para 8.11.

[962] *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13 para 172, and 175 – 195.

[963] *Smuts & another v Botha* [2022] ZASCA 3. Botha has appealed the judgment, and the matter is to be heard on 9 November 2023 at the Constitutional Court, see Constitutional Court of South Africa 'Herman Botha v Bool Smuts and another'. *https://collections.concourt.org.za/handle/20.500.12144/38290* (Accessed: 23 October 2023) – the judgment has not been handed down.

[964] In terms of the Protection of Personal Information Act 4 of 2013 the individual or person releasing their personal information is called the data subject.

their privacy has been infringed,[965] ie they no longer have a legitimate interest to keep their information private. The Supreme Court of Appeal illustrated where the information or activity will be on the continuum when it set out that Mr Botha had himself placed his business activities into the public domain, and could no longer expect to be protected under the blanket of privacy when he receives uncomfortable and critical remarks, the information remained public, and so on the public sphere of the continuum.[966]

On 9 October 2024, the Constitutional Court finally handed down its judgment in *Botha v Smuts*.[967] The Constitutional Court held that an invidual's business address will rather be found on the public end of the spectrum, and their home address closer to the private end of the spectrum.[968] Some of the reasons given by the Constitutional Court include,[969] first, Mr Botha would have had an expectation that his home address be kept private, as the home address is "deeply intimate" information, which the public has little or no interest in.[970] Second, a business address, especially one such as an insurance brokerage, cannot be considered private, as that is where the public are able to contact the individual if they have an interest in what they offer.[971] Being involved in business activities, even if these are engaged with at a private home, are generally removed from the inner sanctum, as the individual is interacting with the "world outside."[972] Third, and interestingly, the court held that the ongoing publication of personal information, for longer than is required, would amount to an infringement of personal privacy.[973] Continuous publication of a post on an online platform, although initially lawful, may at some point become unlawful.[974] Fourth, the reason for the defamatory claim was based on his trapping activities, and these had nothing to do with his personal address.[975] Fifth, where an individual widely posts their business address on various online platforms they

[965] *Smuts & another v Botha* [2022] ZASCA 3 paras 8, 9, 18, 19, and 31.
[966] *Smuts & another v Botha* [2022] ZASCA 3 para 20.
[967] *Botha v Smuts & another* 2025 (1) SA 581 (CC). *Botha v Smuts* has produced four judgments, with each aspect having its own majority. The Constitutional Court partly upheld the order of the Supreme Court of Appeal. A complete discussion of the judgment, although relevant to the topic of this thesis will not be undertaken, because the judgment was handed down after the submission date. But for completeness some of the reasons for the varying majority opinions will be mentioned. The discussions of the Constitutional Court could also fall under the discussions for a legitimate expectation of privacy.
[968] *Botha v Smuts & another* 2025 (1) SA 581 (CC) in the introductory remarks before the start of the first judgment framed their finding based on the legitimate expectation.
[969] There is no majority as to the reasons for each conclusion, however, across the various judgments some of the reasons will set out in the text.
[970] *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 151 – 153, Kollapen J's judgment.
[971] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 136 of Kollapen J's judgment.
[972] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 137 of Kollapen J's judgment.
[973] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 192, 232, and 238 of Chaskalson AJ's judgment.
[974] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 193 and 240 of Chaskalson AJ's judgment
[975] *Botha v Smuts & another* 2025 (1) SA 581 (CC) paras 226 – 229 of Chaskalson AJ's judgment.

cannot now claim privacy, merely because the post, even though unrelated to the actual business, will harm their business activities. Commercial activities and economic rights or interests do not "carry any significant weight in . . . an application . . . founded on the right to privacy."[976]

In summary the Constitutional Court, in its latest judgment in *Botha v Smuts*, confirmed the principle in *Bernstein v Bester* that business activities, due to the nature of the interaction, will more likely be placed on the public sphere of the continuum. Put differently, private activities remain within the inner sanctum. Private activities included the consumption and possession of cannabis, as held in *Prince III*. By contrast, *S v Jordan*, dealing with commercialised prostitution, found that the State has a legitimate interest to regulate and criminalise moral conduct, although the conduct is engaged in private. Therefore, the application of the continuum has not always been that clear. This is best seen in circumstances where the individual has interacted within the public sphere, yet their identity had to be protected and kept private, such as in *Centre for Child Law v Media 24 Ltd* and *Johncom Media v M*. Or, where the status of the person, such in *Arena Holdings (Pty) Ltd t/a Financial Mail v South African Revenue Services*, will determine when sensitive information, such as tax records, may be made available to the public. What is evident is that each matter must be decided on its own facts as to whether the activity in that specific instance will be classified more on the public or private sphere on the continuum.

(iii) The inner sanctum

The third and final principle is the reasonableness of protecting the "inner sanctum" because each person needs an intimate space or personal sphere and this promotes a constitutional value, the protection of "one's own autonomous identity" or the "unencumbered self".[977] The Constitutional Court has agreed that the right encompasses a range of factors to consider, including the emotional and intellectual needs of a person within their private home.[978] The "inner sanctum" is the individual's colloquially termed "happy place" and encompasses a person's home and family, their physical and mental health, their character and standing within the community or business partners, as well as private photographs, embarrassing or not, as

[976] *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 234 of Chaskalson AJ's judgment and paras 251 – 255 of Rogers J's judgment.
[977] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 65. See also M Sánchez de Diego 'Right to one's own image in Spain: What it is and what it is not' (2018) 8 *Journal of Information Policy* 401 – 416.
[978] *Stanley v Georgia* 394 US Reports 557 (1969); *Minister of Justice and Constitutional Development & others v Prince; National Director of Public Prosecutions & others v Rubin; National Director of Public Prosecutions and others v Acton & others* [2018] ZACC 30, 2018 (6) SA 393 (CC) (*Prince III*).

well as thoughts and information that has been given or received in confidence,[979] these include private communications.[980]

The keeping of telephonic conversations and other private communications confidential and private and that they fall within the inner sanctum was illustrated in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice*.[981] The Constitutional Court held that the inner sanctum also includes private communications in the form of written exchanges, be they emails, short message service (SMS) or WhatsApp messages, and private telephone conversations. Madlanga J stated this a little differently: "[i]magine how an individual in that situation would feel if she or he were to know that throughout those intimate communications, someone was listening in or reading them".[982] There was a special emphasis placed on the communications between, first, an attorney and his client – these are subject to the highest standards of privilege in order to promote the rule of law, and the mass interception thereof seriously infringed this guaranteed privilege. Secondly, a journalist and his sources, whose sources are crucial to the performance of their journalistic functions, and have been held to be an essential part of the right to freedom of expression.[983]

---

[979] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) paras 65 – 69 and 72 – 73, see also Article 8 of the European Convention on Human Rights.

[980] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC). See also the comments in UNCHR (Sub-commission) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40 para 25.

[981] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC).

[982] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC) para 23:

> "The interception and surveillance of an individual's communications under RICA is performed clandestinely. By nature, human beings are wont – in their private communications – to share their innermost hearts' desires or personal confidences, to speak or write when under different circumstances they would never dare do so, to bare themselves on what they truly think or believe. And they do all this in the belief that the only hearers of what they are saying or the only readers of what they have written are those they are communicating with. It is that belief that gives them a sense of comfort – a sense of comfort either to communicate at all; to share confidences of a certain nature or to communicate in a particular manner. Imagine how an individual in that situation would feel if she or he were to know that throughout those intimate communications someone was listening in or reading them."

[983] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC) paras 115 – 119. Note, originally, Sutherland J in *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & other*s [2019] ZAGPPHC 384 declared the invasion of privacy justifiable to combat crime, in terms of the Criminal Procedure Act 51 of 1977, but only in so far as it related to the metadata, ie not the content of the written exchange or telephonic communication, but the fact that a message was sent or a phone call was made and to whom it was directed to. The Constitutional Court seems to have placed the emphasis not on the metadata, but on the content of the written exchange or telephonic conversation and that this is to be kept completely private – there is no mention regarding the use of the metadata. Note, metadata only describes the actual data, it is not the content of cell phone call, or short message service (known as SMS), or email, or other messaging and telephonic service. The metadata may be the Internet Protocol address (IP address) or location data or other cell phone or similar technological data that notes that a call was made and for how long, or that a SMS was sent, it can also provide the other parties IP or cell phone number – see Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 23 – 26, and E Larson 'Tracking criminals with Internet Protocol Addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 – 358. In light of the

Simply put, there is restricted access and interference to this private sphere by State authorities in matters of law enforcement, State security and the general protection of rights and freedoms in a democratic society.[984] However, Ackermann J warned that this is "not. . . unproblematic", especially in the determination of the scope of privacy as a whole.[985] The final conclusions of the Nordic Conference on the Right to Respect for Privacy of 1967, may provide some solution in this instance, by including additional elements, such as the "prohibition to use a person's name, identity or photograph without his/her consent, the prohibition to spy on a person, respect for correspondence and the prohibition to disclose official information." The right to privacy, in conjunction with other constitutional rights, is essentiual for the fulfilment of an individual's personality, and the right to maintain and establish relationships with other individuals. It certainly, as was mentioned at various points in Ackermann J's judgment, encourages the establishment of an individual's identity within society as a whole, "allowing a person to relate to him- or herself and to be able to relate to others in a meaningful way."[986]

O'Regan J in *NM v Smith*[987] elaborated on the interrelation between an individual's inner sanctum within a community and their interaction with others in that community. First, the Constitution recognises that human beings "may and do exclude" the community, in order to pursue interests and ambitions, however mundane, to live meaningfully.[988] This includes fostering and establishing human relationships within this sphere, as well as allowing daily life to take its course.[989] Second, O'Regan J held that the protection of the private daily sphere of an individual "highlights the interrelationship between privacy, liberty and dignity as the key constitutional rights which construct our understanding of what it means to be a human being,"

Constitutional Court's judgment in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC), the legislature has proposed changes to various sections in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) – see Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill B28- 2023, *GG* 49189 of 25 August 2023. *Shange & others v The State* [2017] 3 All SA 289 (KZP) illustrates how cell phone metadata was used (including location data) and that it may form a part of evidence that successfully leads to a criminal conviction, provided all procedural steps in obtaining that data have been followed. Compare with the United States' Supreme Court judgment in *Carpenter v United States*, 22 June 2018, 138 S. Ct. 2206 (2018) dealing with cell phone location data.

[984] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 72.

[985] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 72.

[986] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) paras 65 – 73, quotes in the text are specifically from the concluding remarks in para 73, see also *S v Naudé* 1975 (1) SA 681 (A). Note the eight conditions set out in the Protection of Personal Information Act 4 of 2013 – they echo these considerations from the Nordic Conference on the Right to Respect for Privacy of 1967. These eight conditions are briefly discussed in chapter 5 of the thesis.

[987] *NM & others v Smith & others* 2007 (5) SA 250 (CC) paras 130 – 131. For a commentary see G Penfold & D Milo 'Media freedom and the law of privacy: *NM & Others v Smith & Others (Freedom of Expression Institute as amicus curiae)* 2007 (5) SA 250 (CC): case comments' (2008) 1(1) *Constitutional Court Review* 311 – 334.

[988] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 130.

[989] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 130.

and that these rights may work independently or in conjunction with one another. This provides an overall framework in which to allow individuals to pursue an autonomous life within a broader community. This sense of autonomy "flows from our recognition of individual human worth, presupposes personal space within which to live this life."[990]

Ackermann J concluded his discussion on the scope of privacy in the US, Europe and Germany, the right to privacy only protects the most personal sphere of an individual's existence and not necessarily everything that may be in their personal knowledge.[991] The learned justice remarked that in "defining the right to privacy, it is necessary to recognise that the content of the right is crystallised by mutual limitation. Its scope is already delimited by the rights of the community as a whole (including its members)."[992]

Langa CJ in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*[993] elaborated on the essence of the right to privacy is to be left alone from the State, whether they are in their offices or cars or on their cell phones (as well as telephones), the State may only interfere with good reason. This includes, but is certainly not limited to what the person wishes to disclose to the public, otherwise considerations of privacy will come into play. Hence, where individuals "move beyond the 'intimate core'," and depending on the individual's position in society, privacy is not retained.[994]

The idea of being left alone is central to the right to privacy and the closer that the State or any other person (whether juristic or natural) moves into the core aspects of a person's life, the greater the expectation that an inner core will find protection. The protection of the private sphere is an important aspect for individuals within any democratic society.

The aspect of being left alone binds all three of the principles set out in *Bernstein v Bester* together. This is especially evident in the wording of s 14 of the Constitution, which is based on the acts of the past apartheid government.[995] Authoritarian governments tend to deny

---

[990] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 130.
[991] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 79.
[992] *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) para 79. See also footnote 84 of *Certification of the Constitution of the Republic of South Africa, 1996* 1996 (4) SA 744 (CC), where the court stated:

> "In southern and eastern Europe the general rule is for constitutions to contain express provisions protecting marriage and family life, while in northern Europe the tendency is the opposite. Germany (art 6 of the Basic Law) has an express provision, while Austria has none; the Belgian Constitution (art 22) simply protects family privacy while the constitution of the Netherlands has no such provision at all."

[993] *Investigating Directorate: Serious Economic Offences & others v Hyundai Motor Distributors (Pty) Ltd & others: In re Hyundai Motor Distributors (Pty) Ltd & others v Smit NO & others* 2001 (1) SA 545 (CC) para 16.
[994] *Investigating Directorate: Serious Economic Offences & others v Hyundai Motor Distributors (Pty) Ltd & others: In re Hyundai Motor Distributors (Pty) Ltd & others v Smit NO & others* 2001 (1) SA 545 (CC) para 16.
[995] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 133; see also *De Lange v Methodist Church & another* 2016 (2) SA 1 (CC) para 80.

the inner sanctum by allowing for routine searches of personal homes or private spaces. *NM v Smith* held that "privacy is a necessary part of a democratic society" and places "a constraint on the power of the State."[996] The denial of privacy is consequently a denial of human dignity and is impermissible within the bounds of a democratic society.[997] The protection of the private sphere provides for the much-needed "peace of mind" for individuals, since there will not be arbitrary interference in their lives. *NM v Smith* emphasised that it will only be in terms of exceptional circumstances where inroads into the privacy of an individual will be made, for example during commissions of inquiry – the right is qualified to the point of what is allowed by the law and the weighing of the interests of the individual, against those of the community.[998]

(c) The State's interests and privacy

Ackermann J in *Bernstein v Bester* seems to suggest that the "inner sanctum" is absolute or inviolable and that there is absolutely no possibility of interference. However, there are instances in which the protection of the "inner sanctum" might yield to other considerations. For example, the Constitution also guarantees freedom and security of the person, which includes freedom from all forms of violence whether in public or in private.[999] In the private sphere, this will include domestic violence, gender-based violence and further punishable crimes. Hence, individuals are not guaranteed an inviolable right to privacy. A women's protection from violence, cannot be sacrificed at the expense of "the inviolability of the home".[1000] The refusal of State officials to act cannot be tolerated in terms of a constitutional democracy, which guarantees that every citizen has the right to be free from all forms of violence, whether committed in public or private. This does not mean that privacy is less worthy of protection. The balancing and co-existence of the rights protected within the Constitution is what guarantees a dignified human life.[1001] This reiterates the point above, that in democratic societies the State has the power, as well as a moral duty, to prohibit certain offensive conduct, enforcing these through criminal sanctions.[1002]

The Constitutional Court, in *Tshabalala*,[1003] voiced its opinion against gender-based

[996] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 133.
[997] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 133.
[998] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 70. See also generally *Carmichele v Minister of Safety and Security & another* 2001 (4) SA 938 (CC).
[999] Section 12 of the Constitution, *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 134.
[1000] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 134.
[1001] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 134. See also *Carmichele v Minister of Safety and Security & another* 2001 (4) SA 938 (CC) paras 29 – 30 and 62.
[1002] *Prince v President, Cape Law Society, & others* 2002 (2) SA 794 (CC) para 108.
[1003] *S v Tshabalala; S v Ntuli* 2020 (5) SA 1 (CC) para 1, quoting *S v Chapman* 1997 (3) SA 341 (SCA).

violence, domestic violence and in general violence against women and children, emphasising that their private or domestic space should be a safe place to live and not a place of fear. The Constitutional Court also expressed the view that even in public spaces, women and children should be afforded protection to grow and continue with daily life without fear that they may be next. The majority in *Tshabalala*[1004] approved an oft quoted extract, from *Chapman*,[1005] although it deals specifically with rape, a crime that has become associated with gender-based violence. In *Chapman* the court emphasised the seriousness of the offence. It humiliates, degrades and brutally invades the privacy and dignity of the victim. Both the rights to dignity (including integrity) and privacy form part of "the ethos of the Constitution *and to any defensible civilisation*."[1006] Women may rightfully claim to enjoy their lives in peace and without fear, whether in public, as well as revelling in the peace and tranquillity of their own home, such enjoyment should not be diminished by fear.[1007]

As was illustrated in *Tshabalala* gender-based violence and violence in general, are often used to degrade the weaker members within communities, it goes to the heart of the principles of human dignity as well as privacy – that within a person's own private space, there should be no fear of attack. Although this thesis does not deal with gender-based violence, rape, etc. the above demonstrates that even where the violent act occurs in the sanctity of the personal space of the victim or the perpetrator, the courts and State still have the power to act and deal with the matter. Violent acts within the private sphere are vehemently condemned and hence the right to privacy is limited in such instances.

Based on the above, it may be best to view the inner sanctum, not just as a physical space, but also as a mental state of mind, a feeling, or an activity, ie individuals, be they adults or children, should be able to be active within public or find a space within their personal surroundings, where they may "just be" without the interference of others.

(d) Conclusion

Privacy is closely linked to self-worth, ie privacy provides individuals with the freedom to find a space (albeit mental or physical) in which to grow and develop their sense of being and

[1004] *S v Tshabalala; S v Ntuli* 2020 (5) SA 1 (CC) para 1.
[1005] *S v Chapman* 1997 (2) SACR 3 (SCA).
[1006] *S v Chapman* 1997 (2) SACR 3 (SCA) – emphasis part of the original.
[1007] Similar sentiments have been expressed in *Masiya v Director of Public Prosecution* 2007 (5) SA 30 (CC) para 78, *Director of Public Prosecutions, Kwazulu-Natal Pietermaritzburg v Ndlovu* [2024] 2 All SA 315 (SCA) paras 1, 72 – 76, and *Director of Public Prosecutions, Eastern Cape, Makhanda v Coko* [2024] ZASCA 59 paras 2, 6 and 95.

personality, without interference from others. The ability to protect information, and aspects of one's life, etc. under the right to privacy, enhances the dignity and gives value to an individual's life. Being able to keep information private and enjoying a private sphere, however, is just as important as being able to speak one's mind and impart and receive information. The right to freedom of expression, including its scope, is set out hereunder.

III FREEDOM OF EXPRESSION

(a) Introduction and historical context

Freedom of expression is one of the "cornerstone" rights within a democracy. It is based on the right that each individual may express their views, their thoughts and opinions in an open democratic society. It allows for the free-flowing exchange of ideas and information.[1008] However, its protection was often severely curtailed under the apartheid government. Rumpff JA in a separate dissenting judgment in *Publications Control Board v William Heinemann, Ltd*[1009] illustrated the fragility of freedom of expression, a "hard-won and precious asset" that is one of the first rights threatened by governments in general and thus easily lost.[1010] Freedom of expression definitely faced its fair share of opposition during the apartheid era. Rumpff JA encouraged that any suppression of the right should only be to the extent clearly determined by parliament, as parliament is a "product of political liberty".[1011]

Instead of preserving the right, the government rather suppressed it, to the extent of "[prohibiting] that with which one does not agree".[1012] Langa DCJ in *Islamic Unity Convention v Independent Broadcasting Authority*[1013] in dealing with the historical importance of the right, recognised that it had always found its place in the common law. He emphasised that certain forms of expression were severely curtailed, specifically, artistic expression and political opinions. The restrictions placed on one democratic freedom, Langa DCJ opined, systematically affected all other rights and freedoms, and thus democracy was denied. These restrictions, he found, would be incompatible with South Africa's "commitment to a society based on a 'constitutionally protected culture of openness and democracy and universal human

[1008] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 122; *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC) para 8.
[1009] *Publications Control Board v William Heinemann, Ltd and others* 1965 (4) SA 137 (A). Holmes JA and Potgieter JA concurred with Steyn CJ, Rumpff JA and Williamson JA both wrote separate dissenting judgments.
[1010] *Publications Control Board v William Heinemann, Ltd and others* 1965 (4) SA 137 (A) at 160E-H.
[1011] *Publications Control Board v William Heinemann, Ltd and others* 1965 (4) SA 137 (A) at 160E-H.
[1012] *Publications Control Board v William Heinemann, Ltd and others* 1965 (4) SA 137 (A) at 160E-H.
[1013] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC). See also *Smuts & another v Botha* [2022] ZASCA 3 para 15.

rights for South Africans of all ages, classes and colours'".[1014]

Both Van der Westhuizen J, in *Print Media SA v Minister of Home Affairs,*[1015] and Mogoeng CJ, in *EFF v Minister of Justice,*[1016] discussed the historical context in their respective judgments. In summary of the points expressed, and irrespective of print or spoken words, the right to freedom of expression was stifled based on censorship of various publications, songs and even television programs and movies, and this severe curtailment led to persons serving jail time or even being killed for certain utterances. In *Print Media SA* the thrust of the argument was based on censorship, in terms of the repealed Publications Act,[1017] where publications would be banned based on "vague criteria like 'indecent', 'obscene', 'offensive' and 'harmful to public morals'" or even "prejudicial to the safety of the State". The criteria were sourced from the government's preferred "narrow Calvinist and cultural notions of morality and good taste" and applied to all.[1018] The censorship was not only for local but also internationally produced content and would amount to either an age restriction on the one end to a complete ban on the other, depending on how obscene, indecent or objectionable the content was.[1019]

Mogoeng CJ, although highlighting the criminal consequences for those who incited protests against the apartheid regime, also emphasised that accepted expressions found their origin in the apartheid institution, amounting to conformity of thought and censorship.[1020] The value to express oneself, to vocalise hurt and thereby find solutions to heal is critical and cherished in our democracy. Where the expression causes no harm, the right should not be restricted.[1021] Kriegler J in *S v Mamabolo*[1022] and O'Regan J in *SA National Defence Union v Minister of Defence*[1023] had previously emphasised the importance of freedom of expression, based against the backdrop of South Africa's history of oppression.[1024]

[1014] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 27. See also *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 124.
[1015] Minority judgment in *Print Media South Africa and another v Minister of Home Affairs and another* 2012 (6) SA 443 (CC) para 94, the judgment agreed with the proposed order of Skweyiya J (majority judgment).
[1016] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 paras 42 – 44.
[1017] Publications Act 62 of 1974.
[1018] *Print Media South Africa and another v Minister of Home Affairs and another* 2012 (6) SA 443 (CC) para 94.
[1019] *Print Media South Africa and another v Minister of Home Affairs and another* 2012 (6) SA 443 (CC) para 94; *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 37.
[1020] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 42; *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 37. See also *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 76.
[1021] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 42.
[1022] *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 37.
[1023] *South African National Defence Union v Minister of Defence & another* 1999 (4) SA 469 (CC) para 7.
[1024] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 paras 43 – 44.

Freedom of expression is one of few unique rights within the Constitution, which provides for certain limitations within its wording, immediately setting out part of its scope; however, this has been held to merely provide for 'the ordinary bounds of the right to freedom of expression'.[1025] Section 16 reads as follows:

> "(1) Everyone has the right to freedom of expression, which includes
>
> *(a)* freedom of the press and other media;
>
> *(b)* freedom to receive or impart information or ideas;
>
> *(c)* freedom of artistic creativity; and
>
> *(d)* academic freedom and freedom of scientific research.
>
> (2) The right in subsection (1) does not extend to
>
> *(a)* propaganda for war;
>
> *(b)* incitement of imminent violence; or
>
> *(c)* advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm."

Skweyiya J, in *Print Media* described s 16 with the focus on s 16(2) that provides an "exclusionary list" of the kinds of speech that will not be protected under the right, whereas s 16(1) is seen as a non-exhaustive list of the kinds of speech that is protected. Briefly, whatever expression is not excluded from the list in s 16(2) must seek protection in terms of s 16(1).[1026] *Mamabolo*, sounded a warning that the courts "should be particularly astute to outlaw any form of thought control, however respectably dressed."[1027] However, *Mamabolo* further held that "[with] us it is not a preeminent freedom ranking above all others. It is not even an unqualified right."[1028]

The discussion of the right to freedom of expression will be in terms of the following topics: the importance of free expression, the structure of s 16 of the Constitution, the specific protections afforded by s 16(1) and lastly, a brief discussion on hate speech.

(b) The importance of free expression

The scope and aim or purpose of the right to freedom of expression are intrinsically linked. It

---

[1025] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 21.
[1026] *Print Media South Africa and another v Minister of Home Affairs and another* 2012 (6) SA 443 (CC) para 48.
[1027] *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 37.
[1028] *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 41; *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC) para 47.

embraces the flow of information, and the airing of opinions, to protect and promote "the moral agency of individuals."[1029] Skweyiya J acknowledged that at the core of the right is the need for individuals to communicate with one another, no matter how important or insignificant the communication is within a democratic society, as long as the communication remains within the legally set bounds of expression.[1030] In defining the scope of freedom of expression, the Constitutional Court has called for a generous approach.[1031]

The right of freedom of expression allows for the promotion of what is termed the "marketplace of ideas." The "marketplace of ideas" is an integral part of a free, democratic and vibrant society, and promotes the free exchange of beliefs, thoughts, ideas, and emotions about different issues unaffected by censorship, and forms a vital part of an individual's liberty.[1032] It encourages healthy debate, the airing of opinions, the exposure of mis-judgments and wrong-doing within government structures. Debate between individuals and within society stimulates and enhances truth finding, allowing the electorate to scrutinise political and social issues.[1033]

Freedom of expression is one of the most fundamental rights that the citizens of a country have in an open and democratic society. The idea of an open and democratic society is a norm that many countries aspire to – especially when reading and studying their "bills of rights".[1034] But not only is press freedom important, freedom of expression is a part of the important collective of rights that allow persons to express their opinions as individuals, or in the collective.[1035] Citizens are entitled to voice their opinions and concerns.[1036] In *DA v ANC*[1037]

[1029] *Print Media South Africa and another v Minister of Home Affairs and another* 2012 (6) SA 443 (CC) para 35.
[1030] *Print Media South Africa and another v Minister of Home Affairs and another* [2012] ZACC 22, 2012 (6) SA 443 (CC) para 35. See generally R Venter 'The role of freedom of expression in a democratic system (part 1)' (2018) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 52 – 87, and R Venter 'The role of freedom of expression in a democratic system (part 2)' (2018) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 308 – 343.
[1031] *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC) para 47.
[1032] 'What is Freedom of Expression' available at https://www.freedomforuminstitute.org/about/faq/what-is-freedom-of-expression/; accessed 7 February 2019; *Taylor and Western Guard Party v Canadian Human Rights Commission* [1991] 3 CRR (2d) 116 at 159 and 168; *Ex parte Simms* [1999] 3 All ER 400. See also *Case & another v Minister of Safety and Security & others* 1996 (3) SA 617 (CC) para 26; *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 37.
[1033] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 122.
[1034] The term is applied loosely as there are a myriad of names for the various legislative instruments that protect human rights. DW Freedman (assisted by RM Robinson & GE Pugsley – original text GE Devenish) 'Constitutional Law: Bill of Rights' in WA Joubert (founding ed) *Lawsa* vol 5(4) 2ed (2012) para 106; The Constitution of the Republic of South Africa, 1996, is an example of such an aspirational document, as well as the Canadian Charter of Rights and Freedoms and the United Kingdom's Human Rights Act, 1998. See also *S v Mamabolo* 2001 (5) BCLR 449 (CC).
[1035] *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security* [1996] ZACC 7; 1996 (3) SA 617 (CC) para 8.
[1036] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 123.
[1037] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC). See also *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC) para 8.

Cameron J canvased an example by interlinking freedom of expression with the right to vote.[1038] The right to vote only gains its true meaning and value where there is political debate and the voicing of opinions. This link between the two rights is integral to a democratic system of government. *Khumalo v Holomisa*[1039] described this as "the ability of citizens to make responsible political decisions and to participate effectively in public life."

Not only is freedom of expression linked to the right to vote but also to freedom of religion, belief and opinion, the right to freedom of association and the right to assembly.[1040] With the last two, it is the ability to meet and associate with like-minded individuals, where similar views and opinions are moulded, even where these are "particularly controversial or unpopular views or those that inconvenience the powerful."[1041] Importantly, freedom of expression is a right that focuses on the individual, allowing that person to express themselves in their individualistic style. It is one of the rights that is closely linked to the right to human dignity and the independence of the individual human being.

Case described an important, and at times (I venture to add) overlooked factor, when dealing with freedom of expression and that is tolerance. Tolerance of different opinions to that of one's own is important where each person's uniqueness is celebrated. That does not mean that individual views and opinions are less worthy or should be aborted. *Case* held that in "essence, it requires the acceptance of the public airing of disagreements and the refusal to silence unpopular views."[1042]

Langa DCJ in *Islamic Unity* agreed with the above, and highlighted that diversity and tolerance are central aspects of an open and democratic society. However, diversity may threaten democratic pluralism itself where it is the central focus of the protection of freedom of expression. Within open and democratic societies, a certain number of prohibitions will be permitted to protect the collective.[1043] These amount to certain forms of speech or expression

[1038] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) paras 124 – both freedom of expression and the right to vote were denied to many, especially the majority under apartheid.
[1039] *Khumalo & others v Holomisa* 2002 (8) BCLR 771 (CC) para 21.
[1040] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 124.
[1041] *Democratic Alliance v African National Congress & another* 2015 (2) SA 232 (CC) para 125. See also the comments made in *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 26 and *Smuts & another v Botha* [2022] ZASCA 3 para 15.
[1042] *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security* 1996 (3) SA 617 (CC) para 8. See also Langa DCJ in *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC); *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 47; and *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 74.
[1043] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 29. Note, s 1 of the Constitution lays out the basis and founding values of 'human dignity, the achievement of equality and the advancement of human rights and freedoms.'

that form a substantial threat to the stability of a community as well as constitutional values.[1044]

The Constitutional Court, in the opening lines of a judgment, in which allegations of incitement to commit a crime were levelled at the Economic Freedom Fighters,[1045] and tying in with the notions of tolerance, held that "even the most venomous of toxicities" must be emitted through "the virtual exhaust pipe" of freedom of expression in order to heal hurt, calm frustrations and thereafter focus on the building a peaceful future.[1046] When looking at it from this aspect, freedom of expression is a tool used to keep a democratic society stable, especially in terms of healing and finding a balance for any injustices committed.[1047]

Some of the more important aspects of the scope are discussed briefly below.

(c) Structure of section 16

(i) Introduction

Moseneke J summarised s 16 as containing two parts. The first part, ie s 16(1) protects and promotes expression that will be justified within a democratic society and any limitation of expression protected under s 16(1) must be considered in terms of the limitations clause, whereas s 16(2) sets out all the forms of speech that will not find protection under the Constitution.[1048]

(ii) Section 16(1): The meaning of expression

The Constitutional Court has often in explicit terms set out that only protected expression, ie that falling in terms of s 16(1) will find its place in a democratic society. This form of expression includes the media and press, artistic expression and academic debate. These forms of expression give value to public debate and promote democratic and constitutional values within society.[1049] The Constitutional Court has also gone as far as to point out that this may

---

[1044] In para 29, *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) sets out that the prohibitions in terms of free speech often led to the guarantee of a fair trial, or the protection of fair and peaceful elections, where speech "of an inflammatory or unduly abusive kind may be restricted".
[1045] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 6ffg.
[1046] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 1.
[1047] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 1.
[1048] *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC) para 47. See also Langa DCJ in *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 31.
[1049] *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International (Freedom of Expression Institute as amicus curiae)* 2006 (1) SA 144 (CC) paras 46 – 47; P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 672 – 673. See the comments of the SCA in *Smuts & another v Botha* [2022] ZASCA 3 paras 15 and 25. Regarding the protection of academic research or scientific research, see DW Thalder & M Steytler 'Time for Cinderella to go to the ball: Reflections on the right to freedom of

include certain forms of expression that may be excluded, depending on the circumstances, such as pornography, child pornography and commercial speech.[1050] These forms of expression, are also, easier to limit in terms of s 36 of the Constitution.[1051] The limitation clause must be considered where a law of general application seeks to limit those forms of expression that are protected by s 16(1) or where two or more rights are being balanced against each other.[1052]

The above was taken discussed in *De Reuck v DPP*.[1053] The Constitutional Court ruled that s 27(1) of the Films and Publications Act 65 of 1996, which concerns child pornography, was a reasonable and justifiable limitation of s 16(1) of the Constitution. Although child pornography fell into the scope of s 16(1), the court applied the limitations clause, and substantiated as follows: First, expression may be restricted where the expression is of no to little value within democratic societies, and it was held that child pornography has very little value within the South African society.[1054] Secondly, the Constitutional Court focusing on the purpose of the limitation, and held that this was to protect the dignity and privacy of children by preventing sexual grooming, and reinforcing the prohibition against sexual activities with children, which amounts to abuse and is an "evil in all democratic societies".[1055] Thirdly, s 27(1) of the Films and Publications Act did not place a blanket ban on the prohibition of possessing child pornography by researchers and documentary film makers, where these images "fall within legitimate academic or documentary projects". Section 22 of the Films and Publications Act provided for this exception, where persons apply, for legitimate academic research or documentary projects, to the relevant cabinet minister for an exception to possess or deal in the material.[1056]

---

scientific research' (2021) 138(2) *South African Law Journal* 258 – 286.

[1050] *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and others* 2004 (1) SA 406 (CC) para 30, P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 673.

[1051] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 21; *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC) para 47; *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 46. *Johncom Media v M* described s 16 as setting out the ordinary bounds of freedom of expression. However, emphasised that there may be further limitations placed on it by s 36 of the Constitution, ie the limitation clause (para 21).

[1052] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 35.

[1053] *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and others* 2004 (1) SA 406 (CC). See also *Du Toit v The Magistrate & others* 2016 (2) SACR 112 (SCA) paras 13, and 16 – 17.

[1054] *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and others* 2004 (1) SA 406 (CC) paras 59 – 60, and *Du Toit v The Magistrate & others* 2016 (2) SACR 112 (SCA) para 13.

[1055] P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 674, *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and others* 2004 (1) SA 406 (CC) paras 64 – 65.

[1056] *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and others* 2004 (1) SA 406 (CC) paras 71 – 79; P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 674. This does open the question of whether adult pornography, as opposed to child pornography, has any value within

It deserves noting that unbridled attacks on any institution, including the courts and their functionaries, the Legal Practice Council (LPC), the Judicial Service Commission (JSC), and so on, especially by legal practitioners or officers of the court, will generally not be protected under freedom of expression. *Chalom* warned that "unfounded, offensive, insolent and vexatious allegations" made against a government structure such as the LPC, in court papers, shall not be tolerated by the courts, including personal attacks on the judiciary. *Chalom* emphasised that everyone has inherent dignity and that this right must be respected and protected, and warned that the "trampling of these values cannot be promoted and be associated with an officer of the court".[1057]

Expression includes symbols. The SCA confirmed in *Afriforum NPC v Nelson Mandela Foundation Trust and others*[1058] the Equality Court's[1059] conclusion that expression includes symbols. The facts find their origin in the "Black Monday" protests. The old South African flag had been displayed prolifically during these protests. The SCA confirmed that the public display of the old South African flag by individuals and organisations amounts to hate speech. However, unlike the Equality Court,[1060] the SCA did not ban the private display of the old South African flag, as this would amount to an unjustified infringement of the inner sanctum.[1061] The SCA held that prohibiting hate speech did not extend to personal or private communications.[1062] This thesis focusses on communications, etc. that are in the public realm, and hence this point will not be further explored. The court did provide the following proviso with regards to the display of the old South African flag within private homes, namely that there are instances where the private display may amount to hate speech. These include situations where the display is used to indoctrinate persons who are vulnerable to influences,

a democratic society. It has been argued that it does play a vital role in assisting individuals "to make important life choices about their true sexual identity" (P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 674). However, this is beyond the scope of this thesis – for more on this debate, see P de Vos & W Freedman (eds) *South African Constitutional Law in Context* 2ed (2021) at 674 – 675 and the sources quoted therein.

[1057] *South African Legal Practice Council v Chalom* [2020] ZAGPPHC 663 para 54. Human dignity is one of the founding principles of the Constitution.

[1058] *Afriforum NPC v Nelson Mandela Foundation Trust & others* [2023] ZASCA 58.

[1059] *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC).

[1060] The Equality Court ordered a complete ban against the display of the old flag which also included private homes. The court argued that this amounted to a just and reasonable limitation of the right to freedom of expression because it was in private homes where many domestic workers are employed. See *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC). The Equality Court acknowledged that the old flag should not be completely banned, but that it should be kept for historical purposes, namely, "confined to genuine artistic, academic or journalistic expression in the public interest".

[1061] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 paras 69 – 73.

[1062] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 para 72.

eg older and younger members of society.[1063] The case is also discussed again below.

(iii) Section 16(2): Limits to freedom of expression

The courts protect the right to freedom of expression, vehemently, but this does not mean that every utterance made in pursuance of the notion of freedom of expression, is given a carte blanche protection. Statements that are defamatory or incite hatred, especially those that lead to violence or propagate war are not protected forms of expression.[1064] Hate speech and defamation are discussed under their own headings later in the chapter.

There are however instances where the right to freedom of expression should be curtailed for the benefit of individual persons, as well as society as a whole,[1065] and the limitation must be reasonable.[1066] Broadly, freedom of expression will be limited when "national interests, our democracy, the dignity or physical integrity of people or property could be imperilled."[1067] The constitutional guarantee of freedom of expression, in s 16(2), "places limits upon its exercise," as briefly mentioned above. Where this goes beyond an impassioned expression and advocates hatred or instituting incitement to cause harm, those limits are overstepped and the expression loses any constitutional protection.[1068] Further, s 16(2) defines those limits to which freedom of expression will not extend.[1069] Certain expressions do "not deserve constitutional protection," as these forms of expression will adversely affect the founding constitutional principles of dignity, equality and freedom.[1070] There are three broad categories regarding expression that are not protected, namely expression that incites (a) propaganda or war, and (b) imminent violence, and (c) what is referred to as hate speech.[1071]

In illustration of the above, the SCA in *Premier of the Western Cape Province v The Public Protector*[1072] discussed the interpretation of s 16(2)*(b)*, as not all expression will be

[1063] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58.
[1064] Section 16(2) of the Constitution, *Holomisa v Argus Newspapers Ltd* [1996] 1 All SA 478 (W); *Print Media South Africa & another v Minister of Home Affairs & another (Justice Alliance of South Africa & another as amici curiae)* 2012 (6) SA 443 (CC) para 48; *Hotz & others v University of Cape Town* [2016] 4 All SA 723 (SCA).
[1065] *Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International* 2005 (8) BCLR 743 (CC) para 47.
[1066] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 47.
[1067] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 46.
[1068] *Hotz & others v University of Cape Town* [2016] 4 All SA 723 (SCA) para 67, *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 32.
[1069] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 76.
[1070] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 32.
[1071] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 33. Hate speech will receive its own discussion later in this chapter.
[1072] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16. The facts are that the former Premier of the Western Cape Province, Ms Helen Zille, had after a visit to Singapore, tweeted certain remarks regarding the impact of colonialism and the possible lessons that South Africa, based on her

categorised as hate speech, especially "since hate speech goes beyond mere offensive expression".[1073] The SCA pointed out that there are "two critical requirements" used in the interpretation of s 16(2)*(b)*, namely, first, objectively speaking, there must be an intention to incite violence, and secondly, that the violence is imminent, or as described as "'impending, or close at hand."[1074] In deciding whether these requirements have been satisfied, the intention to influence another's behaviour must be present as this is a fundamental component of incitement.[1075] The SCA in *Premier of the Western Cape Province v The Public Protector* stated that "insensitive speech still falls under the purview of protected speech".[1076] Even though, the views expressed are unpopular or "insensitive to people's race, religion, or gender",[1077] these should not be silenced at random.[1078] The SCA held, in term of s 16(2)*(b)* that although the speech was offensive, shocking and disturbing, the words were never meant to "incite violence" or bring about an "imminent [threat of] violence".[1079] The SCA in *Afriforum v Nelson Mandela Foundation*,[1080] discussed above, and again below, correctly found that the prohibition on hate speech does not extend to personal or private communications – everyone does need a trusted individual with whom they can vent. However, even private communications may amount to unprotected expression, especially where vulnerable individuals are influenced into action, or to openly express hate, based on private communications where feelings of hate and anger are expressed.[1081]

(iv) Conclusion

The limitations mentioned thus far, do not necessarily deal with the specific limitations that privacy places on freedom of expression. These limitations, however, are important to note as they form the basis of the rights as well as the protection that is afforded in terms of s 16 of the

experiences in Singapore, should learn. This unleashed an incredibly strong reaction from Twitter users, culminating in the Public Protector investigating as to whether Ms Zille had breached the Ethics Code, that was drafted in terms of the Executive Ethics Act 82 of 1998, in light of s 136 of the Constitution.

[1073] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 22.

[1074] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 33.

[1075] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 34; and *EFF & another v Minister of Justice and Constitutional Development & another* 2019 (2) SACR 297 (GP).

[1076] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 36.

[1077] E Ugland & JL Lambe 'Newspaper theft, self-preservation and the dimensions of censorship' (2010) 15(4) *Communication Law and Policy* 365 at 379.

[1078] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 para 36; and *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 79.

[1079] *Premier of the Western Cape Province v The Public Protector & another* [2022] ZASCA 16 paras 38 – 39.

[1080] *Afriforum NPC v Nelson Mandela Foundation Trust & others* [2023] ZASCA 58.

[1081] Section 16(2) of the Constitution, see also *SAHRC obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC) paras 98 – 100, and *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 44.

Constitution. Freedom of expression will not, as a cornerstone to any democratic society, be allowed to be trampled on and restricted, without good reason.

(d) Specific protections afforded by section 16(1)

The following is a brief discussion of two important aspects of protected expression. The Protection of Personal Information Act 4 of 2013 (POPI) will impact press freedom and the right to receive and impart information in light of protecting personal information, which is discussed in the next chapter. What is useful to note, at this stage is what the courts have held thus far on these two crucial aspects of freedom of expression, and the function they serve in a democratic society.

(i) Press freedom

One of the sentinel aspects of freedom of expression is the crucial role that the press or media play within a functioning democracy. To encroach on press freedom is often a blow to the public's "right to a healthy unimpeded media."[1082] The vital function that press freedom plays as well as the ability to limit it, where strictly necessary, is dealt with in the section dealing with the balancing of the rights to privacy and freedom of expression, hereunder.

(ii) Convey and receive information

Generally, with regards to s 16(1)*(b)*, freedom of expression is impoverished where the ability to not only convey information, but the ability for persons to receive information is limited. Freedom of expression is also limited where ideas cannot be freely exchanged. Mokgoro J explained this as the ability to share and inform as well as adjust a person's own personal opinion and thereby what they express.[1083] This is the concept behind the above-mentioned marketplace of ideas, where expression is used to shape, what has been referred to as the conversation of society, allowing societies to empower individuals but also encourage the collective. The fundamentality of "the right to receive others' expressions has more than merely instrumental utility," it establishes the basis for the individual's right to impart the information

[1082] *Print Media South Africa & another v Minister of Home Affairs & another* 2012 (6) SA 443 (CC) para 54. The European Court of Human Rights pointed out that this includes maintaining archives, including internet archives, see *Times Newspapers Ltd (Nos. 1 and 2) v The United Kingdom* [2009] ECHR 451 para 27. As has been demonstrated in Chapter 3, although the keeping of archives is a function of the press in terms of their right to freedom of expression and information, it must be balanced with an individual's right to privacy, where an infringement has been proven, and a suitable remedy must be put in place. See also A Wiśniewski 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 at 113.

[1083] *Case & another v Minister of Safety and Security & others* 1996 (3) SA 617 (CC) para 25; I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) 350 – 351.

or expression.[1084] In *Blind SA v Minister of Trade, Industry and Competition*[1085] the Constitutional Court highlighted the importance of publishers, etc. providing resources to those who have print and visual impairments in the form of informative texts and literary works so that they too are able to not only impart but also receive information in light of s 16(1)*(b)*.[1086]

(e) Hate speech

Majiedt J in *Qwelane v SAHRC* vividly wrote: "Hate speech is the antithesis of the values envisioned by the right to free speech – whereas the latter advances democracy, hate speech is destructive of democracy."[1087] Hate speech goes beyond mere offense, it provokes, vilifies, shocks, and disturbs open-minded, tolerant members of a democratic society, who have been exposed to unpopular views.[1088] The expression must not merely be hurtful, as hurtful speech may only aim to upset or wound another.[1089] The court applied the reasonable person test as

---

[1084] *Case & another v Minister of Safety and Security & others* 1996 (3) SA 617 (CC) para 26; I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) 350 – 351.

[1085] *Blind SA v Minister of Trade, Industry and Competition & others* [2022] ZACC 33.

[1086] *Blind SA v Minister of Trade, Industry and Competition & others* [2022] ZACC 33 para 72.

[1087] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 78. See also W Brugger 'The treatment of hate speech in German constitutional law (part I)' (2003) 4 *German Law Journal* 1 – 22 and W Brugger 'The treatment of hate speech in German constitutional law (part II)' (2003) 4 *German Law Journal* 23 – 44, although dealing with the German Law perspective, the author explains and compares hate speech with permitted speech and provides useful descriptions of the relevant concepts. For a discussion on hate speech and the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 see ME Marais 'Hate speech in the Equality Act following the Constitutional Court judgment in *Qwelane v SAHRC*' (2023) 26 *Potchefstroom Electronic Law Journal* 1 – 33. In relation to hate speech and the internet, and the increase in "cyberhate related crimes", see L Leets 'Responses to internet hate sites: Is speech too free in cyberspace?' (2001) 6(2) *Communication Law & Policy* 287 – 317, although it is a discussion from an US perspective, it still provides insights as to how "cyberhate" may influence individuals committing "real world" crimes. For a discussion on how civil defamation laws can be utilised in hate speech matters, see CR Carlson & C Terry 'The devil's in the details: How countries' defamation laws can (and can't) combat hate speech' (2023) *Journalism Practice* 1 – 23 where the authors compare German, Brazil and US laws. Although this article does not feature South Africa, it provides useful insights and ideas to consider in hate speech matters where an individual sues for defamation. For an insight as to how social media is being used to recruit and radicalise internet users and the difficulty in combatting radicalisation, especially where the messages sent are encrypted, see B Farrand '"Is this a hate speech?" The difficulty in combating radicalisation in coded communications on social media platforms' (2023) 29 *European Journal on Criminal Policy and Research* 477 – 493.

[1088] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 81, and *Chinese Association v Henning & others* (Gauteng Local Division, Johannesburg sitting as the Equality Court) unreported case no EQ2/2017 (28 July 2022) para 208, compare with *Chinese Association, Gauteng v SABC 2* (Broadcasting Complaints Commission) unreported case no 02/2020 (6 March 2020), and *Afriforum v Economic Freedom Fighters & others* [2022] ZAEQC 2. See also W Brugger 'The treatment of hate speech in German constitutional law (part I)' (2003) 4 *German Law Journal* 1 at 11.

[1089] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) paras 135 – 144. The Constitutional Court specifically stated:

> "[139] With respect to the term 'hurtful', much of what is relevant to the justification analysis has already been discussed. The importance of the right to freedom of expression on the one hand and the importance of the purpose of the limitation of that right, namely to protect the equally important rights to equality and dignity by way of prohibiting hate speech, have been expounded. So too, the nature and extent of the limitation and the relation between the limitation and its purpose. However, it is here that the usefulness of the term 'hurtful' becomes less clear. If speech that is merely hurtful is considered hate speech, this sets the bar rather low. It is an extensive limitation. The prohibition of hurtful speech would certainly

follows: objectively taken, do the impugned statements both hurt and incite harm against those that are the subject of the impugned statements.[1090] In *Qwelane* the expression was aimed at stigmatising the sexual orientation of members of society, namely those that are a part of the LGBT+ community.[1091] The court held that there are no less restrictive means, other than a complete prohibition of the statements written by Mr Qwelane. The statements had "vilified the LGBT+ community as 'animals', as less than human beings. Their sexual preferences and relations were degraded to bestiality".[1092] The statements were homophobic, striking not only at the "dignity of members of the LGBT+ community", but also contributing "to an environment that serves to delegitimise their very existence and their right to be treated as equals".[1093] Majiedt J concluded "that Mr Qwelane's abhorrent article [constituted] hate speech".[1094]

In *Hotz v University of Cape Town*,[1095] the court, quoting with approval from *Mamabolo*[1096] and *Islamic Unity Convention*[1097] said, the "issue regarding the content of the slogans, whether painted on the War Memorial and the bus stop or worn on a T-shirt, as well as statements, such as those made by the third appellant in the confrontation with a student, is

---

> serve to protect the rights to dignity and equality of hate speech victims. However, hurtful speech does not necessarily seek to spread hatred against a person because of their membership of a particular group, and it is that which is being targeted by section 10 of the Equality Act. Therefore, the relationship between the limitation and its purpose is not proportionate."

[1090] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) paras 95 – 96, and 176.

[1091] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) paras 145 – 146. LGBT+ is an acronym and stands for Lesbian, Gay, Bisexual and Transgender individuals. The "+" allows the acronym to be expanded to include other forms of sexuality and gender such as Intersex, Queer and Asexual, etc – see footnote 3 in *Qwelane*.

[1092] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 165.

[1093] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 168.

[1094] *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC), specifically para 181, see the arguments in paras 145 and 164 - 182. Mr Qwelane had compared the lifestyle and sexual preference of gay men to that of bestiality – these statements "evoked universal umbrage" and the statements were considered by many to strike at the heart of "dignity and self-worth" by delegitimising human beings for ultimately being who they are, and how society accepts them. See paras 1 – 12 regarding the facts in this matter. The Constitutional Court concluded:

> "[182] There can be no question then that Mr Qwelane's statements constitute hate speech. Mr Qwelane was advocating hatred, as the article plainly constitutes detestation and vilification of homosexuals on the grounds of sexual orientation. He was publicly advocating for law reform in favour of the removal of legal protection for same sex marriages. In doing so, he was undermining the protection of the law, the dignity of the LGBT+ community and the public assurance of their decent treatment in society as human beings of equal worth, deserving of human dignity and the protection and enjoyment of the full panoply of rights under the Constitution. In the context of hate speech prohibitions as civil remedies, a proven causal link between the hateful expression and actual harm is not required."

[1095] *Hotz & others v University of Cape Town* [2016] 4 All SA 723 (SCA) para 67. *Hotz* resulted from the "fees must fall campaign" which led to damage to property and included strongly worded and hurtful statements.

[1096] *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 28; see also *The Citizen 1978 (Pty) Ltd and others v McBride* 2011 (4) SA 191 (CC) paras 99 – 100.

[1097] *Islamic Unity Convention v Independent Broadcasting Authority & others* 2002 (4) SA 294 (CC) para 32.

a delicate one." The SCA insisted that a robust approach must be taken, as the ability to be heard and express "hurt, pain and anger" by those that have been oppressed or disempowered, is vital where the Constitution promotes the freedoms in sections 15 to 19 of the Bill of Rights, namely, "conscience, expression, assembly, association and political participation".[1098] In terms of s 16(2)*(c)* of the Constitution, a person inciting another to cause war, imminent violence or harm will not be able to invoke the protection of freedom of expression.[1099]

The Constitutional Court in *SAHRC obo SAJBD v Masuku*,[1100] Khampepe J, referencing *Qwelane*, reiterated that for an impugned statement to amount to hate speech, it must, objectively considered, be both harmful and hateful.[1101] Khampepe J proceeded to examine the statements made by Mr Masuku, and concluded that at least one of the four statements amounted to hate speech. In this particular statement Mr Masuku insinuated that those of the Jewish faith identify themselves as Zionists are no different from Adolf Hitler. Any mention of Hitler immediately brings to mind his anti-Semitic policies, etc.[1102] Put differently, these statements were specifically aimed at harming and inciting hate against those who profess that

---

[1098] *Hotz & others v University of Cape Town* [2016] 4 All SA 723 (SCA) para 67, *S v Mamabolo* 2001 (5) BCLR 449 (CC) para 28.

[1099] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 32; see also *EFF & another v Minister of Justice and Constitutional Development & another* 2019 (2) SACR 297 (GP).

[1100] *South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC). Important to note is that the Constitutional Court was alive to the fact that the judgment would carry ramifications, and pronounced in para 2 the following:

> "It should be said at this earliest opportunity that what this Court is not called upon to do is to make any pronouncement on that situation, which is a concern of international relations and not a justiciable issue. To pronounce on this situation would be both wholly inappropriate and totally irrelevant to the legal questions that are the objects of our attention."

The SCA's order in *Masuku & another v SAHRC obo South African Jewish Board of Deputies* 2019 (2) SA 194 (SCA) was overturned, and the Equality Court's order (see *SAHRC v Masuku & another* 2018 (3) SA 291 (GJ)) was re-instated with some adjustments.

[1101] *South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC) para 122, reads as follows:

> "After giving due consideration to the debate as to whether the phrase "that could reasonably be construed to demonstrate a clear intention" connotes an objective or subjective test, this Court held that—
>
> > 'it is plainly an objective standard that requires a reasonable person test. This is based on the gloss "reasonably be construed" and "to demonstrate a clear intention", implying an objective test that considers the facts and circumstances surrounding the expression, and not mere inferences or assumptions that are made by the targeted group.'"

See *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) para 96. The court in *Masuku* had declared that the use of the word "hurtful" was constitutionally vague, and thus unjustifiably limited the right of freedom of expression. See *South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC) para 120 – 133, *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) paras 155 – 157, and also J Phillips '*South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku*: The rejection of the International Holocaust Remembrance Alliance definition' (2023) *South African Journal on Human Rights* 1 at 8.

[1102] *South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC) paras 156 – 160, and also J Phillips '*South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku*: The rejection of the International Holocaust Remembrance Alliance definition' (2023) *South African Journal on Human Rights* 1 at 9.

they are Jewish or Zionist. The other three statements, although hurtful, were not only aimed at Zionists or Jews, but at those that supported Israel through pro-Israel organizations or the Israeli Defense Force.[1103] Limiting hate speech underscores South Africa's international obligations to "curb incitement of offences that seriously threaten the public interest, national security, the dignity or physical integrity of individuals – our democratic values."[1104]

Solidarity v Black First Land First[1105] dealt with the issue of hate speech in light of celebrating the death of children where a walkway collapsed at the school at which these children were in attendance. The court wrote an extensive judgment, basing much of its reasoning on *Qwelane.*[1106] The court declared the comments as hate speech and reasoned that the celebration of the death of these children, not only vilified them but also robbed them of their dignity, equality and freedom. The families were not only mourning the death of their children but were also faced with a disturbing celebration of their deaths as amounting to a racial victory.[1107]

The phrase "a picture is worth a thousand words" took on a new dimension in *Afriforum NPC v Nelson Mandela Foundation Trust,*[1108] which is also discussed above. The SCA in *Afriforum NPC v Nelson Mandela Foundation Trust*[1109] confirmed the decision of the Equality Court[1110] where it held that the deliberate display of the old South African (apartheid) flag,

---

[1103] *South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another* 2022 (4) SA 1 (CC) paras 161 – 166, and also J Phillips '*South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku*: The rejection of the International Holocaust Remembrance Alliance definition' (2023) *South African Journal on Human Rights* 1 at 9.

[1104] *EFF & another v Minister of Justice and Correctional Services & another* [2020] ZACC 25 para 47.

[1105] *Solidarity & another v Black First Land First & others* [2022] ZAEQC 1. The facts are as follows: the members of Black First Land First movement celebrated when a school building collapsed, killing three (the judgment also mentioned four) white children. The issue before the Equality Court was whether this amounted to hate speech.

[1106] *Solidarity & another v Black First Land First & others* [2022] ZAEQC 1 paras 31 – 54, and *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC).

[1107] *Solidarity & another v Black First Land First & others* [2022] ZAEQC 1 paras 55 – 107. The court stated in its argument:

> "98. There can be no greater advocacy of hatred than to rejoice and celebrate the death of innocent children because of the fate relating to their colour of their skin. There can also be no greater advocacy of hate speech to proclaim and celebrate the death of another human being, and to proclaim such death as a victory. The hatred and hate speech is galling even more so when those who have died were fallen by a tragedy and their only crime according to the respondents is because they are the [offspring] of white parents whom the respondents categorised as land thieves."

[1108] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58.

[1109] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58.

[1110] *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC). The case was specifically brought in terms of s 10 of the Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000. Note: Afriforum NPC is a non-profit organisation which seeks to protect and promote the interests of the Afrikaans people in South Africa. *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC) para 17. Afriforum was supported by the second amicus curiae, namely, Federasie van Afrikaanse Kultuurvereniginge ("FAK"). The Nelson Mandela Foundation Trust,

during the so-called "Black Monday" demonstrations, amounted to a form of hate speech. The old flag with all the symbolism that it contains, polarises rather than encourages interaction between South African citizens, it certainly did not encourage the aim of "one nation united in its diversity".[1111] Similar arguments have been raised regarding the display of the Nazi swastika.[1112] The SCA held that the display of the old flag "provides fertile ground for the violence and brutality of racism", and that the Equality Act, in conjunction with the Constitution, is aimed at eradicating hate speech, unfair discrimination, and harassment, based on race,[1113] as it "demeans, humiliates and creates a hostile and intimidating environment for victims of apartheid".[1114]

(f) Conclusion

The right of freedom of expression is certainly one of the many rights that are jealously guarded in many jurisdictions around the world, as it has been held, in more or less the same wording:[1115] "the importance of freedom of expression is fundamental in a modern democratic

---

referred to as "the Foundation", was established by the late former president, Mr Nelson Mandela, shortly after he retired from office in 1999. The judgment describes it as follows: "Its vision is 'a society that remembers its past, listens to all its voices, and pursues social justice'". Its mission is "to contribute to the making of a just society by promoting the legacy of Nelson Mandela, providing an integrated public information resource on his life and times, and convening dialogue around critical social issues". *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC) para 16. The Foundation was supported by the second appellant, the South African Human Rights Commission and the first amicus curiae, Johannesburg Pride NPC. The facts, main submissions and issues discussed in *Nelson Mandela Foundation Trust v Afriforum* are as follows: on 30 October 2017, Afriforum organised protests against farm murders. During the demonstrations, branded "Black Monday", people carried and thus displayed the old South African flag. The Nelson Mandela Foundation took issue therewith, through the vivid personal recollections of its chief executive officer, how African people were dehumanised under the apartheid era, and the visual display of the old flag involuntarily brought to mind these painful recollections (paras 23 – 26). The matter, essentially, turned on two issues: (1) the symbolism of the old flag, and (2) the context of hate speech in light of freedom of expression.

[1111] *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC) paras 210 – 203. See *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 paras 40 – 51.

[1112] *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC) para 68 – the submissions of the second and third respondents namely, the Minister of Justice and Correctional Services and the Department of Justice and Correctional Services. As set out above, in para 186 the Equality Court agreed with the Foundation that the old flag should not be displayed in private homes, as this is where black people are often employed and they will find such an open display as offensive. Further, the youth cannot, through the display of hurtful, divisive symbols that harbour racial views, be encouraged to openly express them. In para 201, as stated above, the Equality Court provided the following proviso: where the old flag is displayed in light of "genuine artistic, academic or journalistic expression in the public interest" and for historical purposes, such expression will be protected (see *Nelson Mandela Foundation Trust & another v Afriforum NPC & others* [2019] 4 All SA 237 (EqC)). See also *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 para 58 regarding the display for historical, academic and journalistic expression. The SCA did not confirm the ban against the display of the old flag within a private space, this amounted to an infringement on the right to privacy – see paras 71ffg.

[1113] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 para 56.

[1114] *Afriforum NPC v Nelson Mandela Foundation Trust and others* [2023] ZASCA 58 para 67.

[1115] *R (on the application of British Broadcasting Corporation and another) v Secretary of State for Justice* [2012] 2 All ER 1089 para 73 (per Neuberger LJ) as well as paras 39 – 43 and *Masuku & another v SAHRC obo South African Jewish Board of Deputies* 2019 (2) SA 194 (SCA) para 16; see also in the United States Supreme Court

society". This is evident from what has been discussed above. Kriegler J remarked that South Africa's freedom of expression is no less important than that found in other jurisdiction, including the United States, however, unlike the United States, freedom of expression is not an absolute right and will face limitation in appropriate circumstances.[1116] Expression adds value to human dignity, the right to vote, etc. as well as self-worth and encourages healing and growth within communities and society as a whole. The limitations that are made with specific reference to privacy, but including dignity and other protected rights, are dealt with below.

IV HOW THE CASES HAVE BALANCED PRIVACY AND EXPRESSION

(a) Introduction: general remarks

The Constitutional Court has held in respect of the fundamental rights contained in the Constitution that none of them should be viewed in isolation "but as part of a web of mutually supporting rights enumerated in the Constitution".[1117] This process may amount to "the balancing of two parallel equations, which are by all means not always equal" where two rights are in conflict with each other.[1118]

Midi Television v DPP[1119] quoting from *S v Manamela*[1120] set out the approach to be followed where competing constitutional rights are balanced with one another. The approach involves determining the proportionality of the "extent of the limitation of the right considering the nature and importance of the infringed right, on the one hand, and the purpose, importance

judgments of *Abrams v. United States*, 250 U.S. 616 (1919) at 630 – 631 and *Cohen v. California*, 403 U.S. 15 (1971) at 24; in Canada the judgment of *RWDSU v. Dolphin Delivery Ltd*., [1986] 2 S.C.R. 573 discusses freedom of expression, before the enactment of the Canadian Charter of Rights and Freedoms in Canada, still even before the Canadian Bill of Rights was passed in 1960 – see also *R v Keegstra; Attorney-General of Canada & other intervening parties* [1991] 3 CRR (2d) 193 at 213, and V Goswami 'Algorithms, expression and the Charter: A way forward for Canadian Courts' (2017) 7(1) *Western Journal of Legal Studies* Article 2 at 1 – 15. See *Qwelane v South African Human Rights Commission & another* 2021 (6) SA 579 (CC) which discusses most of the cases listed herein.

[1116] *S v Mamabolo* 2001 (5) BCLR 449 (CC) paras 37 and 40.

[1117] *Case & another v Minister of Safety and Security & others* 1996 (3) SA 617 (CC) para 27, although the focus of this discussion was on freedom of expression in the Interim Constitution, the sentiments expressed therein still have ample application today: *British American Tobacco South Africa (Pty) Ltd v Minister of Health* [2012] 3 All SA 593 (SCA) para 16 and *Growthpoint Properties Ltd v SACCAWU & others* [2011] 1 All SA 537 (KZD) para 1.

[1118] *Indigenous Film Distribution (Pty) Ltd & another v Film and Publication Appeal Tribunal &others* [2018] 3 All SA 783 (GP) para 35. Note the comments in *Modiri v Minister of Safety and Security & others* [2011] ZASCA 153 paras 22 and 24. See also UNCHR (Sub-commission) 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40 para 27.

[1119] *Midi Television (Pty) Ltd t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) para 10.

[1120] *S v Manamela and another (Director-General of Justice intervening)* 2000 (3) SA 1 (CC) para 66.

and effect of the infringing provision, taking into account the availability of less restrictive means available to achieve that purpose".[1121] In some instances there may be a need to curtail both rights in question to some extent in order to achieve fairness and ultimately a beneficial outcome for both parties – keeping in mind the provisions of s 36 of the Constitution.[1122] The task is certainly not easy.[1123]

O'Regan J in her minority judgment in *Bernstein v Bester* remarked that "freedom has two interrelated constitutional aspects."[1124] The first part is procedural, which requires that freedom will be deprived only where this is substantively fair in light of the Constitution. The second part recognises that freedom will not be curtailed where the reason is unacceptable, even if it may be lawfully fair. Limiting freedom of expression must serve the principle of open justice.[1125] This is often the starting point, as freedom of expression is one of the cluster or umbrella rights, together with the right to a public trial, which is associated with the right to a fair trial.[1126] A testament to the notion of open justice is the "media box" where members of the press find a special place to sit, observe and report on the proceedings before the court. *Centre for Child Law*[1127] endorsed this approach of transparency and accountability of courts in administering justice, as it lies at the heart of the oft-quoted phrase "that justice should both be done and manifestly seen to be done". This principle is recognised in international law and foreign jurisdictions. [1128] The SCA emphasised the vital role that the media plays as an overall "watchdog" and added that open justice included keeping the public "timeously and

---

[1121] *S v Manamela and another (Director-General of Justice intervening)* 2000 (3) SA 1 (CC) para 66; *Midi Television (Pty) Ltd t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) para 10.

[1122] *Midi Television (Pty) Ltd t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) para 9 – 11, see the following:

> "[9] Where constitutional rights themselves have the potential to be mutually limiting - in that the full enjoyment of one necessarily curtails the full enjoyment of another and vice versa - a court must necessarily reconcile them. They cannot be reconciled by purporting to weigh the value of one right against the value of the other and then preferring the right that is considered to be more valued, and jettisoning the other, because all protected rights have equal value. They are rather to be reconciled by recognising a limitation upon the exercise of one right to the extent that it is necessary to do so in order to accommodate the exercise of the other (or in some cases, by recognising an appropriate limitation upon the exercise of both rights) according to what is required by the particular circumstances and within the constraints that are imposed by s 36."

[1123] Jafta J in *Johncom Media Investments Ltd v M & others* 2001 (5) BCLR 449 (CC) para 1.

[1124] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 145

[1125] *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC) para 91.

[1126] *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC) para 92.

[1127] *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC); the court quoted from *Van Breda v Media 24 Ltd & others* 2017 (5) SA 533 (SCA) paras 46 and 47.

[1128] *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC) para 94. Some examples that were referenced in the footnotes include *R (Guardian News and Media Ltd) v Westminster Magistrate's Court* [2013] QB 618; *R v Legal Aid Board, Ex parte Kaim Todner (a firm)* [1999] QB 966; *Hogan v Hinch* [2011] 243 CLR 506; and *Attorney General (Nova Scotia) v MacIntyre* [1982] 1 SCR 175.

accurately" informed of proceedings that will be of interest to them.[1129]

The following topics are areas where a balance needs to be struck between the rights of privacy and freedom of expression, namely in terms of classified information, the confidentiality of information and the free press, with regard to journalistic sources and public access to information in court files, and lastly, in light of technological advances. These are each discussed below.

(b) Classified information

The need to keep certain documents completely confidential and the right to access and receive information[1130] is generally a challenging issue to resolve. Skweyiya J expressed this tension in that the classification of documents by an administrative body places an immediate restraint on freedom of expression. Where there has been prior classification, by the administrative body, it eases the burden of policing and prosecuting possible leaks.[1131] The fact that a publication is classified makes inroads into the right of press freedom and the ability to bring important information to the attention of the public. Even if the public is later informed of the publication, the content may be redundant, alternatively the publisher could face prosecution for withholding vital information.[1132]

(c) Confidentiality and a free press

A recurrent and important point to note is that a sharp distinction needs to be drawn "between

---

[1129] *Van Breda v Media 24 Ltd & others* 2017 (5) SA 533 (SCA) para 47; *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC) para 95.

[1130] See s 16(1)*(b)* of the Constitution.

[1131] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 59:

> "According to academic commentators, under a system of administrative prior restraint, the opportunity for public scrutiny and comment on a fresh publication is denied. An administrative body is more likely to restrict publications when it can classify upfront than when it must take punitive or restrictive action after publication. The greater propensity for prior restraint when controlled by an administrative body is explained by the nature of prior classification itself, where, by restraining upfront, the state is relieved of the greater burden on resources, personnel and time necessitated by policing and possibly prosecuting after material has been made public. Last but not least, an administrative body is mandated and incentivised to classify, which also increases the likelihood of restraint." (footnote omitted)

See also the comments of the European Court of Human Rights in *Mosley v. The United Kingdom* [2011] ECHR 774.

[1132] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 60:

> "Deepening the fracture in the right is the fact that throughout the classification process the fate of the publication remains uncertain. In some instances, the very delay in bringing important information to the public's attention makes inroads into the right to freedom of the press and other media. The contents of the publication may even be redundant by then, yet there would be no remedial action open to the publisher. Equally, if a publisher were not to submit material that, on the face of it, fell to be submitted, but would ultimately have emerged unrestrained, he could still be prosecuted for breaching the very duty to submit." (footnotes omitted)

what is in the public interest and what is merely of interest to the public."[1133] However, there are instances where the marking of a document as "confidential" will be justifiable in the circumstances. But absolute confidentiality might be infrequent.[1134] *Johncom Media v M*,[1135] dealt with the publishing of information during divorce proceedings, and the need that privacy should be enjoyed in respect of certain facts and information, especially due to the nature and sensitivity of the information that is discussed in court, particularly when dealing with children. *Johncom Media v M*[1136] held, quoting with approval from *National Coalition for Gay and Lesbian Equality & another v Minister of Justice*,[1137] with regard to the limitation of the right of freedom of expression in favour of privacy, that the limitation must still be reasonable in light of the factors described in s 36 of the Constitution.[1138] Bearing in mind the discussion above on the approach to be used, *Midi Television* held that constitutional rights have the ability to limit one another, and a court will need to find a suitable solution in resolving these differences. None of the rights in the Constitution are superior to one another, all rights are of equal value. The limitation of the infringed right will be allowed only insofar as it is needed to exercise the other right, it may be for the benefit of both that both rights will be limited to a certain extent. All this is dependent on the situation as well as keeping in mind the limitations clause.[1139] Jafta J also pointed out that the constitutional promise of a free media does not protect press-specific interests. The idea of "press exceptionalism," meaning that the press has special and superior protection in terms of the Constitution is not only implausible but treacherous. Limiting the rights of the press will involve a limitation for all citizens.[1140]

News agencies are holders of the right to freedom of expression, these include the rights of a free press and media as well as the right to receive and share information, specifically with

---

[1133] This is a recurrent theme between the rights to privacy and freedom of expression, see *Centre for Child Law & others v Media 24 Ltd* 2020 (1) SACR 469 (CC) para 96, see also *Tshabalala-Msimang & another v Makhanya & others* 2008 (6) SA 102 (W).
[1134] *Mail & Guardian Media Ltd &others v Chipu NO* 2013 (6) SA 367 (CC) para 71.
[1135] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) paras 1 – 2. See also *NM & others v Smith & others* 2007 (5) SA 250 (CC) at paras 144 – 148; and *Khumalo & others v Holomisa* 2002 (5) SA 401 (CC) paras 21 – 28.
[1136] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC).
[1137] *National Coalition for Gay and Lesbian Equality & another v Minister of Justice & others* 1998 (12) BCLR 1517 (CC) para 35.
[1138] *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 24. *Midi Television (Pty) Ltd t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) paras 9 – 11.
[1139] *Midi Television (Pty) Ltd t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) para 9; see also *National Coalition for Gay and Lesbian Equality & another v Minister of Justice & others* 1998 (12) BCLR 1517 (CC) para 35; *S v Manamela and another (Director-General of Justice intervening)* 2000 (3) SA 1 (CC) para 66; and *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) paras 24 – 25.
[1140] *Midi Television (Pty) Limited t/a E-TV v Director of Public Prosecutions (Western Cape)* 2007 (5) SA 540 (SCA) para 6; *Johncom Media Investments Ltd v M & others* 2009 (4) SA 7 (CC) para 28; see also *Holomisa v Argus Newspapers Ltd* [1996] 1 All SA 478 (W).

the public.[1141] This includes holding the courts accountable in terms of the principle of open justice and informing the public of these proceedings. However, where the courts are exercising their discretion, set out in s 173 of the Constitution, and this encroaches on rights set out in Chapter 2 of the Constitution, the court must only exercise the discretion in proportion to what is needed to limit the said right. This does not amount to a limitations analysis, it is merely an inquiry that must be undertaken.[1142] It was acknowledged by the Constitutional Court that journalists have a special role to play in the protection of freedom of expression in line with journalistic activities.[1143]

To illustrate this point: in *UKZN v Independent Newspapers*[1144] the court was required to balance the right to privacy with the right to freedom of expression in circumstances where part of a summary of a confidential report was leaked to a journalist by a whistle-blower. The report was the conclusion of a forensic investigation into the fraudulent sale of "positions for prospective students" at the University of KwaZulu-Natal medical school (UKZN). The base of the claim for the journalist and publisher was that the summary of the report had lost its confidential status, the entire report was no longer subject to privacy or confidentiality.[1145] Koen J, emphasised the importance of a free, vigilant, and independent media that investigated and reported on allegations of fraud, corruption and State capture. Curtailing press freedom amounts to a curtailment of the public's right to information, but this right is not absolute.[1146] He acknowledged that balancing competing interests is often challenging, finding support in *NM v Smith*, where Langa CJ observed that a reasonable journalist or publisher can, with minimal effort avoid possible harm, when they seek consent to publish, from the person/s concerned.[1147]

[1141] *SABC Limited v National Director of Public Prosecutions* 2007 (1) SA 523 (CC).

[1142] *SABC Limited v National Director of Public Prosecutions* 2007 (1) SA 523 (CC) para 42:

> "While the SABC is, as the national public broadcaster, obviously a bearer of s 16(1) rights, the general public also has a fundamental constitutional right to freedom of expression; indeed, it may be said that the primary bearer of the right to 'receive information and ideas' is the general public. It is also true, as contended by counsel for the SABC, that openness and accountability are underlying values of the Constitution and that, in accordance with the principle of open justice, the public should, as far as possible, be informed and aware of what takes place in our courts. Where a Court exercises a discretion under s 173, it must ensure that if in so doing it impinges upon rights entrenched in ch 2 of the Constitution, the extent of the impairment of rights is proportional to the purpose the Court seeks to achieve. We do not need to consider here whether this is a s 36 limitation analysis or not. It is clear that it is a proportionality enquiry that a Court exercising its s 173 powers must undertake." (footnote omitted)

[1143] *Khumalo & others v Holomisa* 2002 (5) SA 401 (CC) para 22.

[1144] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD).

[1145] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD).

[1146] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) para 26.

[1147] *NM & others v Smith & others* 2007 (5) SA 250 (CC) para 111; *University of Kwazulu-Natal v Independent*

In *UKZN v Independent Newspapers* the competing interests, broadly, were that UKZN requested that the summary, report and final conclusions from the investigation remain confidential until the investigation was complete. In other words, that publication be deferred, in order to verify that the result was fair and reasonable. The press maintained that the public interest outweighed UKZN's confidentiality.[1148] The court observed that, whilst striking the balance between the competing rights of privacy (or confidentiality) and freedom of expression, first, despite a part of the summary having been leaked, ie accessible "in the public domain", this did not automatically deny the confidentiality of the balance of the summary as well as the report. Secondly, the naming and shaming of individuals before proper verification of the information may result in harm resulting in a possible redress for damages suffered. Thirdly, there was nothing to suggest that the applicant had acted insincerely by protecting the identity of the alleged perpetrators.[1149] Hence, Koen J was not convinced that merely because a part of the summary, alternatively the report, came to the attention of the public via unlawful means, this resulted in the loss of confidentiality.[1150] Koen J concluded that only those portions of the unlawfully leaked summary that had already been published would remain in the "public domain", the remainder of the unpublished summary as well as the full report would remain confidential and therefore private.[1151]

From the cases cited above, journalism seems to be the main area of contention. Although, s 16(1)*(a)* of the Constitution contains a specific reference to journalists and their work, namely "freedom of the press and other media", *UKZN v Independent Newspapers* warns that this does not amount to a carte blanche protection in terms of the right to freedom of expression, and journalists carry a certain amount of responsibility in obtaining consent where they are reporting on contentious issues.[1152]

Khumalo v Holomisa held that journalists, when reporting, need to remember to do so with respect, as every individual is entitled to dignity, especially where the matter deals with a defamation claim. This encouraged journalists to "act with due care and respect" in order to

Newspapers (Pty) Ltd & others [2018] JOL 40414 (KZD) para 27.

[1148] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) para 28.

[1149] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) para 29.

[1150] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) para 23.

[1151] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) paras 24, 25, 26 & 30.

[1152] *University of Kwazulu-Natal v Independent Newspapers (Pty) Ltd & others* [2018] JOL 40414 (KZD) para 29.

avoid situations where freedom of expression, human dignity as well as privacy need to be balanced, which may result in a "winner-takes-it-all" conclusion. This won't preclude the publishing of defamatory material, but respect needs to be shown to the individual as the subject of the article.[1153]

(d) Journalistic sources

Another contentious issue that the courts have had to contend with, in the light of freedom of expression, is the protection of journalistic sources. Journalists often claim the privacy of their sources, as the protection of whistle-blowers also has an important function in protecting freedom of expression.[1154] Willis J in *SABC v Avusa*,[1155] quoted Lord Denning's observations in *British Steel Corporation v Granada Television Ltd*[1156] where he emphasised the need for journalists to generally keep their sources confidential, otherwise no one would be prepared to speak out, fraudsters, imposters or criminals would not be uncovered, crimes or maladministration within government and companies would not be uncovered and remain behind closed doors. Hence, the power of investigative journalism's value cannot be overstated. Tsoka J in *Bosasa v Basson*[1157] observed that "journalists are not entitled to a blanket journalistic privilege" and thereby avoid revealing their sources. However, Tsoka J warned that journalists cannot claim the protection afforded by s 16 of the Constitution, where information relates to the possible or pending commission of a serious crime and would obstruct the investigation.[1158] In other words, in appropriate circumstances journalists must reveal their sources.[1159]

(e) Public access to information in court files

An application brought by SANRAL in the Western Cape, which was taken on appeal to the SCA, dealt with redacting portions of affidavits and keeping certain documents private or out of the court file, until the matter had been placed before a judge hearing the main application – the reason was to protect business interests and hence the information contained therein to be

[1153] *Khumalo & others v Holomisa* 2002 (5) SA 401 (CC) para 43.
[1154] *SABC v Avusa Ltd & another* 2010 (1) SA 280 (GSJ) paras 30 – 31, *Bosasa Operations (Pty) Ltd v Basson & another* 2013 (2) SA 570 (GSJ) para 25.
[1155] *SABC v Avusa Ltd & another* 2010 (1) SA 280 (GSJ) para 30.
[1156] *British Steel Corporation v Granada Television Ltd* [1981] 1 All ER 417 at 441.
[1157] *Bosasa Operations (Pty) Ltd v Basson & another* 2013 (2) SA 570 (GSJ) para 26.
[1158] *Bosasa Operations (Pty) Ltd v Basson & another* 2013 (2) SA 570 (GSJ) para 52.
[1159] *SABC v Avusa Ltd & another* 2010 (1) SA 280 (GSJ); *Bosasa Operations (Pty) Ltd v Basson & another* 2013 (2) SA 570 (GSJ), *South African Airways SOC v BDFM Publishers (Pty) Ltd & others* 2016 (2) SA 561 (GJ); *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) para 47.

kept confidential and private.[1160] The Western Cape High Court granted the order allowing the redaction of the information until the main review application was heard. However, on appeal, the order was overturned. The SCA first reiterated the fact that all proceedings, including applications and trials, are generally heard in open court, making justice accessible to the public. All documents filed in a court file, are automatically, public documents, and are therefore accessible for public scrutiny.[1161] Having matters heard in open court and subjected to public scrutiny is part of the "foundational constitutional values of accountability, responsiveness and openness, and apply to the functioning of the judiciary as much as to other branches of government." The "soul of justice" which amounts to a "constitutional imperative" is to dispense justice in open court.[1162] The fact that information in the court documents would be redacted and the matter heard in camera would amount to a grave infringement of the rights of freedom of expression and access to information, which rights are crucial to accurate reporting.

The SCA did note that there might be specific instances in which court proceedings as well as the access to court documents will be restricted, in the interests of justice,[1163] describing the position as follows: "The principle of open justice has its limits of course and concomitantly a commitment to open justice does not mean that there should always be unrestricted reporting, nor that there may not be good and genuine reasons why information should sometimes be restricted." But a departure from the general rule of open justice will always be considered as an exception.[1164] The SCA sent out the following reminder in terms of the discovery process

[1160] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA).
[1161] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) para 12ffg. The SCA, in substantiation hereof quoted from various foreign authorities: *R v Legal Aid Board, ex parte Kaim Todner (a firm)* [1998] 3 All ER 541, *Detroit Free Press v John Ashcroft* 303 F.3d 681, *Attorney General (Nova Scotia) v MacIntyre* [1982] 1 SCR 175, *Richmond Newspapers v Virginia* 448 US 555 (1980) as well as various speeches from Judges appointed in Canada and Australia.
[1162] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) para 16; *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services & another, In Re Masetlha v President of the Republic of South Africa & another* 2008 (5) SA 31 (CC) para 42.
[1163] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) para 23ffg. See also the following authorities: *Harman v UK* (1985) 7 EHRR 146 (EComm); *Rank Film Distributors Ltd v Video Information Centre* [1982] AC 380 (HL); *Attorney General for Gibraltar v May & osthers* [1999] 1 WLR 998; *Alterskye v Scott* [1948] 1 All ER 469; *Home Office v Harman* [1982] 1 All ER 532 (HL); *Hearne v Street* [2008] HCA 36; *Australian Competition and Consumer Commission v Allphones Retail Pty Limited (No 3)* [2009] FCA 1075; *British American Tobacco Australia Services Ltd v Cowell (No 2)* (2003) 8 VR 571; *Esso Australia Resources Ltd v Plowman* [1995] 183 CLR 10; *Andrew Koh Nominees Pty Ltd v Pacific Corporation Ltd [No 2]* [2009] WASC 207; *Juman v Doucette* 2008 SCC 8, as well as *Crown Cork & Seal Co Inc & another v Rheem South Africa (Pty) Ltd & others* 1980 (3) SA 1093 (W); *Replication Technology Group & others v Gallo Africa Ltd* 2009 (5) SA 531 (GSJ); *Mathias International Ltd & another v Baillache & others* 2015 (2) SA 357 (WCC).
[1164] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) para 46. An example of where a professional, in this instance a teacher, posted defamatory remarks about their students online is discussed in SA Coetzee 'A legal perspective on social media use and employment: Lessons for South African educators' (2019) 22 *Potchefstroom Electronic Law Journal* 1 – 37.

in Uniform Rule 35, which includes actions relating to defamation, the *actio injuriarum* – preventing the publication of private facts – the court has a discretion to limit the discovery of confidential documents as well as reasonably limit the use of these documents.[1165]

The SCA did accept that there are concrete instances in our law, which would constitute exceptions such as State security, the interests of children, as well as commercial secrecy. However, in this instance, the SCA opined that the public interest in the matter, with the concomitant rights of freedom of expression, access to information and access to courts, which form the basis of the argument for open justice, would suffer far more damage, than that resulting from a sacrifice of the confidentiality of SANRAL and its business partners.[1166]

POPI will also have an impact on the personal information processed in terms of the court proceedings, this is dealt with in the next chapter.

(f) Defamation and technology

With today's technology, it is easy to express oneself to a wide audience instantaneously.[1167] The internet has revolutionised the way people communicate with each other. It is often as easy as the click of a button. The potential to damage reputations, and thereby tarnish the dignity of an individual, reaches a wider audience than printed newspapers, journal articles, periodicals, etc. Iyer suggests that the exponential rise of online defamation cases is directly related to a bad decision to post an incident on social media, which gives individuals access to a large audience at little cost.[1168] Defamation cases often involve questions surrounding privacy and freedom of expression. Although, not directly linked to the main topic, this is discussed to round off the discussion of this chapter. The discussion here will be kept as brief as possible.[1169] It is useful to keep this discussion in mind, especially with regards to the chapter discussing POPI.

In one of the first reported cases in South Africa involved a claim in delict, which arose

---

[1165] Section 173 of the Constitution; rule 35 of the Uniform Rules of the High Court; *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) paras 46 – 47. In light of discovery procedures and the need for confidentiality of sensitive documents, see *Caxton and CTP Publishers and Printers Ltd v Novus Holdings Ltd* [2022] ZASCA 24 paras 78 – 83.

[1166] *City of Cape Town v SANRAL* 2015 (3) SA 386 (SCA) paras 17 and 47.

[1167] See generally D Sive & A Price 'Regulating expression on social media' (2019) 136(1) *South African Law Journal* 51 – 83.

[1168] D Iyer 'An analytical look into the concept of online defamation in South Africa' (2018) 32(2) *Speculum Juris* 124 at 125. On the topic of social media and POPI, see generally Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 601 – 627.

[1169] See A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *South African Law Journal* 375 – 402, and D Iyer 'An analytical look into the concept of online defamation in South Africa' (2018) 32(2) *Speculum Juris* 124 – 134 for a further discussion on this topic.

when the defendant, a friend of the applicant, typed an offensive post on Facebook.[1170] The applicant, an insurance broker, had separated from his wife and the post made specific reference to the separation as well as the fact that the applicant loved to drink alcohol when at a social event.[1171] *Heroldt v Wills* discussed various aspects of the use of social networking sites in great detail, which is not needed for the present discussion.[1172] An aspect that was highlighted by Willis J was that although social media sites do promise to keep personal information private, in line with their policies, they generally fail to do so, and that it will be up to the courts to initiate ideas for the practical protection of privacy.[1173] Willis J noted that *Bernstein v Bester* emphasised the close link shared by human dignity and privacy.[1174] Based on this close link Willis J concluded, in light of the principles of, as well as applying the test for, defamation that there had been a "prima facie invasion" of privacy and that the Facebook post was indeed defamatory.[1175] The court, after analysing the defences raised, ordered the payment of damages as well as that the Facebook posts be removed.[1176]

[1170] *Heroldt v Wills* 2013 (2) SA 530 (GSJ).
[1171] *Heroldt v Wills* 2013 (2) SA 530 (GSJ).
[1172] The discussion included how to join a social networking site, such as Facebook, and also made reference to Twitter (now X) as well as Google, and summarised the main points from the case law dealing with the aspects of defamation, in the light of privacy and freedom of expression. When joining a social media website, such as Facebook, Twitter (now X), Instagram, a person is compelled to provide certain personal information, so as to connect with other users, but that information, even though private, may be used for gain. Although social media websites (also referred to as social network sites or services) promise in their policies to make every effort to protect the privacy of individual users, through the relevant privacy settings, "these privacy settings are not foolproof" (para 19). Willis J concurred with the concerns of the cited academics, that social media sites do create problems for their users in failing to stringently deal with privacy issues, and legislation may not be able to solve this problem with great satisfaction, however, the courts will need to take an active role in finding practical solutions (paras 36 and 44 – 46).
[1173] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) paras 36 and 44 – 46.
[1174] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 24; *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC); para 68.
[1175] *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 25; *Jansen van Vuuren & another NNO v Kruger* 1993 (4) SA 842 (A) at 850. The test for defamation was taken from *Mthembi-Mahanyele v Mail & Guardian Ltd & another* [2004] 3 All SA 511 (SCA) para 25: the test for determining whether or not the words complained of are in fact defamatory, will be "whether a reasonable person of ordinary intelligence might reasonably understand the words concerned to convey" a defamatory meaning. Note in *EFF & others v Manuel* [2020] ZASCA 172 para 30 it was applied in a two-stage approach, first, the meaning of the words must be determined, and second, whether the words carry a defamatory meaning. See also *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 26; *EFF & others v Manuel* [2020] ZASCA 172 para 31: just because social media is used, the SCA held that the reasonable reader need not be redefined. In *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 22, Davis J confirmed the test for defamation is that "a reasonable person with ordinary intelligence would understand that the words concerned to convey a defamatory meaning against the litigant concerned" and further that such a situation demands a resolution be found between the rights of freedom of expression and dignity (reputation of the person injured).
[1176] Even though the post was defamatory, the judgment emphasised, in light of the defences that, first, the information must also be for the public benefit, ie a "distinction must always be kept between what 'is interesting to the public', as opposed to 'what it is in the public interest to make known'", it was not enough to merely be true. (See *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 27, *Modiri v Minister of Safety and Security & others* [2011] ZASCA 153 22 – 24, and *EFF & others v Manuel* [2020] ZASCA 172 para 37.) The court held that the information was neither of public interest nor would it benefit the public. Second, it did not amount to fair

Also, note the discussion regarding the defences in *Waldis v Von Ulmenstein* as they relate to an internet blog.[1177] What is important to note in light of *Waldis v Von Ulmenstein* is that an internet blog is unique, in comparison to a newspaper article, as it allows for the offending passages to be removed, leaving the rest of the article intact "because the balance of the report does not breach the law of defamation and can be preserved, pursuant to a commitment to freedom of speech".[1178] This could easily be applied to the removal of private information that is revealed on an open-access blog or similar internet post.

Interestingly, in *Isparta v Richter*, the principles of defamation were extended to where a person had been "tagged"[1179] in the post by the original author thereof – if they choose not to remove the "tag" they will automatically be associated with the post and they too will be liable for damages in a defamation claim.[1180] It has been suggested that it is best to "tag" a person

comment as considering the facts, the respondent had acted out of malice, alternatively an improper motive, when posting the comment. (See *Heroldt v Wills* 2013 (2) SA 530 (GSJ) paras 28 – 29, and as substantiation, Corbett CJ in *Financial Mail (Pty) Ltd & others v Sage Holdings Ltd & another* 1993 (2) SA 451 (A) at 462F-H.) When drawing the line between what is lawful and unlawful regarding the infringement of personal privacy, the court uses the lens of the current *boni mores* of the community, and what the community perceives to be the general sense of justice, a "weighing of competing interest". (*Financial Mail (Pty) Ltd & others v Sage Holdings Ltd & another* 1993 (2) SA 451 (A) at 462F-H.)

[1177] Note, *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC): in terms of truth and public interest, the court stressed, that obvious "wrongfulness of a defendant's conduct will be rebutted if he or she proves that the defamatory remarks are true and in the public interest". Put differently, the defendant need not prove literal truth but substantial truth of the statement, that "the sting of the charge is true". What this amounts to will depend on "the time, the manner and the occasion of the publication", as well as the convictions of the community. Further, merely because the comment is fairly recent does not exclude the defence of truth and public interest (See *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) paras 41 – 42; *EFF & others v Manuel* [2020] ZASCA 172 para 37; *Independent Newspapers Holdings Ltd & others v Suliman* [2004] 3 All SA 137 (SCA) para 47 and *Kemp & another v Republican Press (Pty) Ltd* 1994 (4) SA 261 (E) at 265B – F). With regards to fair comment, Davis J added that obvious wrongful publication may be rebutted where the defendant proves that the publication amounts to fair comment, or the facts are true and in the public interest. For this rebuttal the following four factors are considered: The defamatory statement (1) amounts to a comment and not to a mere "assertion of an independent fact"; (2) the statement must be fair; (3) the facts on which it is based are true; and (4) it is indeed in the public interest (*Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 43; *EFF & others v Manuel* [2020] ZASCA 172 para 38).

[1178] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 48. See the discussion in *Dimension Data (Pty) Ltd v Pearton* [2021] ZAECPEHC 54 in light of information placed onto a website.

[1179] In *Isparta v Richter & another* 2013 (6) SA 529 (GNP) para 7, Hiemstra AJ describes the process of being "tagged" as follows: "A user may 'tag' another user to any postings placed on his or her wall. The name of the tagged user will then appear at the end of the user's message as 'with ... (tagged user's name)'. The message would also appear on the wall of the tagged person. The tagged person's consent is not required, but he or she may remove his or her name from the message." However, as stated above in the main text, tagging provides individuals, who are also featured in the message or image, with the power to decide whether the post should remain available, whether access thereto should be restricted, etc. See Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, at 45. For a commentary of the case, see A Roos & M Slabbert 'Defamation on Facebook: *Isparta v Richter* 2013 6 SA 529 (GP)' (2014) 7(6) *Potchefstroom Electronic Law Review* 2845 – 2868.

[1180] *Isparta v Richter & another* 2013 (6) SA 529 (GNP) paras 7 & 36. See the High Court of Australia's judgment in *Fairfax Media Publications Pty Ltd v Voller; Nationwide News Pty Limited v Voller; Australian News Channel Pty Ltd v Voller* [2021] HCA 27 where media companies maintained public Facebook pages which contained hyperlinks to published news articles. Some of the comments from Facebook users in response to these published articles were defamatory in nature. The High Court held that the media companies could be held responsible via

when an image is posted that includes that person. It allows them to choose whether the image should remain on the site or not, alternatively restrict access to the image.[1181] *Netshipise v Munnick*[1182] opined that the wide reach that social media platforms have "cannot be downplayed", which means that there is a greater "potential for devastating consequences" to individual reputations when considered against the backdrop of the uninformed users, who are ignorant of "what may or may not constitute [as] acceptable" online interaction on platforms such as Facebook, Twitter (now X), Instagram, etc.[1183]

Worth noting, in both Australia[1184] and England,[1185] the respective courts held that the use of emojis or emoticons, depending on the context, may amount to a defamatory expression. South Africa is yet to deal with a case with similar facts.[1186]

Even with the use and advancement of internet technology freedom of expression may be curbed. As technology advances and subscriptions to magazines, journals, and other publications become more easily available, cases involving defamation are likely to become more frequent, especially where the account is marked public, or the blog is easily accessible, even if confined to a closed community, but generally the websites are open to all to locate and read. News outlets are using the internet more frequently to reach a wider audience, for

association where these comments are not removed. By contrast in *Google LLC v Defteros* [2022] HCA 27 the High Court of Australia held that a search engine cannot be held liable by association for defamatory material that appears on the results page where the defamed person's name was the keyword used for the search. See also D Rolph 'Liability for the publication of third-party comments: *Fairfax Media Publications Pty Ltd v Voller*' (2021) 43(2) *Sydney Law Review* 225 – 240, and S Goodman & M Clayton 'When is an online publisher a publisher?' (2022) *Lexology* 14 September. *https://www.lexology.com/library/detail. aspx?g=3ca7b651-1da3-467c-9f72-0c5a18b71257* (Accessed: 21 September 2022). Note in certain instances "tagging" has the potential to highlight certain stigmas associated with groups or people, irrespective of whether along racial lines, or where this is due to a specific trait of that group of persons, ie albinism – see MM Mswela 'Tagging and tracking of persons with albinism: A reflection of some critical human rights and ethical issues arising from the use of the global positioning system (GPS) as part of a solution to cracking down on violent crimes against persons with albinism' (2019) 22 *Potchefstroom Electronic Law Journal* 1 at 17.

[1181] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age* at 45.

[1182] *Netshipise v Munnick & others* [2018] ZAGPJHC 547.

[1183] *Netshipise v Munnick & others* [2018] ZAGPJHC 547 para 6. Note also, the discussion in *EFF & others v Manuel* [2020] ZASCA 172, a defamatory statement, pretexted as a media statement, had been circulated via Twitter (now X) to all the media houses. The circulation through a social media platform meant that the statement was immediately available to a wider audience and not merely a small inclusive group of people (para 31). See also *National Media Ltd & others v Bogoshi* 1998 (4) SA 1196 (SCA). See also M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 at 14 – 15 where Malahleka mentions the need to protect human rights in terms of data portability, including the right to privacy, and specifically in light of children's rights and social media, see P Gabriel 'The Protection of Personal Information Act 4 of 2013 and children's right to privacy in the context of social media' (2019) 82 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 605 – 620.

[1184] *Burrows v Houda* [2020] NSWDC 485.

[1185] *Lord McAlpine of West Green v Bercow* [2013] EWHC 1342 (QB).

[1186] P Singh 'Can an emoji be considered as defamation? A legal analysis of *Burrows v Houda* [2020] NSWDC 485' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 26.

example, it may be as easy as downloading an app or application onto your cell phone, tablet, notepad or computer to catch up on the latest news.[1187] If the persons themselves published the information, for example on a blog, then generally it is easy to remove, unless it has been shared. But where a third-party posts intimate or defamatory information about an individual, the position is more complex – especially because the internet, mainly with reference to social media sites, has a wide, public appeal.[1188]

V CONCLUSION

The one lesson that can be learnt from the aforementioned discussions, is that it is certainly not always easy to find a balance between competing constitutional rights. Where a situation demands that matters be brought into the open and underlying issues be exposed, it is important to give freedom of expression greater protection. However, there will be a need to keep reports confidential, until verified for distribution, or keep the personal sphere of an individual private.

As noted by most judgments, and best set out in *Print Media SA*, in Van der Westhuizen J's judgment, in a diverse constitutional democracy, not all rights are absolute.[1189] The ability to choose is central to human dignity. However, when it comes to rights, it is not as simple as picking a favorite item from a supermarket shelf in the free market of ideas. These choices may lead to the infringement of another's human dignity.[1190] How people wield power and communication, ie language, visuals, etc., may also harm vulnerable members of society. Hence, it is important to find a delicate balance between the rights of freedom of expression, human dignity, equality, privacy, and other rights or considerations, depending on the circumstances.[1191] Free expression must not be used to promote war, incite violence or harm or encourage hatred, "based on race, ethnicity, gender or religion." [1192]

Discussing this delicate balance between the various rights is the focus of this thesis, however, as the case law reiterates the circumstances will often dictate which right should

[1187] News24 has a downloadable mobile app or application that may be obtained from the relevant store for the cell phone system that an individual may be using, the three most popular are iOS (for Apple products, ie iPhone), Android (for Samsung, Microsoft, etc.) and Harmony (for Huawei).
[1188] Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age*, (May 2016) at 39 – 40.
[1189] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 97. Van der Westhuizen J agreed with the order and most of the reasoning of Skweyiya J, but wanted to add to the discussion regarding freedom of expression.
[1190] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 97.
[1191] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 97.
[1192] *Print Media South Africa & another v Minister of Home Affairs &another* 2012 (6) SA 443 (CC) para 97.

receive greater protection and which will be justifiably limited in the circumstances.

The above discussion is to serve as the backdrop for chapter 5. Personal information is sensitive and individuals expect that such information will not be divulged, meaning it will remain confidential during the collection, processing, and storage thereof. It is this expectation that personal information will be protected that runs like a thread through the principles of data processing that is discussed in both chapters 2 and 5 of this thesis.

CHAPTER 5

POPI AND THE RIGHT TO BE FORGOTTEN IN SA

I INTRODUCTION

To what extent do individuals want to reveal their personal information or data? And if revealed, what will happen to it? Will it be safe or secure? Or will it be abused? Is there a possibility of deleting personal information when stored in data banks? These are some of the questions that individuals ask when they share personal information with a third party – be it a natural or juristic person – for example when joining a local supermarket's rewards programme, or when opening a social media account. When it comes to divulging their personal information, individuals wish to exercise informational self-determination and decide for themselves how much of their personal information they wish to divulge in any given circumstance.[1193] This is where the Protection of Personal Information Act 4 of 2013 (POPI), which commenced on 1 July 2020,[1194] fits in.

POPI follows the international trend, as well as meeting the need for national legislation, to specifically deal with the increasing phenomenon of the availability and instantaneous exchange of information, (including personal information) via the internet in the form of data protection laws.[1195] The South African legislature, through the enactment of POPI, has sought to actively address s 14 of the Constitution, ie the right to privacy, but also to align itself with international standards, and especially European standards.[1196]

[1193] JC Buiterlaar 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 at 187 – 189.

[1194] See Proc R21 in *GG* 43461 of 22 June 2020, with the exception of sections 110 and 114(4). Sections 110 and 114(4) came into effect on 30 June 2021, see Proc R21 in *GG* 43461 of 22 June 2020. The Protection of Personal Information Act is generally acronymed to POPI, the POPI Act or POPIA. In this thesis the preferred acronym is POPI, unless quoted from a text. For a history of POPI, including the drafting of the legislation and the national and international climate at the time of drafting, as well as where it fits into the SA legal system, see A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *South African Law Journal* 400 – 433. For a complete overview of POPI, see also A Roos 'Data Protection Law in South Africa' In A Makulilo (ed) *African Data Privacy Laws* (2016) at 201 – 222. See also *Ibex RSA Holdco Ltd & another v Tiso Blackstar Group (Pty) Ltd & others* [2024] ZASCA 166 para 27.

[1195] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 4 – 5, and G Katzav 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 at 433.

[1196] See the preamble to POPI as well as N Kirby 'What SA law says about the right to be forgotten', dated 13 June 2014; available at *https://www.iol.co.za/business-report/opinion/what-sa-law-says-about-the-right-to-be-forgotten-1702860#.VdLApPmqqko*, accessed 27 September 2021, AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 51, and M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 at 2. Cf A Naude *Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments* (unpublished LLM thesis, University of Pretoria,

Generally, data protection laws find their support in terms of the right to privacy. The right to privacy is a broad concept, whereas data protection laws protect one aspect of a person's privacy.[1197] Data protection laws also seek to find a balance between the right to privacy and the right to freedom of expression, mainly in the form of the right to impart or receive information.[1198] POPI, as stated in its preamble, also addresses the need to encourage the free flow of information, including personal information – thereby, to a certain extent, addressing the right to impart and receive information, in the wider context of freedom of expression. POPI, is an instrument "within the framework of the information society" and is designed to regulate the protection of privacy, specifically protecting personal information during the processing thereof, however subject to specific limitations, that are justifiable within an open, and democratic society. POPI provides the mechanisms for balancing the respective rights and freedoms, as well as remedies where the provisions of POPI are breached.[1199] The rights of privacy and freedom of expression were discussed in the previous chapter. How POPI strikes the balance between the right to freedom of expression, specifically in terms of the right to impart and receive information, and the right to privacy will be mentioned throughout,

December 2014). For a generally comparison between POPI and various international data protection legislative instruments, see J Botha, MM Grobler, J Hahn & MM Eloff 'A high-level comparison between the South African Protection of Personal Information Act and international data protection laws.' In *Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS)* (2 – 3 March 2017, Dayton, Ohio, USA). For a discussion on New Zealand's equivalent legislation see A Roos 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Review* 62 – 109. In relation to other African countries see T Ilori 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions' *Association for Progressive Communications*, 15 June 2020 1 – 18. For a discussion of the data protection laws in California see S Shatz & SE Chylik 'The California Consumer Privacy Act of 2018: A sea change in the protection of California consumers' personal information' (2019) 75 *The Business Lawyer* 1917 – 1924.

[1197] D Van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17(1) *Potchefstroom Electronic Law Review* 296 at 306, J Ballaschk 'In the unseen realm: Transnational intelligence sharing in the European Union - Challenges to fundamental rights and democratic legitimacy' (2015) 51 *Stanford Journal of International Law* 19 at 22, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 – 26. See XZ Pang 'Civil law protection of personal information in the era of big data' (2021) 8 *Open Access Library Journal* e8016 at 1 – 12 regarding China, where the data protection laws are scattered, and thus offer a very narrow protection were personal information is being processed.

[1198] 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 (Directive 95/46), ML Rustad & S Kulevska 'Reconceptualizing the right to be forgotten to enable transatlantic data flow' (2015) 28 *Harvard Journal of Law & Technology* 349 at 359, and A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 400. In relation to drones, or remotely piloted aircraft systems, and POPI see N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) 51(1) *De Jure Law Journal* 140 – 158. See also *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 18.

[1199] Preamble to POPI.

specifically in the discussion on the right to be forgotten.

In terms of data protection, originally the Electronic Communications and Transactions Act 25 of 2002 (ECTA) provided limited protection of personal information. POPI, on the complete commencement of all its provisions, repealed sections 45, 50 and 51 of the ECTA. The following is important to note generally, as an introduction to POPI. Briefly, the ECTA defined personal information extensively, but the personal information had to relate directly to the data subject.[1200] Furthermore, the ECTA applies to information in general, ie the ECTA is primarily aimed at enabling and facilitating "electronic communications and transactions in the public interest" by generally promoting public confidence in the use of electronic applications or technology, such as the internet and computers, including the storage of information within electronic databases. The promotion of the use of electronic applications and technology is in light of the "importance of the information economy for the economic and social prosperity of the Republic".[1201] The sections that were repealed by POPI in the ECTA, are replicated and expanded within POPI, namely s 45 which dealt with unsolicited goods, services or communications,[1202] s 50 which dealt with the scope of protecting personal information, and s 51 which dealt with the principles of electronically collecting personal information.[1203] Protection of personal information in the ECTA was voluntary[1204] – hence the need for POPI.[1205]

POPI is designed to protect the personal information of individuals and organisations

[1200] Section 1 of the ECTA. See *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* 2014 (2) SA 569 (GSJ) para 60, and *S v Miller & others* [2015] All SA 503 (WCC) para 48. Since the enactment of POPI, the definition of personal information in the ECTA has been aligned to correspond with the definition found in POPI.

[1201] Section 2 and Chapter VIII of the Electronic Communications and Transactions Act 25 of 2002 (ECTA). – see Proc R21 in *GG* 43461 of 22 June 2020.

[1202] Also known as "spam". This is specifically now set out in POPI in section 69 – 71 in Chapter 8 of POPI, and this is discussed below. For a brief discussion on s 45 see L Swales 'Protection of Personal Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)" (2016) 28 *South African Mercantile Law Journal* 49 at 68 – 71.

[1203] Chapter VIII of the ECTA, which contains section 50 – 51 was specifically limited to personal information that was collected (and thereafter processed) through electronic means. This is now fully covered in POPI, where there is no distinction between how the personal information is collected, ie either in the form of a paper trail or through electronic means, this is the thrust of this chapter. It has been argued that the ECTA is outdated, and that the rest of the provisions will need to be brought in line with POPI, especially those provisions relating to data privacy – see V Lawack, BM Mupangavanhu & E Olivier 'The protection of consumers of retail central bank digital currency – Some considerations' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 285 at 305.

[1204] Section 51 of the ECTA. See also J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce' (2004) 15(3) *Stellenbosch Law Review* 501 at 510.

[1205] D Van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17(1) *Potchefstroom Electronic Law Review* 296 at 305, and L Swales 'Protection of Personal Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) 28 *South African Mercantile Law Journal* 49 at 49.

processed by both private and public (or State) entities. It applies to a "person", a term defined to include both a natural and juristic person.[1206] It is designed to operate alongside the Promotion of Access to Information Act 2 of 2000 (PAIA).[1207] Both POPI and PAIA regulate how personal information must be protected. However, the thrust of PAIA is to give effect to s 32 of the Constitution, which provides for the right to information.[1208] Important for this thesis is whether South Africa has a right to be forgotten and how that right is defined.

The discussion in this chapter will cover: an analysis of the relevant sections of POPI, for this thesis, inlcuding the application, interpretaion and purpose of POPI, and the processing of personal information. Thereafter the supervision of POPI will be outlined. There is also a brief discussion on jurisdiction. Lastly, an analysis on whether POPI provides a right to be forgotten within its framework. In this chapter, the phrase "personal information" will be preferred over "personal data" as POPI uses the term "personal information".[1209]

II POPI: AN OVERVIEW

(a) Introduction

POPI is organised into various chapters. The ones most relevant to the thesis are: Chapter 1, which contains the definitions and purpose; Chapter 2, which deals with the application and interpretation of the Act; Chapter 3, which sets out the conditions for the lawful processing of personal information; and Chapter 4, which sets out the exemptions that may apply when processing personal information.[1210] Each will be discussed insofar that they relate to the topic

[1206] See s 1 of POPI. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 471. See also s 1 of PAIA.
[1207] See the long title, sections 23 (Access to personal information), 25 (Manner of access), and Chapter 5 of POPI. Note, other legislation that has an impact on POPI includes the Promotion of Administrative Justice Act 3 of 2000 (PAJA), Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (RICA), Electronic Communications and Transactions Act 25 of 2002 (ECTA) and the National Credit Act 34 of 2005 (NCA). For a short comment on POPI see A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 at 57 – 59.
[1208] See generally AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 41ffg. Compare with M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 – 19.
[1209] See Chapter 3 regarding the debate surrounding the terms of "personal data" and "personal information" as well as the texts quoted in the relevant footnote. This is merely something to note, so that readers are not confused by the change in terminology.
[1210] Chapter 5 provides for the supervision of POPI in the form of an information regulator and their office. Chapter 6 requires that prior authorisation must be obtained when processing personal data. Chapter 7 provides for the codes of conduct, ie from issuing, guidelines for their content to failure to comply with them. Chapter 8 sets out the rights of data subjects with regards to telemarketing. Chapter 9 provides for 'transborder information flow'. Chapter 10 provides for the enforcement of POPI, which should be read with Chapter 11 which deals with the offences and penalties. Lastly, Chapter 12 has further general provisions.

of this thesis, and in relation to the rest of the Act, where this is necessary. In this part of the chapter, some overarching remarks as well as some of the important definitions will be set out. Thereafter, the application, interpretation and purpose of the Act will be discussed. Next, I shall consider the processing of personal information and how the right to be forgotten is dealt with. Finally, I shall discuss further important points that deserve to be noted for the overall thesis.

(b) Definitions

One of the "themes", borrowing from the creative writing literature, that runs through POPI is that consent is required for processing personal information. Given that the terms "consent", "data subject", "personal information", "processing", and further related terms will be mentioned throughout this chapter, it is useful to set out the manner in which they are defined in POPI.

The term "consent" is defined as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".[1211] De Stadler *et al* explain that there seems to be a "myth" that once consent is given for the processing of information, it allows the responsible party to do whatever they may wish with the personal information. This is not true as part of the definition refers to "specific" consent, or consent limited to the purpose for which it was given.[1212] This issue is explored in a bit more detail later in the thesis. "Data subject" means "the person to whom personal information relates".[1213] The definition of "data subject" is not limited to an "identifiable living person", but includes an "existing juristic person", as juristic personae too have a private sphere that is worth protecting.[1214]

"Personal information" bears a longer definition, which reads as follows:[1215]

[1211] Section 1 of POPI.

[1212] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 65 – 70 – here the authors explain every aspect of what it entails to give consent, as the words are explicit, ie "voluntary", "specific", "informed expression". The authors often refer to consent as "the c-word" based on the myth and the staggering number of blanket consents in contracts (that are hidden and are often invalid). Hence, the definition of consent is important to keep in mind throughout POPI. De Stadler *et al* give an enormous amount of information and pointers to keep in mind with regards to "consent", which goes beyond the scope of this work, however, important to note is that withdrawing consent should be as easy as giving it, see De Stadler *et al* at 432, 486 – 487, and 574 – 575.

[1213] Section 1 of POPI. Note the definition of 'person' set out above.

[1214] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 79 – note the "key point" discussion on that page. See also SALRC (Project 124) *Report on Privacy and Data Protection* (2009) para 3.3.40ffg. For an in-depth discussion, see Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 629 – 649.

[1215] See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 80 – 81 for a breakdown of parts *(a)* to *(h)*. De Stadler *et*

"information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to —

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

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

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

(d) the biometric information of the person;[1216]

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

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

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

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

The definition of personal information is deliberately kept wide to allow the courts, the information regulator, and any other responsible person to expand on and make a suitable decision, depending on the circumstances.[1217] Apart from personal information, POPI also

al at 79 points out that this is not an exhaustive list, and "should not be treated as a checklist", there is possibly other information that may be considered to be personal information, depending on the circumstances of each matter. A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 403 – 404.

[1216] "Biometric information" does not have a specific definition in terms of POPI, but "biometrics" in POPI is defined in s 1 as "a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition." E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 214 suggest that biometric information, especially with regards to photos and videos of individuals, in the practical sense should mean data that has undergone some technical processing for it to be considered biometric information – see the definition of biometric data in Article 14 of the GDPR. See also s 1 of PAIA.

[1217] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 19, 79 – 82, 298 – 299 (in relation to online identifiers and cookies), and 562 – 563 (note that in PAIA and POPI the definitions of personal information differ slightly, because PAIA protects third party deceased's personal information for 20 years before releasing it in terms of access requests whereas POPI applies to living individuals or natural persons – see also F Cronjé and E Laubscher *PAIA: What you need to know* (2016) at 19). See N Mashinini 'The processing of personal information using

makes provision for "special personal information", which is defined as "personal information as referred to in section 26". There is a short discussion on this aspect later in the chapter. Generally, personal information will be kept in a "filing system". According to the definition of a "filing system", the system need not be centralised and may be geographically dispersed. A filing system must merely be "a structured set of personal information . . . which is accessible according to specific criteria".[1218]

"Processing", similarly to personal information, has a very comprehensive definition, which reads as follows:[1219]

> "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;
>
> *(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".

"Restriction", considering the definition for processing, is defined as "to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information". "Operator" is another important definition to bear in mind. POPI defines an operator as "a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party".[1220] In other words, an operator may only process personal information on behalf

---

remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140 at 150 – 153 and S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 401 – 403. According to Edros, the GDPR does not apply to deceased persons, see D Edros 'Dead ringers? Legal persons and the deceased in European data protection law' (2021) 40 *Computer Law & Security Review* 105495 1 at 3.

[1218] Section 1 of POPI, N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) De Jure Law Journal 140 at 154, and S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 403.

[1219] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 84 – note where 'an organisation has personal information, it is processing it', and N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140 at 149 – 150. See also *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 32.

[1220] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 115 – 116, specifically at 116, the authors write that in terms

of the responsible party with their knowledge or authorisation.[1221] "Responsible party" is defined as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[1222] The responsible party will still be responsible for the processing of the personal information, even where this is carried out by a third person or company, on their behalf, ie an operator.[1223]

As set out above, personal information is information that identifies the person. Regarding "identifying", the concepts of "de-identifying" and "re-identifying"[1224] are important. Starting with "de-identifying" ("de-identified" has a corresponding meaning) the legislature has defined it as[1225]

> "in relation to personal information of a data subject, means to delete any information that—
>
> *(a)* identifies the data subject;
>
> *(b)* can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

---

of POPI, operators are not directly accountable to the Information Regulator, instead, they are accountable only to the responsible party. Unlike operators, responsible parties are directly accountable to the Information Regulator. Although operators are not directly accountable to the Information Regulator and therefore cannot be sued in terms of POPI, data subjects are still entitled to sue operators in terms of the common law. The EU addressed a similar loophole in the GDPR by making "it clear that data processors can be held directly liable" by the supervisory authority, ie the GDPR's Information Regulator.

[1221] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 121 – note there should be a clear agreement that specifies that operators are to process personal information on behalf of a responsible party, where it explicitly clarifies their authorisations, and outline the measures that are in place to ensure confidentiality. See also S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 400 – 401.

[1222] The definition encompasses both natural and juristic persons, and allows for more than one responsible party, to work in conjunction with another. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 85, and L Swales, D Thaldar & D-L Donnelly 'Why research institutions should indemnify researchers against POPIA civil liability' (2022) 118(3/4) *South African Journal of Science* 22 at 22. See also *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 33. For an in-depth discussion, see Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 651 – 679.

[1223] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 113 – 114, see also the SALRC (Project 124) *Report on Privacy and Data Protection* (2009) para 4.2.34, N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140 at 153 – 154, and S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 400 – 401. See also European Data Protection Board *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* adopted 2 September 2020 at 3 – 4, note the concept of a "controller" is, in the EU, the equivalent of a "responsible party" in South Africa, and "processor" is the equivalent of an "operator".

[1224] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 90.

[1225] Section 1 of POPI, and for a discussion see E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 90 – 91.

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject".

And "re-identifying" ("re-identified" has a corresponding meaning) is defined as:

> "in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—
>
> *(a)* identifies the data subject;
>
> *(b)* can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
>
> *(c)* can be linked by a reasonably foreseeable method to other information that identifies the data subject".

De-identified information or pseudonymised information should not be confused with the term "anonymisation", as de-identification merely disguises the information, and the process is reversible, making it possible to find out who is behind the façade.[1226] De-identifying involves "deleting" the personal information to the extent that it can no longer be allocated to the data subject, but it is still possible to reverse the process, using a reasonably foreseeable method.[1227] The same cannot be said for anonymisation, as the process used is irreversible, meaning the personal will no longer be attributable to the original data subject. However, in s 6, POPI excludes "de-identified" (or pseudonymised) personal information that is no longer be capable of being re-identified. Hence, the possible confusion created by POPI with these three terms.[1228] Re-identifying information allows for the "resurrection" of any de-identified personal information to make it locatable to the data subject.

Similarly, to the definitions of "personal information" and "processing", "record" has a wide definition to incorporate as many types of records as possible, with the word "including" suggesting that it is not a closed list, and that other forms of "recordings" could also constitute a "record" for the purposes of POPI.[1229] A "record" that contains personal information, is

---

[1226] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 92. For a discussion on de-identified data and whether POPI will apply see D Thaldar 'Does data protection law in South Africa apply to pseudonymised data?' (2023) 14 *Frontiers in Pharmacology* 1238749 1 – 6. Note also M Hintze & K El Emam 'Comparing the benefits of pseudonymisation and anonymisation under the GDPR' (2018) 2(2) *Journal of Data Protection & Privacy* 145 at 146 – 147.

[1227] L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808 1 at 2.

[1228] L Swales 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808 1 at 1 – 2.

[1229] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 6 – 7 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The*

defined as follows:[1230]

> "any recorded information—
>
> *(a)* regardless of form or medium, including any of the following—
>
> (i) Writing on any material;
>
> (ii) information produced, recorded or stored by means of any tape-recorded, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
>
> (iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
>
> (iv) book, map, plan, graph or drawing;
>
> (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
>
> *(b)* in the possession or under the control of a responsible party;
>
> *(c)* whether or not it was created by a responsible party; and
>
> *(d)* regardless of when it came into existence".

A record will therefore include information that details decisions, processes and any further necessary information that is documented, ie is proof of decisions or actions taken by the responsible party or operator, as required in terms of legal obligations, financial regulations, for operational requirements, or historical purposes.[1231] The inclusion of "personal information" in the definition of "record" indicates that a responsible party may have had previous interactions with a data subject, and where these are documented, the documented interactions will amount to a record in terms of POPI. However, that does not mean that the

last POPIA book you will ever need (2021) at 84 – 85. De Stadler *et al* added to the list, as set out above from POPI, 'cave paintings, clay tablets and smoke signals', these possibly are 'records' in terms of part *(a)* and *(d)* of the definition, S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 403.

[1230] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 519 provide the following simplified definition of "record":

> "Any recorded information, regardless of form or medium, in the possession of the responsible party, whether or not it was created by a responsible party, and regardless of when it came into existence."

[1231] The information may be created by the responsible party, but that does not mean that it is no longer the personal information of the data subject – see E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 520.

information recorded belongs to the responsible party – it still belongs to the data subject.[1232] Based on the definition of personal information, POPI applies to information that is stored in electronic form in an electronic database as well as in a hard copy paper filing system.[1233] Keeping in mind the discussion on "record", note that a "public record" means "a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body."[1234]

The last definitions to note are those of a private body and public body, as there are specific duties regarding the protection of personal information that are applicable to either a private or public body, in terms of both POPI and PAIA. In certain instances, there is an overlap, but there are differences. A private body refers to natural persons or partnerships which run their own company, trade, business or profession – in their personal capacity. The definition also includes "former or existing juristic persons, but excludes a public body." A public body refers to departments of State or the administration in the national, provincial and local (municipal) spheres of government. A public body includes functionaries or institutions that exercise or perform a duty as set out in the Constitution or a provincial constitution or "in terms of legislation".[1235]

(c) Conclusion

The above are the definitions that are most relevant to the thesis. Some of these definitions are elaborated on, especially in terms of the conditions for the lawful processing of personal data, later in this chapter.

[1232] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 519 – 520. Note also s 23 of POPI. Also see s 1 of PAIA, where the definition for record has been kept simpler - F Cronjé and E Laubscher *PAIA: What you need to know* (2016) at 20 – 21.

[1233] N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140 at 153, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 84 – 85.

[1234] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 273. At 274 De Stadler *et al* hold the view that where a fee is payable, it may not be considered to be in the public domain. However, they also point out that in New Zealand, publicly available information may be accessible to the public generally, whether it is free or there is a fee payable. I don't agree with De Stadler *et al* and prefer the New Zealand definition – the fee payable for accessing a public record or record in the public domain, which may be housed by a public body, often amounts to a payment for the copies made or an administrative fee, which does not prevent individuals from reading the documents, etc. containing the information and making their own personal notes. See also the relevant provisions of PAIA.

[1235] Note, that where a public body is processing personal information with regards to national security interests or in terms of criminal investigations and prosecutions, these processing activities are excluded from POPI. However, processing activities, such as the provision of basic services, will fall under the provisions of POPI. POPI does apply to the government where it is processing personal information, the justification for the processing will often be found in a legislative duty – see s 38 of POPI.

III APPLICATION, INTERPRETATION, AND PURPOSE

Section 2 sets out POPI's purpose in broad terms. It provides in this respect that POPI is aimed at "giving effect to the constitutional right to privacy by safeguarding personal information" when it is processed by a responsible party subject to justifiable limitations.[1236] These limitations must be aimed at "balancing the right to privacy against other rights"[1237] and "protecting important interests", especially the "free flow of information".[1238] Apart from safeguarding personal information, section 2 also provides that POPI is aimed at regulating the way in which personal information may be processed, by prescribing minimum legal thresholds for the "lawful processing of personal information" that is in "harmony with international standards",[1239] and by providing persons "with rights and remedies to protect their personal information from" being processed in a manner that is not authorised by the Act.[1240] Finally, section 2 also provides that the purpose of POPI is to establish the Office of the Information Regulator "to ensure respect for and to promote, enforce and fulfil the rights protected" under POPI.[1241]

Section 3 provides for the application and interpretation of POPI.[1242] Specifically,

---

[1236] Section 2*(a)* of POPI.

[1237] Section 2*(a)*(i) of POPI. Section 2*(a)*(i) makes specific reference to the protection of the right to access information as provided in s 32 of the Constitution, but that does not mean that all other rights are excluded from the balancing where there are competing interests. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 45. Note also *My Vote Counts NPC v Speaker of the National Assembly & others* 2016 (1) SA 132 (CC) para 85, and *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 18.

[1238] Section 2*(a)*(ii) of POPI. Section 2*(a)*(ii) includes the free flow of personal information within South Africa as well as "across international borders". See M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 – 19. For a complete discussion or data portability or cross-border data flow, and how SA measures up with the GDPR see M Malahleka 'The problem of trans-border information flows in the protection of personal information' (2024) 27 *Potchefstroom Electronic Law Journal* 1 – 41. Specifically with regards to tax records, see C Fritz '"South African taxpayers" right to privacy in cross-border exchange of tax information' (2021) 11 *Constitutional Court Review* 411 – 432.

[1239] Section 2*(b)* of POPI. See also D Sive & A Price 'Regulating expression on social media' (2019) 136(1) *South African Law Journal* 51 – 83, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 47 – 49. See the following as an example: W Rosenberg 'The mother's right to privacy in infant abandonment cases' (2022) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 92 at 101 – 102 where POPI's purpose is discussed when mothers abandone their infant children and still want their right to privacy to be respected. P Esselaar, L Swales, D Bellengère, B Mhlongo & D Thaldar 'Forcing a square into a circle: Why South Africa's draft revised material transfer agreement is not fit for purpose' (2024) 15 *Frontiers in Pharmacology* 1333672 1 at 3 emphsises that when legislation does not meet the minimum data protection standards as provided in POPI, then POPI must be followed. Where the specific legislative instrument has a more stringent data protection regime in comparison to POPI, then that legislative regime's standards must be followed.

[1240] Section 2*(c)* of POPI.

[1241] Section 2*(d)* of POPI.

[1242] See generally Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 44 – 45, and 396 – 397.

regarding the application of POPI, s 3 states:

> "(1) This Act applies to the processing of personal information—
>
> *(a)* entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and
>
> *(b)* where the responsible party is—
>
> (i) domiciled in the Republic; or
>
> (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic."

"Automated means", for the purposes of s 3, is defined as "any equipment capable of operating automatically in response to instructions given for the purpose of processing information."[1243] Section 3(2) sets out that POPI will override any legislation that provides for the processing of personal data where the legislation is "materially inconsistent" with the provisions of chapter 3, however, where the legislation provides for more extensive conditions and safeguards, then that legislation will be preferred over POPI.[1244] Section 3(3) deals with the interpretation of POPI, and reads:

> "This Act must be interpreted in a manner that—
>
> *(a)* gives effect to the purpose of the Act set out in section 2; and
>
> *(b)* does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of personal information and such processing is in accordance with this Act or any other legislation, as referred to in subsection (2), that regulates the

[1243] Section 3(4) of POPI. Where the processing takes place by "non-automated means" then the physical records are to be kept in a "filing system" which POPI defines "as any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria." See N Mashinini 'The processing of personal information using remotely piloted aircraft systems in South Africa' (2020) *De Jure Law Journal* 140 – 158 at 154, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 85, and S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 403. Note that there is no definition of automated decision-making, or any other similar phrase – Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 7, see also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 133 – 135.

[1244] Section 3(2) of POPI. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 74 and 76.

processing of personal information."

Although s 3 does not expressly state so itself, it can be gathered from the provisions of s 3 that POPI operates within a specific framework. Two points may be made about this framework. First, the field of application of POPI is very wide, especially in comparison to the provisions of the ECT Act. Second, given that its field of application is very wide, POPI is alert to the fact that its provisions may infringe on other fundamental rights and seeks to limit any possible infringements to the bare minimum. Given that POPI is very new and, consequently, that there is very little in the way of relevant case law, it is difficult to know whether POPI has achieved this goal. Only time will tell how POPI will affect the rights and freedoms, especially the right to freedom of expression and the right to information, in the Constitution. De Stadler *et al* point out that, as with all other legislation, a purposive interpretation should be adopted in regard to the provisions of POPI, taking into account the Constitution and the rights enshrined therein.[1245]

Section 4 sets out the conditions for the lawful processing of personal information and the circumstances in which the processing of personal information is excluded or exempted from these conditions. The section also prohibits the processing of the special personal information of a data subject and the processing of the personal information of a child, subject to certain exemptions and specific conditions. POPI provides an overview of the rights of data subjects in s 5. Section 5 of POPI will not be discussed in great detail, because this will amount to a repetition of what will be said throughout this Chapter.[1246] One last point to note regarding s 5 is that it provides a useful starting point where the rights of the data subject have been infringed during the processing of their personal data, as most of the rights listed in s 5 include a reference to their corresponding sections in POPI.[1247]

Sections 6 and 7 provide for certain exclusions in light of the processing of personal data. Section 6 deals with the general exclusions. It provides in this respect that POPI does not apply to the processing of personal information in relation to purely personal or household activities[1248] and in relation to information that has been de-identified to such an extent that it

[1245] Section 3(3) of POPI, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 45 – 46.
[1246] There are other rights that pertain to data subjects that are not listed in s 5 such as those in connection with directories. These are discussed under direct marketing. See s 70 of POPI which deals with directories, see also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 143.
[1247] See s 5 of POPI. See generally Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 133 – 148.
[1248] Section 6(1)*(a)* of POPI. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 89 – 90. See also *Sheburi v Railway Safety Regulator* (CCMA) unreported ruling, case no GATW 15200-21 (2 March 2022) para 24, where the commissioner confirmed that presenting a case at the CCMA "constitutes a purely personal activity". The CCMA

cannot be re-identified.[1249] In addition, section 6 also provides that POPI does not apply to the processing of personal information by public bodies, which involves "national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety".[1250] Neither does POPI apply to the processing of personal information by public bodies which prevent, detect, and investigate offences, in order to combat money laundering, as well as during the prosecution of offenders, nor subsequently, in relation to the execution of sentences or security measures for those convicted.[1251] The legislator must ensure that there are adequate safeguards in place where the personal information is processed during an investigation, prosecution and when a sentence is being executed.[1252] The processing of personal information by the Cabinet, Cabinet Committees and the Executive Councils of provinces,[1253] as well as the processing of personal information by the courts in relation to their functions in terms of s 166 of the Constitution, is also excluded from the provisions of POPI in terms of section 6.[1254]

The exclusions in s 7 relate to journalistic, artistic or literary freedom, and are worded in such a manner that they will apply to the extent necessary in balancing the right to privacy with the right of freedom of expression.[1255] Section 7(2) provides that where a person is

commission missed the mark in this instance, the CCMA is a tribunal, which requires that personal information will be processed in order to comply with a legal obligation (s 11(1)*(c)*) or to protect a legitimate interest of the data subject (s 11(1)*(d)*). This means that POPI does apply to a CCMA matter, as the CCMA is a public body, and may process personal information to comply with its functions (s 11(1)*(e)*). Also the documents (as a record containing personal information) in the matter form a part of a filing system and a CCMA matter is certainly not a household activity. See also S Papadopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 – 408 for a comprehensive discussion on the case.

[1249] Section 6(1)*(b)* of POPI. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 90 – 92.

[1250] Section 6(1)*(c)*(i) of POPI. Note, s 6(2) specifically defines "terrorist and related activities", for purposes of s 6(1)*(c)*, as "those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004)." It is not unusual to have these exclusions, see SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.6.25. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 102 – 105, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 93 – 94. How "national security information" is defined in South African law, see J Klaaren 'The judicial role in defining national security and access to information in South Africa' (2015) 11(3) *Democracy and Security* 275 – 297.

[1251] Section 6(1)*(c)*(ii) of POPI. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 93 – 95.

[1252] Section 6(1)*(c)*(ii) of POPI. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 94.

[1253] Section 6(1)*(d)* of POPI. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 95.

[1254] Section 6(1)*(e)* of POPI.

[1255] See generally Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 105 – 108 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 70 and 95 – 97. Note also *NM & others v Smith & others* 2007 (5) SA 250 (CC), and the courts extensive discussion on the rights at play with regards to

employed as a professional journalist, and that person is subject to a code of conduct that adequately protects personal information, then that code of conduct and not POPI will apply to the processing of personal information. It also provides that any disputes relating to the processing of personal information must be adjudicated in terms of the code. Section 7(3) lists the points that must be considered in "the event that a dispute may arise in respect of whether adequate safeguards have been provided for in a code as required in terms of subsection (2) or not".[1256]

To conclude this part of the discussion, the legislature has made an effort to remind everyone that ultimately, freedom of expression and the right to privacy will need to be balanced, where there is a conflict in terms of POPI. The right to privacy is not absolute, except perhaps in a few limited circumstances. The legislature, through the enactment of POPI, has emphasised the importance of protecting personal information, and the need to keep such information private and confidential.

IV PROCESSING OF PERSONAL INFORMATION

(a) General principles

POPI places itself within the constitutional values of democracy and openness.[1257] The principal aim of POPI is to give effect to s 14 of the Constitution, which "includes a right to protection against the unlawful collection, retention, dissemination and use of personal information".[1258] As these quoted words indicate, POPI distinguishes between lawful and

---

this exemption. Compare with N Bitiukova 'The GDPR's journalistic exemption and its side effects: GDPR anniversary – What does it mean for the media?' *VerfBlog*, 16 June 2023.

[1256] See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 97 and *The Press Code of Ethics and Conduct for South African Print and Online Media* is available at *https://presscouncil.org.za/ContentPage?code=PRESSCODE*, accessed 3 February 2022. The considerations in s 7(3) read as follows:

> "*(a)* the special importance of the public interest in freedom of expression;
> *(b)* domestic and international standards balancing the—
> (i) public interest in allowing for the free flow of information to the public through the media in recognition of the right of the public to be informed; and
> (ii) public interest in safeguarding the protection of personal information of data subjects;
> *(c)* the need to secure the integrity of personal information;
> *(d)* domestic and international standards of professional integrity for journalists; and
> *(e)* the nature and ambit of self-regulatory forms of supervision provided by the profession."

[1257] Preamble of POPI, A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 at 53.

[1258] Preamble of POPI. Note the discussion of the role of the courts in *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* [2019] ZAGPPHC 384 and *Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others* 2021 (3) SA 246 (CC). Regarding the processing of personal information during criminal investigations,

unlawful processing of data. In the eyes of the legislature the unlawful processing of personal information unjustifiably infringes the constitutional right to privacy. The lawful processing of personal information thus lies at the heart of POPI. Hence, the legislature has tried to strike a proportionate balance between privacy and other rights, especially the right to freedom of expression, through the mechanism of the "lawful" processing of data.[1259] The lawful processing of personal information is dealt with in Chapter 3. This chapter provides that the processing of personal information will be lawful only if it satisfies the conditions set out in the chapter itself. These conditions are based on the concepts of fairness and reasonableness and have been divided into eight categories.[1260] These categories are as follows (1) accountability, (2) processing limitation, (3) purpose specification, (4) further processing limitation, (5) information quality, (6) openness, (7) security safeguards, and (8) data subject participation. They are the minimum standards for the lawful processing of personal information. Apart from these eight conditions, there are additional conditions that apply when special personal data is being processed, when the personal data of a child is being processed or when data is being processed for direct marketing.[1261]

All of these conditions will be discussed in this next part of the chapter.

(i) Condition one: Accountability

The first condition of lawful processing is entitled "accountability" and it is set out in s 8. Accountability is one of the key themes that runs throughout POPI. Section 8 provides that the

---

and the safeguarding thereof see C Hugo & W Spruyt 'Money laundering, terrorist financing and financial sanctions: South Africa's response by means of the Financial Intelligence Centre Amendment Act 1 of 2017' (2018) 2 *Journal of South African Law* 277 at 236. For the importance of protecting personal information against identity theft see F Cassim 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18(2) *Potchefstroom Electronic Law Journal* 69 at 78 – 80.

[1259] M Pelteret & J Ophoff 'Organizational information privacy strategy and the impact of the PoPI Act' In *2017 Information Security for South Africa (ISSA)* (16 - 17 August 2017, Johannesburg, South Africa) 56 at 58. For a longer discussion, with a comparative with the GDPR, see Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 177 – 293.

[1260] POPI does indicate that there will be instances where data processing falls outside of these eight categories, but expects that the processing does comply with these basic conditions on a whole – see M Njotini 'Securing shareholder information in the digital age — An analysis of the proposed amendments to section 26 of the Companies Act' (2020) 32(3) *South African Mercantile Law Journal* 334 – 359, especially at 349.

[1261] See generally A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 61 – 64, chapter 4 in Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 43 – 81, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) the conditions are discussed throughout the book in quite some detail. See V Basdeo 'Criminal and procedural legal challenges of identity theft in the cyber and information age' (2017) 30 *South African Journal of Criminal Justice* 363 at 373 – 375 where the author discusses how POPI's processing principles could effectively be used in proceedings dealing with identity theft.

data subject may hold the responsible party, including the operator in certain instances, accountable when processing their personal information, and where the minimum safeguards have not been met.[1262] Section 8 is specifically titled "responsible party to ensure conditions for lawful processing". This means that the responsible party is obliged to ensure that all conditions and measures as set out in Chapter 3, but also throughout POPI, are complied with at the time the purpose for processing is determined as well as "during the processing itself".[1263]

(ii) Condition two: Processing limitations

The second condition is entitled "processing limitations". These limitations are set out in sections 9, 10, 11 and 12. Each section will be discussed separately:

1. Section 9 is labelled "lawfulness" and provides that the processing of personal information must be lawful and reasonable. De Stadler *et al* suggest that it is possible to determine the lawfulness of the processing by using the six legal justifications contained in s 11(1) of POPI (these are discussed below).[1264] In relation to reasonableness, it is submitted, that the factors set out in *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs*[1265] to determine whether administrative decisions are reasonable or not, may provide useful guidance.[1266] The requirements of lawfulness and reasonableness ensure transparency during the process.[1267]

[1262] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 45 – 46 and E De Stadler, IL Hatting, P Esselaar, J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 112, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 23 – 24, and 26. See also Recital 25 of the Preamble of Directive 95/46.

[1263] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 111 – 153, B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *South African Law Journal* 122 at 121 – 123.

[1264] And I agree, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 3. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 48. De Stadler *et al* suggests that "lawfulness" or rather "lawful purpose" requires the responsible party to first, determine the reason (ie purpose) for the processing of the personal information. Second, do one of the six legal justifications apply? (See point 3 in this discussion as well as the complete discussion on these points further below.) E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 185 – 204. See *Munetsi v Madhuyu & another* [2024] ZAWCHC 209 para 8.

[1265] *Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs & others* 2004 (4) SA 490 (CC) para 45:

> "Factors relevant to determining whether a decision is reasonable or not will include the nature of the decision, the identity and expertise of the decision-maker, the range of factors relevant to the decision, the reasons given for the decision, the nature of the competing interests involved and the impact of the decision on the lives and well-being of those affected."

See also *Minister of Health & another NO v New Clicks South Africa (Pty) Ltd & others (Treatment Action Campaign & another as amici curiae)* 2006 (2) SA 311 (CC).

[1266] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 48 – 49.

[1267] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 50. See

2. Section 10 is labelled "minimality" and provides that the processing of personal information must be adequate for the purpose and not excessive. The minimum amount of processing required to meet the reason for the processing of personal information satisfactorily is required – "less is more".[1268] Minimality requires that the minimum amount of data, applicable for the purpose and outcome of the processing be collected.[1269]

3. Section 11 is labelled "consent, justification and objection" and provides that the processing must be with the consent of the data subject. It should be emphasised that consent is but one of the justifiable grounds for the processing of personal data.[1270] The data subject may object to the processing of their data (discussed in full below).[1271] It is worth noting at this point that several sections specifically mention the need to obtain the data subject's consent to process their personal information, hence consent is a very important requirement for the lawful processing of personal information.[1272] However, personal information may also be lawfully processed in terms of a contract or law.[1273]

4. In s 12 the legislature requires that the data is collected directly from the data subject,

---

also Recital 63 of the Preamble to Directive 95/46, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 52, 185 – 204 and 254, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 8 – 10, and 25. See also W Lim 'Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa' (2020) 20(2) *African Human Rights Law Journal* 540 at 551 – 553.

[1268] See also s 16 of POPI regarding quality of information. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 50 – 51, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 253 – 268, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 13 – 14, and 25.

[1269] See also Recital 28 of the Preamble and Article 6(1)*(c)* of Directive 95/46, and A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 407 to compare with the UK.

[1270] W Freedman & H Schultz 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 at 25.

[1271] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 51 – 58 and 108 – 120 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 185 – 204, 432, 486 – 487 and 574 – 575. See also *Divine Inspiration Trading 205 (Pty) Ltd and another v Gordon and others* 2021 (4) SA 206 (WCC) para 30ffg, and Article 6 of the GDPR. Sections 11(3)*(a)* and *(b)* are rights specifically listed in sections 5*(d)* and *(e)*(i).

[1272] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 69. De Stadler *et al* encourage responsible parties to not base their reason for the processing on consent alone – the data subject has an absolute right to withdraw the consent. It is best to justify the processing in terms of a contract or law, as this will, unless there is an objection, make it easier for the responsible party to maintain a smooth flow when processing personal information – see at 198 – 199, and 574 – 575.

[1273] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 198 – 199. The courts do not process personal information based on consent, but in terms of a legal obligation within the relevant legislation or regulation or rules.

unless one of the exceptions apply, for example, where the information is contained in a public record, or there would be no prejudice arising irrespective of where this data is collected, or where it is not practical to obtain the consent of the data subject.[1274] POPI allows for the collection of data from other sources and not directly from the data subject, in specific instances.[1275]

(iii) Condition three: Purpose specification

The third condition is entitled "purpose specification". It is important that a responsible party specifies the purpose for collecting and retaining personal information in sufficient detail so the data subject knows what they are consenting to. The requirements are set out in sections 13 and 14 of POPI. Each section will be discussed in turn.

1. Section 13 is labelled the "collection for [a specified] purpose" and provides that the information must be collected for a "specific, explicitly defined and lawful purpose" that is connected to a function or activity of the responsible party, and that it may not be processed beyond that purpose or function. This links in with the notion of minimality.[1276] The responsible party must take reasonably practicable steps to inform the data subject, in terms of s 18(1), that their information is being collected and processed.[1277] There is no requirement in terms of POPI that the data subject must supply their personal information in writing and append their signature below it, however, it is preferable that such information be collected in writing, and duly signed.[1278]

[1274] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 56 – 57, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 102, 104, 271 – 278, 289 – 294, 299 – 304, and 406 – 408.

[1275] See s 12(2) of POPI. These instances include the avoidance of prejudice in the upholding the law by any public bodies (this includes criminal investigations and prosecutions), the legal obligation regarding the collection of revenue – ie the South African Revenue Services, in terms of the procedural rules of courts and tribunals, in the interests of national security, or the preservation of legitimate interests of the responsible or third party to whom the information is supplied. See Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 57 – 58 and 108 – 120, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 279 – 283, 289 – 294, 299 – 300, 406 – 408, and 417 – 418.

[1276] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 106, 188 – 189, 255, and 310. See s 10 of POPI.

[1277] Sections 13(2) and 18 (1) of POPI. There are certain exceptions, see s 18(4) of POPI. Also see Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 58 – 59, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 188, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 11 – 13, and 25.

[1278] Compare with various countries as discussed in SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) paras 4.2.37 and 4.3.8. Regulation 6 of the Regulations relating to the Protection of Personal

2. Section 14, which is labelled "retention and restriction of records" should be read with s 24 where the deletion or destruction or de-identification of the personal information is granted specifically in terms of s 24(1).[1279] Section 14(1) employs peremptory language and states that records are not to be retained for a period longer than is necessary to achieve the purpose for which the data is collected. However, data may be retained longer than is necessary where this is prescribed by law, or prescribed by a contract or where the data subject, or a competent person in the case of a child, has consented to the longer retention of the data.[1280] Section 14(2) also allows for the retention of records, for periods longer than those prescribed in section 14(1) for historical, statistical or research purposes. In such a case, the responsible party must provide suitable safeguards to ensure that the records will not be used for any other purpose.[1281] Although the general rule in section 14(1) is that records may not be retained for a period longer than is necessary to achieve the purpose for which the information was collected and the subsequent processing thereof, section 14(3) provides that records must be retained where this is authorised by law, or where the responsible party "reasonably requires the record for lawful purposes related to its functions or activities".[1282] Sections 14(4) and (5) require that the responsible party must attend to the destruction, deletion or de-identification of the record containing the personal information as soon as reasonably possible, and in such a manner that it cannot be reconstructed into an understandable document.[1283]

Information Act, GN R 1383, *GG* 42110 of 14 December 2018 requires that in terms of direct marketing (see s 69 in POPI) the data subject must sign a written consent for the processing of the personal data – see also Form 4 in the aforementioned regulation.

[1279] See generally Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 60 – 63, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 517 – 536, W Rosenberg 'The mother's right to privacy in infant abandonment cases' (2022) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 92 at 104 – 105, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 15 – 16, and 26.

[1280] Section 14(1) of POPI reads:

> "Retention and restriction of records. — (1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless —
> *(a)* retention of the record is required or authorised by law;
> *(b)* the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
> *(c)* retention of the record is required by a contract between the parties thereto; or
> *(d)* the data subject or a competent person where the data subject is a child has consented to the retention of the record."

[1281] Section 14(2) of POPI.

[1282] Section 14(3)*(a)* and *(b)* of POPI.

[1283] Sections 14(4) and (5) of POPI. The following should be noted: s 14(6) requires that "the responsible party must restrict that processing of personal information" where the accuracy thereof is disputed, is no longer needed

(iv) Condition four: Further processing limitation

The fourth condition is entitled "further processing limitation" and it is set out in section 15. This section provides that where further processing of the personal information is needed it must be in line with the original purpose for which the personal information was collected.[1284] The factors that must be taken into account to assess whether further processing is necessary are also set out in section 15. These include the reason for which it was collected; the nature of the information; the consequences of the further processing; how the information was collected, and any contractual rights held by, or obligations owed to, the data subject.[1285] However, further processing will not be incompatible with the original reason for the collection where consent was obtained; the information is available in a public record or is public knowledge; for historical, statistical or research purposes; to maintain law and order; where there is an exemption from the Information Regulator;[1286] or to prevent an imminent threat.[1287]

(v) Condition five: Information quality

The fifth condition is entitled "information quality" and it provides that the information must be complete, accurate, not misleading and updated where necessary, that is, the quality of the information must be of a high standard.[1288] The responsible party must also keep in mind the purpose for which the collection of the personal information was authorised.[1289] If the quality

to achieve the responsible party's purpose for the collection thereof, the processing is unlawful and instead of requesting the destruction or deletion thereof, the data subject has requested that the continued processing be restricted, and or it is processed in terms of an automated system. In line with this s 14(7) requires that the personal information may only be processed for the purposes of storing and proving the data subject's (or competent person in relation to a child) consent to the processing thereof or for the protection of another natural or juristic person's rights in light of the processing thereof. Lastly, s 14(8) the responsible party must inform the data subject 'before lifting the restriction on' the processing thereof.

[1284] Section 15(1) of POPI. MM Mswela 'Tagging and tracking of persons with albinism: A reflection of some critical human rights and ethical issues arising from the use of the global positioning system (GPS) as part of a solution to cracking down on violent crimes against persons with albinism' (2019) 22 *Potchefstroom Electronic Law Journal* 1 – 28.

[1285] Section 15(2) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 63 – 64 and 108 – 120 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 351 – 370.

[1286] See s 37 of POPI.

[1287] Section 15(3) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 64 – 65, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 365 – 366.

[1288] Section 16 of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 65 – 66, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 253 – 268, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 14 – 15, and 25.

[1289] Section 16(2) of POPI

of the information is poor, it could be damaging to the data subject.[1290]

(vi) Condition six: Openness

The sixth condition is entitled "openness" and it is aimed at ensuring that data is not processed under a shroud of secrecy and suspicion which would ultimately spark distrust. The condition thus provides that the collection of data must be open and transparent.[1291] Most importantly, this means that the data subject must be made aware, not only of the fact that the information is being collected, but also of the reason for which the information is being collected.[1292] In order to meet this minimum standard, the responsible party must take practical steps to inform the data subject that their personal information is being processed and the source, if not from the data subject directly, from where the personal information was collected. The responsible party must also provide their name and address, the reason for collecting the personal data, whether such collection is mandatory or voluntary and the consequences of not providing the personal information.[1293] Openness has two aspects. These are set out in sections 17 and 18,

---

[1290] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 65, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 261 – 262.

[1291] "Transparency" like "reasonableness" does not carry a specific definition within the case law or any legislative instrument, but, along with accountability and fairness, are constitutional values that are required to act like a thread where administrative processes have an impact on human rights. Transparency is provided in the preamble, amongst others, of the Consumer Protection Act 68 of 2000, to be employed when developing innovative legislative means to protect and redress the rights of consumers. In terms of the Consumer Protection Act, PN Stoop and C Chürr 'Unpacking the right to plain and understandable language in the Consumer Protection Act 68 of 2008' (2013) 16(5) *Potchefstroom Electronic Law Journal* 515 at 520 wrote the following, which describes "transparency" succinctly and sets out possible points to consider that may be of use for the application of POPI:

> "Substantive fairness relates to procedural fairness through the requirement of transparency. That is because a high level of transparency means that the consumer is placed in a position at least to have a chance of being able to exercise a reasonable degree of informed consent. So what is a high level of transparency? A good level of transparency has to do with, among other things, aspects such as information disclosure, awareness of the terms, the size of the print, the clarity of the language, and the interpretation and format, as these procedural factors relate to circumstances surrounding the manner in which agreement is reached. Transparency can be a negative control which allows at most the elimination of unclear and incomprehensible contract terms, or it may provide for positive duties, such as the duty to explain and summarise the implications of certain contractual terms. A high level of transparency means that the consumer is placed in a position at least to have a chance of being able to exercise a reasonable degree of informed consent. Transparency therefore enhances choice and fairness substantively." (footnotes omitted)

S Eiselen 'Digitisation and consumer law in South Africa and Africa' (2021) 3 *Tydskrif vir die Suid-Afrikaanse* 436 – 455.

[1292] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 66 – 67, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 305 – 349.

[1293] Section 18(1) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 66 – 67, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 305 – 349. Section 18(1) requires that "reasonably practical steps" must be taken "to ensure that the data subject is aware of"

> "*(a)* that his or her personal data is being collected, as well as the source for such information where it is not directly from the data subject;

and each is discussed individually as follows:

1. Section 17 provides that the responsible party must safeguard all the documents collected and used during processing, in line with sections 14 and 51 of PAIA.[1294]

2. Section 18 provides that the purpose or reason for collecting the personal information must be communicated to the data subject. In order to fulfil this obligation, the responsible party must make a reasonable effort to provide the data subject with the following information: the source of the data, if not from the data subject personally; whether it is voluntarily or mandatory to give the information and any consequences if not provided; the persons with whom the data will be shared; and so on. This obligation ties in with s 13 of POPI discussed above. Section 18 provides that the data subject may hold the responsible party accountable during the processing of their personal information. There are instances where compliance is not strictly necessary, as set out in s 18(4).[1295]

(b) the contact details of the responsible party, including address and name;
(c) the reason of purpose for the collection;
(d) whether the information supplied is on a mandatory or voluntary basis;
(e) the consequences, if any, for failing to supply the correct information;
(f) whether there is a legal obligation that requires the collection and/or processing of the personal information;
(g) whether the information, depending on the circumstances, will be transferred to a third party, third country or international organisation and the level of protection of that information;
(h) any further information that may be required, regarding the category of the information or persons needing the information, the ability to rectify the information and the objection to the processing, where this is applicable, as well as the right to lodge a complaint with the Information Regulator."

See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 68 – 70 and 108 – 120, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 313 – 323 and 332. Section 18 is a right specifically listed in s 5*(a)*(i).

[1294] Section 14 of PAIA in terms of public bodies and s 51 in terms of private bodies, that the information officers or head officer, respectively, must draft a manual containing their functions, an index of records held, what information must be requested in terms of PAIA and what not, and their functions and reasons for collection as per POPI. These manuals need to be updated regularly, and need to be available, especially for a public body, in all the 11 official languages. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 67 – 68 and 108 – 120, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 36 – 42 (provides examples of the various documents that need to be safeguarded for this purpose) and 307. See also F Cronjé and E Laubscher *PAIA: What you need to know* (2016) at 35 – 39 and 86 – 89.

[1295] Section 18(4) of POPI states that the responsible party need not comply with the requirement of informing the data subject regarding the collection of their personal information where:
(a) consent has been provided for the non-compliance;
(b) the legitimate interests of the data subject, in terms of POPI, will not be prejudiced;
(c) the collection is in light of a legal obligation to maintain law and order, or it is in line with the legislative obligations of the South African Revenue Services, or it is in terms of court or tribunal proceedings, or for interests of national security;
(d) compliance with s 18(1) would interfere with the lawful purpose of the collection;
(e) in the circumstances, compliance would not be reasonably practicable;

(vii) Condition seven: Security safeguards

The seventh condition is entitled "security safeguards" and is couched in explicit terms. The minimum-security standards for the protection of personal information are set out in sections 19, 20, 21 and 22. These must be adhered to due to the sensitivity often associated with personal information, and each section entails the following:[1296]

1. Section 19 provides that the responsible party must take reasonable steps to ensure that the personal information is secured in order to protect the integrity and confidentiality thereof. The reasonable security steps must take the form of "appropriate, reasonable technical and organisational measures" and must be aimed at preventing loss, unauthorised damage or destruction, and unlawful access or processing of the personal information.[1297] The responsible party must also take reasonable measures in order to identify, establish and maintain appropriate safeguards against any foreseeable internal and external risks to the personal information in their control. These safeguards must continually be verified, efficiently implemented and updated in order to respond to any new foreseeable risks or combat any deficiencies.[1298]

2. Section 20 provides that whenever an operator is processing personal information on behalf of a responsible party, that operator must treat it with the necessary confidentiality, and may not disclose such information unless the law requires the

---

(f) the information will be de-identified, ie no one can trace it back to the data subject, alternatively it is for historical, statistical or research purposes.

As paraphrased from s 18(4) of POPI, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 69 – 70, and 157, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 333 – 337.

[1296] The *Oxford Dictionary of Law* 7ed (2009) defines "data protection" as "safeguards relating to personal data, ie personal information about individuals that is stored on a computer and on 'relevant manual filing systems'". See also A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 406, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 19 – 21, and 26.

[1297] Section 19(1) of POPI. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 70 – 71 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 156 – 171.

[1298] Section 19 (2) of POPI. In terms of s 19(3) "the responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations." Note that the definition of "record" includes stored personal information. It is important, especially where personal information is stored in a database, that such database is secured. See generally I Govender 'Mapping "Security Safeguard" Requirements in a data privacy legislation to an international privacy framework: A compliance methodology' In *2015 Information Security for South Africa* (*ISSA*) (12 – 13 August 2015, Johannesburg, South Africa) 1 – 8. See also B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *South African Law Journal* 122 at 123 – 124, and S Huneberg & K Berry 'Big data and the paradigmatic shift from passive insurer towards risk personalisation' (2022) 2 *Tydskrif vir die Suid-Afrikaanse Reg* 283 at 307.

disclosure thereof.[1299]

3. Section 21 provides that where an operator processes personal information on behalf of a responsible party, in terms of a written contract, the responsible party must impose on the operator an obligation to establish and maintain the security measures mentioned and put in place in terms of s 19.[1300] Where there is a security breach, the operator must notify the responsible party accordingly.[1301]

4. Section 22 prescribes that the data subject and the Information Regulator must be notified where there is a data breach.[1302] However, the responsible party may delay notification where the identity of the data subject cannot be established, but must inform them as soon as their identity is known.[1303] The notification must be in writing, it must contain sufficient detail regarding the breach, and it must be communicated to the data subject, as per POPI.[1304] The information contained in the notification must be sufficiently detailed to allow the data subject to take steps proactive against the breach. This will include the consequences for the data subject of the breach, any steps that they may take to mitigate the effects thereof, and the steps that the responsible party intends taking against the breach.[1305]

[1299] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 71 – 72, see generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 118 – 126, 157, and 177 – 180. Note, not all personal information will be protected from non-disclosure, depending in the circumstances of the matter before the court, see *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 29. In light of PAIA, access is to information should be the general default position, to promote transparency, see *South African History Archive Trust v South African Reserve Bank and another* 2020 (6) SA 127 (SCA) para 33.

[1300] Section 21(1) of POPI, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 72, see generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 118 – 126.

[1301] Section 21(2) of POPI, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 72, see generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 118 – 126.

[1302] Section 22(1) of POPI, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 72 – 74 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 171 – 177. Section 22 is a right specifically listed in s 5*(a)*(ii).

[1303] Section 22(3) of POPI, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 72 – 74 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 175 – 176.

[1304] Section 22(4) of POPI. The written communication must be: (a) sent to the last known physical or postal address, (b) by email, (c) placed prominently on the website of the responsible party, (d) be a media notification, or (e) in terms of a directive from the Information Regulator. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 73 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 175 – 176.

[1305] Section 22(5) of POPI. The Information Regulator may request that the responsible party publicise the breach, regarding the compromised personal information where this protects the data subject. See E De Stadler, IL Hatting,

(viii) Condition eight: Data subject participation

The last and eighth condition is entitled "data subject participation". This condition acknowledges the protection of the data subject's personal information, and provides the data subject with a measure of personal influence and control over their personal information.[1306] The sections that set out the relevant requirements are sections 23, 24, and 25, and these provide as follows:

1. In terms of section 23, the data subject may ask the responsible party to confirm, free of charge, whether the responsible party holds any personal information relating to the data subject.[1307] In response to such a request, the responsible party must provide the data subject with a report in which it described the information and indicates who else has access to it.[1308] The record must be provided within a reasonable time, at a prescribed fee, if any, and in a reasonable and understandable manner and format.[1309] If the responsible party refuses to provide such a report to the data subject, then adequate reasons must be provided. POPI acknowledges that the right to access personal

P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 176 – 177.

[1306] See generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 551 – 574 and 583, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 24.

[1307] Section 23(1)(*a*) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 74 – 78, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 552. PAIA also provides for the right of access to personal information – see s 11 (with regards to public bodies) and s 50 (with regards to private bodies). These sections enable the data subject a right of access to the records that are held at the respective bodies, provided the relevant statutory provisions are complied with. F Cronjé and E Laubscher *PAIA: What you need to know* (2016) at 33 – 34, and 84 – 85 where the authors point out that although "require" is not defined in PAIA, it does not amount to a "blanket justification for access requests"– see also *Unitas Hospital v Van Wyk & another* 2006 (4) SA 436 (SCA) para 16 (Brand JA's judgment) and para 51 (Cloete JA's judgment). Section 23 is a right specifically listed in s 5*(b)*. The data subject must provide adequate proof of their identification to the responsible party, when the data subject wishes to confirm whether the responsible party has their personal information.

[1308] Section 23(1)(*b*) of POPI. In terms of s 23(3) of POPI, where a fee is payable, the data subject must be provided with the exact amount, alternatively an estimation, and whether the applicant (the data subject) must pay a deposit or the whole fee before the request is attended to. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 75, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 553 – 554 (set out the difference between a record of information and a description). In summary, a record, as defined in POPI and set out above is used to determine when POPI is applicable. A description, on the other hand, is a detailed explanation of the record(s) kept by the responsible party and who has access to the record(s) and the reason(s) for the access.

[1309] Section 23(1)(*b*)(i) – (iv) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 75 – 76, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 553 – 556. Section 23(2) of POPI requires that the data subject must be informed of their right to correct their personal information in terms of s 24.

information may be limited in certain instances.[1310]

2. In terms of s 24, a data subject may ask the responsible party to correct, delete and destroy personal information, if that information is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or if it was "obtained unlawfully". The data subject must provide sufficient credible evidence in support of the correction, deletion or destruction of the information (see the discussion on the right to be forgotten).[1311]

3. Section 25 states that sections 18 and 53 of PAIA apply where a request is made in terms of s 23 of POPI.[1312]

(ix) Conclusion

The conditions have been set out in some detail because they form the crux of POPI. A breach in the conditions will lead to serious consequences, not only for those processing the information but also for the data subject. These conditions may become considerations in weighing up the competing rights of freedom of expression and privacy, for example where a condition is breached, in applying the right to be forgotten. It could be argued that these conditions are aimed at striking a balance between the right to privacy, on the one hand, and the right to freedom of expression and access to information, on the other. Provided these conditions are satisfied, then any infringement of the right to freedom of expression and information will be justified. If this is correct, then an important question is whether the balance struck by parliament is constitutionally valid.

[1310] Section 23(4) of POPI. In terms of s 23(5) of POPI where only a part of the personal information is not disclosed, then the rest must be disclosed. Note sections 30 (public) and 61 (private) of PAIA that deal with the access of health or other (related) records.

[1311] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 78 – 79 and Y Jooste 'The right to deletion identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 – 483. Section 24 is a right specifically listed in s 5*(c)*.

[1312] Sections 18 (public), and 53 (private) of PAIA deal with the form of requests. *Goosen-Joubert v Women4Women NPC* [2022] ZAWCHC 82 and Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 80. Sections 18(1), 18(2), 53(1) and 53(2) of PAIA are similar. These require that the data subject (or applicant) send through the request, via email or fax or by post, to the information officer (ie requisite person). Further, the request must include: sufficient particulars of the record or records requested, and of the requestor (generally the data subject). The request must also state whether the record needs to be in a particular language, specify the fax or postal address of the requestor that is within the Republic, why the record is required, if the outcome must be communicated in a particular manner, and if on behalf of another, the capacity in which such request is being made. The following only applies to a public body (ie s 18(3) of PAIA): where the person is illiterate or disabled, they may make the request orally, and the information officer must reduce the request to writing, on the prescribed form, and supply a copy to the requestor. The requestor is generally the data subject, if they are not acting in a representative capacity. See F Cronjé and E Laubscher *PAIA: What you need to know* (2016) at 43 – 44 and 90 – 91.

(b) Processing of special personal information

The legislature has provided for an extra definition of, and a few extra principles in relation to "special personal information". It is also referred to as "sensitive personal data".[1313] The processing of special personal information is regulated by the provisions of Part B of Chapter 3 of POPI. The concept of special personal data refers to the data listed in s 26, namely "the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, or biometric information of a data subject". In addition, special personal information also includes the "criminal behaviour" of a data subject, but only insofar as it relates to the commission of any criminal offence by the data subject and the proceedings in respect of any such offence. This would include the date of the offence and the subsequent outcomes of the criminal trial, ie a conviction with sentence (whether imprisonment or a fine) or acquittal.[1314] Most countries (especially in Europe) list these aforementioned types of information as special personal information.[1315]

Apart from identifying what is meant by the concept of "special personal information", s 26 of POPI also prohibits a responsible party from processing this information. It is important to note, however, that this general prohibition is subject to the exceptions set out in s 27.[1316] Section 27 provides in this respect that special personal information may be processed if the data subject has consented to the processing;[1317] the data subject has deliberately made the information public;[1318] the processing is necessary to establish, exercise or defend a legal right

[1313] SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.7ffg, A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 at 65, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 83, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 205 – 238, and Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 295 – 344. Note also Article 8 of Directive 95/46.

[1314] Compare with SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.7.2. In cases where mother's abandon their infant children, see W Rosenberg 'The mother's right to privacy in infant abandonment cases' (2022) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 92 at 100 – 105.

[1315] Section 26 of POPI, and SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.7.2. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 83 – 99 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 207 – 215, De Stadler *et al* provides an in-depth discussion of each of the identifying special personal information. See also A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 403, and 407 – 408.

[1316] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 215 – 220.

[1317] Section 27(1)*(a)* of POPI.

[1318] Section 27(1)*(e)* of POPI. Compare with *Smuts & another v Botha* [2022] ZASCA 3 paras 8, 9, 18, 19, 20 and 31.

or obligation;[1319] the processing is necessary to comply with an international law obligation;[1320] or the processing is necessary for historical, statistical or research purposes, but only to the extent that the purpose serves a public interest or it is impossible or very difficult to obtain consent to process the information.[1321]

Special personal information may be processed, where a responsible party has applied for such authorisation with the Information Regulator. The Information Regulator may also, via a notice in the *Government Gazette*, grant prior authorisation to a responsible party to process the special personal information.[1322] Responsible parties must obtain prior authorisation from the Information Regulator to ensure that they comply with provisions of POPI.[1323]

Sections 28 to 33 of POPI provide responsible parties with the authorisation to process special personal information in relation to six separate categories of information in terms of specific legal justifications.[1324] These are, first, a data subject's religious or philosophical beliefs;[1325] second, the data subject's race or ethnic origin;[1326] third, the data subject's trade union membership;[1327] fourth, the data subject's political persuasion;[1328] fifth, the data subject's health or sex life;[1329] and sixth, the data subject's criminal behaviour and biometric

[1319] Section 27(1)*(b)* of POPI.
[1320] Section 27(1)*(c)* of POPI.
[1321] Section 27(1)*(d)* of POPI.
[1322] Section 27(2) of POPI. In terms of s 27(3), the Information Regulator "may impose reasonable conditions in respect of any authorisation granted under subsection (2)."
[1323] Information Regulator (South Africa) 'Guidance Note on Application for Prior Authorisation' (March 2021). *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf* (Accessed: 8 February 2022). See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 219.
[1324] Section 27(1)*(f)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 220 – 232.
[1325] Section 28 of POPI.
[1326] Section 29 of POPI.
[1327] Section 30 of POPI.
[1328] Section 31 of POPI.
[1329] Section 32 of POPI. See MN Njotini 'Preserving the integrity of medical-related information – How "informed" is consent?' (2018) 21 *Potchefstroom Electronic Law Journal* 1 – 20, C Staunton & E De Stadler 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) 109(4) *South African Medical Journal* 232 – 234, W Lim 'Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa' (2020) 20(2) *African Human Rights Law Journal* 540 at 544 – 545, M Botes, A Olckers & M Labuschaigne 'Data Commercialisation in the South African Health Care Context' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 36, DW Thaldar & BA Townsend 'Exempting health research from the consent provisions of POPIA' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 31, D Donnelly 'First do no harm: Legal principles regulating the future of artificial intelligence in health care in South Africa' (2022) 25 *Potchefstroom Electronic Law Journal* 1 – 44, D Thalder & B Shozi 'Is open-identity gamete donation lawful in South Africa?' (2022) 112(6) *South African Medial Journal* 409 at 411 – 412, and F Cachalia & J Klaaren 'Digitalisation in the Health Sector: A South African Public Law Perspective' (2022) 25 *Potchefstroom Electronic Law Journal* 1 – 24. For an overview of where patient-data subject rights are protected in SA's legislative instruments, including POPI, see L Prinsen & EC Muller 'The leading causes behind medico-

information.[1330] Although the specific circumstances in which authorisation for the processing of special personal data has been granted by sections 28 to 33 differs from category to category, there are some common themes across all three categories.[1331]

One theme that appears time and again is the need for the express consent of the data subject before their personal information is shared with third parties.[1332] The special personal information may be processed within the administrative structures of the organisations to which the data subject belongs, or where this is necessary to further the aims of the organisation.[1333] In other instances, the personal information may be processed only where this is for the protection or advancement of the rights of data subjects that have experienced unfair discrimination.[1334] It is noteworthy that POPI grants some latitude with respect to political activities – specifically where the data subject campaigns for a political party during elections, and health – especially where this will further the rights of the data subject, where necessary.[1335] In respect of biometric and criminal behaviour, POPI states that the processing of such information is permitted when processed by law enforcement authorities in line with the applicable rules and legislation.[1336]

(c) Processing of children's personal information

Apart from prohibiting a responsible party from processing special personal information, POPI also prohibits a responsible party from processing a child's personal information. POPI recognises the importance of protecting a child's right to privacy.[1337] It is important to note,

---

legal claims and the use of mediation as a possible solution' (2023) 34(4) *Stellenbosch Law Review* 387 at 391, and A Gooden & D Thaldar 'The regulation of health-related direct-to-consumer genetic tests in South Africa by the Medicines and Related Substances Act' (2024) 141(1) *South African Law Journal* 112 at 114 – 115.

[1330] Section 33 of POPI. Note *The Queen (on application of Bridges) v Chief Constable of South Wales Police & others* [2019] EWHC 2341 (Admin). See BJ Gordon 'Automated Facial Recognition in Law Enforcement: *The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police*' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 30.

[1331] See generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 220 – 232.

[1332] See sections 28, 30, 31 and 33 of POPI.

[1333] See sections 28(3), 30(2) and 31(2) of POPI.

[1334] See sections 29 and 32(1)*(b)*(iii) of POPI.

[1335] See sections 31 and 32 of POPI.

[1336] Section 33 of POPI. See also S Shanapinda 'Asymmetry in South Africa's regulation of customer data protection: Unequal treatment between mobile network operators (MNOs) and over-the-top (OTT) service providers' (2019) 23 *The African Journal of Information and Communication (AJIC)* 1 at 5 – 12.

[1337] L Hertzog *et al* 'Seven essential instruments for POPIA compliance in research involving children and adolescents in South Africa' (2021) 117(9/10) *South African Journal of Science* Art. #12290 1 at 1. For a comparative of POPI with other jurisdictions, see I Milkaite & E Lievens 'Children's rights to privacy and data protecton around the world: Challenges in the digital realm' (2019) 10(1) *European Journal of Law and Technology* 1 – 24. See generally the following on the topic of children, privacy and autonomy: JM Kruger 'Protection of a Child's Right to Privacy in South African Law' In J Potgieter, J Knobel & R Jansen (eds) *Essays in Honour of Johann Neethling* (215) 269 – 283, H Kruger 'The protection of children's right to self-determination

however, that this general prohibition is subject to the exemptions set out in section 35 of POPI.[1338] Section 35 of POPI provides in this respect that a child's personal information may be processed if the child's parents or guardians or some other competent person has consented to the processing;[1339] the child has deliberately made the data public with the consent of his or her parents or guardians or some other competent person;[1340] the processing is necessary to establish, exercise or defend a legal right or obligation;[1341] the processing is necessary to comply with an international legal obligation;[1342] or the processing is necessary for historical, statistical or research purposes, but only to the extent that the purpose serves a public interest or it is impossible or very difficult to obtain consent to process the information.[1343] The Information Regulator may, through the *Government Gazette*, and where appropriate set out reasonable conditions, authorise the processing of a child's personal information where this is in the public interest and the requisite safeguards are in place.[1344]

in South African law with specific reference to medical treatment and operations' (2018) 21 *Potchefstroom Electronic Law Journal* 1 17, and M Bekink 'The constitutional protection afforded to child victims and child witnesses while testifying in criminal proceedings in South Africa' (2019) 22 *Potchefstroom Electronic Law Journal* 1 at 23.

[1338] See A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 at 65 – 66, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 97 – 99; E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 232 – 238. Note s 1 of POPI defines a child as "natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself", and a "competent person" as "any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child". See also P Gabriel 'The Protection of Personal Information Act 4 of 2013 and children's right to privacy in the context of social media' (2019) 82 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 605 – 620 which discusses where the personal data of children are processed in various scenarios, ie in terms of household activities, or by a school, and other instances in which the consent of the parent or guardian will be required, as well as the protection and remedies available where the personal information is processed without the necessary authority. L Hertzog *et al* 'Seven essential instruments for POPIA compliance in research involving children and adolescents in South Africa' (2021) 117(9/10) *South African Journal of Science* Art. #12290 1 – 5 specifically discusses the processing of a child's personal information with regards to research.

[1339] Section 35(1)*(a)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 234 – 235, and see generally, L Hertzog *et al* 'Seven essential instruments for POPIA compliance in research involving children and adolescents in South Africa' (2021) 117(9/10) *South African Journal of Science* Art. #12290 1 – 5.

[1340] Section 35(1)(e) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 219 and 235 – 236.

[1341] Section 35(1)*(b)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 216 – 217 and 235.

[1342] Section 35(1)*(c)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 217 and 235.

[1343] Section 35(1)*(d)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 217 – 218 and 235.

[1344] Section 35(2) and (3) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 236.

(d) Exemptions/exclusions/exceptions

Certain exemptions, exclusions or exceptions may be applicable in certain instances where personal information is processed. A few exemptions or exclusions have been referred to above, first, the following are merely two examples from s 6, the processing of personal information for personal or household interests is exempted,[1345] or where the processing is in terms of s 166 of the Constitution, ie "the judicial functions of a court".[1346] Second, in terms of s 7 of POPI the processing of personal information for journalistic, literary or artistic expression, is exempted in so far as it is necessary in the public interest taking into account the rights of privacy and freedom of expression.[1347] Third, in terms of s 12(1) and (2) of POPI the processing of personal information may take place even though it has not been collected directly from the data subject.[1348] Further exclusions, exemptions or exceptions are contained in Chapter 4 of POPI.[1349] This Chapter consists of only three sections, namely ss 36, 37 and 38. Each will be discussed in turn.

Section 36 of POPI merely provides an overview, namely that the processing of personal information will not be in breach of a condition where, first, the Information Regulator has granted an exemption in terms of s 37[1350] and, second, where the processing is in accordance with certain functions, as provided for in s 38 of POPI.[1351]

Section 37 of POPI provides that the Information Regulator may grant an exemption to a responsible party in certain circumstances. The Information Regulator may, where necessary, impose certain conditions when granting an exemption. To give effect to the exemption and the accompanying conditions, the exemption must be published in the *Government Gazette*.

[1345] Section 6(1)*(a)* of POPI.
[1346] Section 6(1)*(e)* of POPI. See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 102 – 105, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 89 – 90, S Papdopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 404, and Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 357 – 393.
[1347] See also Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 105 – 108, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 95 – 97, and S Papdopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 404 – 405. Note also *NM & others v Smith & others* 2007 (5) SA 250 (CC) extensive discussion on the rights at play with regards to the press exemption.
[1348] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 102.
[1349] See sections 36 – 38 of POPI. See generally Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 101 – 120, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 98 – 100.
[1350] Section 36*(a)* of POPI.
[1351] Section 36*(b)* of POPI.

Where this is the case, the Information Regulator must be satisfied that:[1352]

> "*(a)* the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or
>
> *(b)* the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing."

Section 38 provides that where a responsible party must discharge a relevant function the processing of personal information is exempt from the conditions in sections 11(3) and (4), 12, 15 and 18 and only to the extent of discharging the specific duty.[1353] Note that this will often

---

[1352] Section 37(1) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 108 – 120. Section 37(2) sets out that public interest includes –

> "*(a)* the interests of national security;
> *(b)* the prevention, detection and prosecution of offences
> *(c)* important economic and financial interests of a public body;
> *(d)* fostering compliance with legal provisions established in the interests referred to under paragraphs *(b)* and *(c)*;
> *(e)* historical, statistical or research activity; or
> *(f)* the special importance of the interest in freedom of expression."

Both Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 108 – 120, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 98 expand on s 37(2) with the following examples, in terms of national security, this not only includes the protection and collective welfare of the State, but also includes acts of terrorism against the people living within the State's borders. This ties up with safeguarding law and order, criminal proceedings (including the right against self-incrimination for an offence), as well as courts and tribunals in general. Furthermore, tax and matters concerning revenue, the public health and safety of the individuals or data subjects, and special educational needs. Lastly, parliamentary privilege (see *De Lille v Speaker of the National Assembly* 1998 (3) SA 430 (C), note *Speaker of the National Assembly v De Lille and another* 1999 (4) SA 863 (SCA), and *Dikoko v Mokhatla* 2007 (1) BCLR 1 (CC)), the legitimate interests of the responsible party also play a role and that the data subject remains anonymous. See also the Guidance Note on Exemptions from the Conditions for Lawful Processing of Personal Information in terms of Section 37 and 38 of the Protection of Personal Information Act 4 of 2013, published by the Information Regulator in June 2021, available at *https://www.justice.gov.za /inforeg/docs/InfoRegSA-GuidanceNote-PPI-LawfulProcessing-202106.pdf*, accessed 8 February 2022. Note also S Papdopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 405.

[1353] Section 38(1) of POPI. Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 109 – 120, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 98 – 99 and 287, and S Papdopoulos 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 at 404. Section 38(2) defines "relevant function" and reads:

> "(2) 'Relevant function' for purposes of subsection (1), means any function –
> *(a)* of a public body; or
> *(b)* conferred on any person in terms of the law, which is performed with the view to protecting members of the public against –
> (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or
> (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity."

involve the statutory functions of public bodies.[1354] The data subject will also not be able to object to the processing of their personal information where the processing is covered by s 38 and is for the "view of protecting members of the public" from "dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of" the relevant authority or person, whether in the financial sector or any other profession, depending on the relevant activity.[1355]

(e) Direct marketing and the rights of data subjects

Briefly, Chapter 8, sections 69 to 71, sets out the "rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making".[1356] Unsolicited direct marketing[1357] is permitted under POPI only when the data subject has consented.[1358] Unsolicited direct marketing is permissible as follows: via electronic communications, which includes automated calling machines,[1359] facsimiles, short

---

[1354] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 342, and 367 – 368.

[1355] Section 38(2)*(b)* of POPI, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 577.

[1356] For more information on this brief discussion see Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 142 – 144, 168 – 170, 186 – 187 and 290 – 304, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 469 – 516, B Hamann & S Papadopoulos 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47(1) *De Jure* 42 – 62, and P Swartz & A Da Veiga 'PoPI Act - opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment' In *2016 Information Security for South Africa* (*ISSA*) (17 – 18 August 2016, Johannesburg, South Africa) 9 – 17. It is worth remembering that based on the definition of "data subject" and "person" in POPI, POPI will also apply to business-to-business marketing – see E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 471. In relation to trade unions, and their supply of goods and services, as well as the direct marketing strategies that they employ when soliciting new members, see J Barnard & MM Botha 'Trade unions as suppliers of goods and services' (2018) 30(2) *South African Mercantile Law Journal* 216 at 235 – 240, and P Swartz & A Da Veiga 'PoPI Act - opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment' In *2016 Information Security for South Africa* (*ISSA*) (17 – 18 August 2016, Johannesburg, South Africa) 9 at 11.

[1357] "Direct marketing" is defined in s 1 of POPI as

> "to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –
>
> *(a)* promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
>
> *(b)* requesting the data subject to make a donation of any kind for any reason"

For an in-depth discussion, see Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 519 – 549.

[1358] B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *South African Law Journal* 122 at 124. Where one member of a "coalition of firms" obtains the consent for all members, and third parties, to process the personal data/information of the data subject, this is often done through the use of cookie consents, for a discussion of possible implications for data subjects and their right to privacy see DW Woods & R Böhme 'The commodification of consent' (2022) 115 *Computers & Security* 102605 1 – 12.

[1359] Section 69(5) of POPI defines "automated calling machine" as "for purposes of subsection (1), means a machine that is able to do automated calls without human intervention".

message service (SMS) and e-mail.[1360] Furthermore, where a directory is available to the public, and it contains personal information, and the data subject has subscribed thereto, the data subject must be informed free of charge before their personal information is added thereto.[1361] Also under this Chapter is a section that deals with automated decision-making. A data subject's personal information shall not be subjected to a fully automated decision-making process where they incur legal and or other substantial consequences,[1362] unless appropriate measures have been put in place to safeguard the data subject's personal information and identity.[1363]

(f) Conclusion

POPI has been designed, together with PAIA, to protect against the unlawful processing of personal information. POPI in particular, through the requirement of safety measures, ensures

---

[1360] Section 69(1) of POPI, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 480. Section 69(1) is a right specifically listed in s 5*(f)*. Section 69(4) states that the direct marketing communication must contain:

> "*(a)* details of the identity of the sender or the person on whose behalf the communication has been sent; and
>
> *(b)* an address or other contact details to which the recipient may send a request that such communications cease."

Section 69(2) of POPI requires that a responsible party may approach a data subject once to obtain their consent, in the prescribed manner and form, to process their personal information. Section 69(2) is to be read with regulation 6 and form 4 of the Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018. Section 69(3) of POPI deals with direct marketing where the data subject is a customer of the responsible party, then the responsible party may send them information regarding their products. Section 69(3)*(c)* is a right specifically listed in s 5*(e)*(ii).

[1361] Section 70(1) of POPI. Section 70(5) of POPI defines "subscriber" as "any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services." This includes informing the data subject of the purpose of the directory and any further uses of the directory, via electronic versions embedded in search functions. See s 70(1)*(a)* and *(b)* of POPI. See s 70(2) where a data subject must, free of charge and without any unnecessary formality, be given the opportunity to object to the use of their personal information. Alternatively, the data subject may request a "verification, confirmation, or withdrawal of" their personal information where there was no prior refusal. Section 70(2) of POPI. Section 70(3) excludes the print editions or off-line directories where these were made available before the commencement of POPI. Personal information may be included in newer versions of directories, after POPI's commencement, where the directories were produced by mobile or fixed telephonic communication companies, whether in print or electronic, and where these companies have obtained the necessary details, in terms of s 70(1) and in fulfilment of a legal duty – see s 70(4) of POPI.

[1362] See s 71(1) of POPI, this includes decisions regarding work performance, credit worthiness, reliability, location, health, personal preferences and conduct.

[1363] Section 71(2)*(a)* and *(b)* of POPI. This exemption may apply where the responsible party needs to meet their duty in terms of a contract with a data subject, and where there are appropriate measures in place to protect or where this is governed by law or a code of conduct, with the aim to protect the data subject's legitimate interests. Section 71(3)*(a)* and *(b)* state that appropriate measures include providing the data subject with the opportunity to make representations, as well as providing the data subject with the "underlying logic of the automated processing" of their personal information in light of the representations. Compare with the UK, see A De Veiga *et al* 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 at 404 – 405. For an in-depth discussion, see Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 417 – 427.

that the processing of personal information is carried out securely, especially with respect to the identity of the data subject. The exceptions, exemptions and exclusions are designed to assist in processing the personal information efficiently and effectively and without undue delay where this will benefit the data subjects. POPI also provides measures to ensure that the work of state departments is not unnecessarily hindered where they are performing their functions or duties towards data subjects.

V SUPERVISION OF POPI

Complaints in respect of the processing of personal information are inevitable. The responsibility of the Information Regulator is to investigate and mediate these complaints, in accordance with the provisions set out in Chapter 5 of POPI.[1364] POPI also provides for an Information Officer. Every public or private organisation, which processes personal information, must have an Information Officer. This is merely a brief overview of the respective roles of the Information Regulator and Information Officer in terms of POPI.

Part A of Chapter 5 of POPI sets out the statutory parameters of the Information Regulator. Section 39 specifically provides for the establishment of the Information Regulator as the overall "watchdog" of POPI. The Information Regulator is tasked with the overall supervision of POPI, throughout South Africa. Section 40 of POPI sets out the general powers, duties and functions of the Information Regulator. For the purposes of this thesis, these will be briefly explained in light of what has been mentioned above.

The Information Regulator is tasked with educating the public with regards to POPI, specifically the conditions for the lawful processing of personal information and good data protection practices, whether this is in relation to a specific group of data subjects or data subjects generally. This also includes giving advice where needed in terms of POPI. The Information Regulator is also required to monitor and ensure compliance with the provisions of the Act in both the private and public sector, especially in relation to the conditions for the lawful processing of personal data. Compliance includes examining proposed legislation, regulations and policies where these may impact on the collection and disclosure of personal

[1364] B Batchelor & T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *South African Law Journal* 122 at 124 – 125 and V Bronstein 'Prioritising command-and-control over collaborative governance: The role of the Information Regulator under the Protection of Personal Information Act' (2022) 25 *Potchefstroom Electronic Law Journal* 1 – 41. See also, Y Burns & A Burger-Smit *Protection of Personal Information: Law and Practice* 2ed (2023) 681 – 708.

information, as well as conducting research and reporting to parliament. The Information Regulator must consult with interested members of the public, and national and international organisations, with regard to the protection of personal data. It must also mediate between opposing parties where the safeguards that protect personal information have been breached. Related to consultation is the need to handle any complaints of violations against the conditions for the lawful of processing of personal information that are received, by investigating, finding possible solutions and serving notices where required. The Information Regulator has also been tasked with the function of researching and reporting to parliament on any international data protection instruments that may be accepted by South Africa, as well as any other necessary legislative amendments. The Information Regulator may also issue codes of conduct, guidelines and adjudicate on good data protection practices. The Information Regulator must assist in cross-border cooperation by enforcing privacy laws where data is transferred. Lastly, the Information Regulator must attend to anything incidental or conducive to its functions, powers and duties. Section 40 provides for the publishing of reports in respect of the duties, powers and functions of the Information Regulator. It is interesting to note that on the commencement of POPI, the Information Regulator took over the supervision of the PAIA from the Human Rights Commission, which confers further listed powers and duties.

Part B of Chapter 5 of POPI sets out the duties and responsibilities of the Information Officer, including the designation and delegation of deputy information officers. The main duties of the Information Officer, once appointed and registered by the responsible party with the Information Regulator, include ensuring and encouraging organisational compliance with POPI, attending to any requests made in terms of POPI, and assisting the Information Regulator with investigations against the responsible party where there is an alleged breach. In line with POPI, de-indexing/de-listing/de-linking requests will first be received by the Information Regulator, hence the need to briefly set out the functions and responsibilities of the Information Regulator, as well as the information officer.

VI JURISDICTION

This may seem a little disjointed, placed here, but the discussion on jurisdiction is important to note, first, in light of the Court of Justice of the European Union's (CJEU) decisions in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* [1365] and *Google LLC v CNIL*;[1366]

[1365] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1366] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.

second, the possible implication that the definitions of "responsible party" and "operator" may have on those processing of personal data in light of the jurisdictional reach of POPI[1367] and, third, it will be useful to summarise the South African position for the discussion in the next chapter.

POPI applies to all responsible parties that process personal data, irrespective of whether they are natural or juristic persons. However, as noted above, there are a few exceptions, for example, POPI will not apply when the personal information is processed for purely personal or household reasons.[1368] Regarding juristic persons, POPI applies to all public and private organisations. In other words, POPI applies to any organisation that processes personal information, including local or foreign companies.[1369] In this chapter, the discussion will be limited to what is necessary for the right to be forgotten. It is important to be aware of the fact that there is a presumption in South African law that South African statutes do not apply extraterritorially.[1370] However, with regards to the possible jurisdictional reach that POPI has, the above-quoted definition of "responsible party" is important to note.[1371] Furthermore,

---

[1367] These definitions were set out in the discussion on definitions above.

[1368] See s 3 provides for the "application and interpretation" of POPI; s 6 provides a list of general exclusions and s 7 provides the "exclusion for journalistic, literary or artistic purposes" in terms of POPI.

[1369] See sections 1, 14 and 23 of the Companies Act 71 of 2008. Foreign companies are termed "external companies" in the Companies Act 71 of 2008. For extra commentary on sections 14 and 23 (which set out the registration of local and external companies, respectively), see P Delport *Henochsberg on the Companies Act 71 of 2008* (November 2021 – Service Issue 27) at 66(1)ffg, and 118(5)ffg, respectively. Also, POPI will apply to those companies that must pay tax in terms of the Income Tax Act 58 of 1962. See also s 1, specifically the definition for "resident" in the Income Tax Act 58 of 1962, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 86. Note: In the United States (US) Google, where its headquarters or offices are, is registered as an "LLC". The "LLC" stands for "limited liability company" and refers to a company:

> "established by statutory law to provide the legal market with a flexible type of legal entity. It combines both the advantage of limited liability of a corporation and the tax status of a partnership, i.e. the avoidance of double corporate income tax.
>
> The formation procedure . . . requires a written LLC agreement and a certificate of formation duly filed with the respective state authorities. However . . . an LLC can only have a limited term. Furthermore, a member of an LLC may transfer its interest in an LLC to a third party without the prior consent of the other members but may not transfer its voting rights without their consent. As in a general partnership, the management of an LLC consists of its members who represent the company vis-à-vis third parties." (footnotes omitted)

G Pfeiffer and S Timmerbeil, 'US-American company law – An overview' (2008) 6 *Zeitschrift für das Juristische Studium* 597 at 598. In South Africa, Google LLC is registered as Google South Africa (registration no. 2006/035611/07), and they are situated in Johannesburg, see BizPortal – Brought to you by the CIPC, available at *https://bizportal.gov.za/bizprofile.aspx* (Accessed 21 April 2022).

[1370] See *Competition Commission v Bank of America Merrill Lynch International Ltd & others* 2020 (4) SA 105 (CAC) paras 36 – 44, *Director of Public Prosecutions, Western Cape v Kouwenhoven* 2021 (1) SACR 579 (WCC) para 40, M Van Staden 'A comparative analysis of common-law presumptions of statutory interpretation' (2015) 26(3) *Stellenbosch Law Review* 550 at 564 - 567, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87, and S Calzati '"Data sovereignty" or "data colonialism"? Exploring the Chinese involvement in Africa's ICTs: A document review on Kenya' (2022) 40(2) *Journal of Contemporary African Studies* 270 at 280.

[1371] For ease of reference: s 1 of POPI: "'responsible party' means a public or private body or any other person

in terms of s 3(1)*(b)* POPI will apply to a responsible party irrespective of whether they are domiciled or not domiciled in South Africa.[1372] The definition may be explained as follows: first, if the "responsible party" processes the information itself, it clearly falls within the jurisdiction of POPI. Second, if an operator rather than the responsible party processes the information, the responsible party will still fall into the jurisdiction of POPI. Third, the reason why the responsible party still falls into the definition of POPI even when it does not process the information, is because the responsible party is responsible (or answerable) for determining the purpose for which the information is going to be processed.[1373] Therefore, based on the definition of "responsible party", POPI, like other data protection laws,[1374] may in certain instances have extraterritorial application.[1375]

To clarify the above, first, if the responsible party or the operator are physically located in South Africa, POPI applies to them irrespective of where the information is collected and processed.[1376] Second, if the responsible party is not physically located in South Africa, but the operator is, POPI applies to both the responsible party and the operator. Third, if the responsible party and the operator are both outside South Africa, but the information is collected and processed using servers in South Africa (if this is possible), POPI applies to both the responsible party and the operator. POPI applies to them irrespective of where the information is collected and processed. However, where both the responsible party and operator are situated outside of South Africa, and the personal data is merely being transported through servers, based in South Africa, then POPI does not apply. POPI will also not apply where the

---

which, alone or in conjunction with others, determines the purpose of and means for processing personal information." TV Warikandwa 'Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared' (2021) 24 *Potchefstroom Electronic Law Journal* 1 at 18.

[1372] Although, s 3(1)*(b)* of POPI is quoted above, for ease of reference:

> "(1) This Act applies to the processing of personal information—
>
> *(a)* . . .
>
> *(b)* where the responsible party is—
>
> (i) domiciled in the Republic; or
>
> (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic."

[1373] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 86 – 87.

[1374] Note Article 3 of Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation or GDPR).

[1375] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87. Unlike Article 3 of Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (or the General Data Protection Regulation or GDPR) which states that where personal data of a European Union citizen is being processed, irrespective of where the citizen is or if the processing takes place outside of the European Union, then the GDPR will apply.

[1376] Storing personal information is a part of the definition of "processing", see above, or s 1 of POPI.

information is merely extracted from the internet, and the responsible party is situated outside South Africa and processes the personal information outside of South Africa.[1377]

The following discussion defines what the possible right to be forgotten could look like in South Africa, with references to both POPI and international as well as national case law.

VII THE RIGHT TO BE FORGOTTEN AND POPI

(a) Introduction

This discussion will focus on the right to be forgotten and how it is defined within the South African context. It is useful to understand where the right to be forgotten fits within the overall scheme of POPI. POPI confers rights on the data subject and imposes obligations on the responsible party. The main focus of the rights conferred on the data subject is to have their data processed in line with the conditions for lawful processing of personal information. While these conditions confer rights on the data subject, they impose obligations on the responsible party. The rights that are important to note for the discussion that follows are:

- The data subject has the right to object to the processing of their information, based on reasonable grounds. The objection will generally relate to the data subject's situation.[1378]
- The data subject has the right to object, at any time, to the processing of their personal information for the purposes of direct marketing.[1379]
- The data subject has the right to have their personal information corrected, destroyed or deleted, depending on the circumstances.[1380]

In addition, there is also the possibility of de-identifying the personal data in terms of s 14. De-identifying, in terms of POPI, requires that the data be deleted. The right to be forgotten, in terms of the *Google Spain*,[1381] merely requires that the personal information be de-linked or de-indexed from the data subject's name. The result is that where the data subject's name is used as the search term in a search engine tool, the unwanted personal information will not

[1377] See generally, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87 – 88. See regarding the extraterritorial reach of the GDPR: OJ Gstrein & AJ Zwitter 'Extraterritorial application of the GDPR: promoting European values or power?' (2021) 10(3) *Internet Policy Review* 1 at 8 – 11, and European Data Protection Board *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* ver. 2.1 adopted 12 November 2019.
[1378] Section 11(3)*(a)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576 – 578.
[1379] Sections 11(3)*(b)* and 69(3)*(c)* of POPI.
[1380] Section 24 of POPI.
[1381] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88.

appear on the results page. Important to note is that the information is not deleted, it is merely more difficult to find as search terms other than the data subject's name must be used to locate same. However, the possibility of de-identifying or deleting personal information is still important to keep in mind, as will be set out later. A discussion of the relevant sections follows.[1382] With respect to the right to be forgotten, sections 11 and 24 of POPI are important to note, specifically s 11(3), s 24(1) as well as s 14(4).

The structure of this part of the thesis will be as follows: the next section will deal with a more general discussion of POPI, privacy, expression and forgetting as a background to the rest of the discussion. Thereafter sections 11 and 24 will be discussed. In light of this discussion, the scope and content of a South African right to be forgotten will be proposed.

(b) POPI, privacy, expression, and forgetting

Whenever legislation is applied, the constitutional rights of all concerned must be considered in the balance – this includes POPI, although the thrust of POPI is aimed at protecting the constitutional right to privacy in relation to personal information.[1383] Hence, the considerations regarding freedom of expression and other constitutional rights do not lose their importance.[1384] POPI itself does remind us that the constitutional imperatives of "democracy and openness" must be kept in mind.[1385] Furthermore, POPI also promotes the free flow of information in accordance with national and international legal principles, within the information society framework. Despite this POPI still does impact on freedom of expression – this is evident in the fact that personal information that has been made available on public platforms may be deleted or destroyed and, in some instances, altered. Hence, the need for a possible middle ground in the form of the right to be forgotten, where the information is de-indexed/de-linked/de-referenced for the data subject's name, but the information itself is left intact and is still accessible – albeit more difficult to find – to the general public. The Article 29 Data Protection Working Party (Article 29 WP)[1386] noted that through the use of a search engine,

[1382] Section 14 of POPI, as far as it is relevant to obtain a solution to deal with the unlawful processing of personal information, will feature in this discussion.
[1383] J Ballaschk 'In the unseen realm: Transnational intelligence sharing in the European Union - Challenges to fundamental rights and democratic legitimacy' (2015) 51 *Stanford Journal of International Law* 19 at 22.
[1384] Section 8(1) of the Constitution.
[1385] Preamble of POPI.
[1386] As stated on the Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 on the covering page:

> "This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC."

internet users are able to locate and access the personal information of data subjects with relative ease. The balancing of the relevant rights and interests will need to be kept in mind, specifically the "nature and sensitivity of the processed data and the interest of the public in having access to that particular information. The interest of the public will be significantly greater if the data subject plays a role in public life."[1387] The essence of what the right to be forgotten entails is set out in Chapter 2 as well as a short description is provided below.

The "constitutional tightrope" to find a balance between the rights of privacy and freedom of expression is certainly not easy – individuals have a right to know (or more formerly a "right to impart and receive information") and the data subject has the right to protect their personal information. POPI provides a solution in its conditions for the lawful processing of personal information – most of which have been briefly set out above. Journalists (where there is a code of conduct), artists and writers or academics do enjoy some protection under POPI through the exclusions listed in s 7. The s 7 exclusions (which are discussed earlier in the chapter) assist in promoting the essence of freedom of expression as detailed in s 16 of the Constitution.

It is interesting to note, and like many countries around the world,[1388] a form of forgetting has been a part of South Africa's legal fabric for a very long time. The Criminal Procedure Act[1389] provides for the expungement of criminal records, whether automatically or by application. The important feature to note is that not all crimes will be expunged, serious crimes, especially sexual offences, such as rape, will remain a part of the former accused's criminal record.[1390]

Lastly for this brief discussion, as a part of its duties, the Information Regulator may exempt a responsible party from the conditions for lawful processing, where this is in the public's interest.[1391] The considerations the Information Regulator must take into account

---

[1387] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2, see also at 5 – 6, 7, and 12. The Article 29 Data Protection Working Party at 13 of the guidelines implementing *Google Spain* tried to define what is meant by where a data subject is considered to play "a role in public life", with the following examples: "politicians, senior public officials, business-people and members of the (regulated) professions can usually be considered to fulfil a role in public life. There is an argument in favour of the public being able to search for information relevant to their public roles and activities."

[1388] See the introduction in Chapter 2.

[1389] Criminal Procedure Act 51 of 1977.

[1390] See generally sections 271A – 271E of the Criminal Procedure Act 51 of 1977, the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, and the Expungement of Criminal Records GN 513 in *Government Gazette* 32205 of 6 May 2009

[1391] Section 37(1)*(a)* of POPI.

before granting such an exemption are set out in s 37(2), which provides, inter alia, that "the special importance of the interest in freedom of expression" must be taken into account.[1392] It is submitted that even in the general course of applying – in terms of s 24 – for the correction, deletion or destruction of information, the right to freedom of expression must be considered. Section 24 is discussed later in this part of the chapter in light of the right to be forgotten. The discussion will also refer to the rights and the application thereof more fully, and why the right to be forgotten may be a good solution in instances where personal information is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully".[1393]

(c) Section 11

(i) Justifying the processing of personal information

Section 11 of POPI requires that the processing of personal information must be lawful, ie "the processing of each piece of personal information must be justified".[1394] There needs to be a connection between the purpose and reason for the processing of personal information. Section 11 also provides a right to object to the processing of personal information in certain instances.[1395] Consent is only one of the six grounds that may be used as a justification to process personal information. The other grounds are: the processing must be necessary for the

---

[1392] Section 37(2)*(f)* of POPI.

[1393] Section 24(1) of POPI.

[1394] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 189.

[1395] Sections 11(1)*(a)* and 2*(a)* and *(b)* of POPI. The two subsections read:

> "11 Consent, justification and objection. – (1) Personal information may only be processed if –
> *(a)* the data subject or a competent person where the data subject is a child consents to the processing;
> *(b)* processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
> *(c)* processing complies with an obligation imposed by law on the responsible party;
> *(d)* processing protects a legitimate interest of the data subject;
> *(e)* processing is necessary for the proper performance of a public law duty by a public body; or
> *(f)* processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
> (2) *(a)* The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)*(a)*.
> *(b)* The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)*(a)*, at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)*(b)* to *(f)* will not be affected.
> (3) 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; or
> *(b)* for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.
> (4) If a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information."

conclusion or performance of a contract, which must be signed by the data subject;[1396] the processing must comply with an obligation in terms of the law;[1397] the processing will protect a legitimate interest of the data subject;[1398] and the processing is in terms of a public law duty by a public body.[1399] Processing may also be necessary for the protection of the legitimate interests of the responsible party, as well as a third party who has been supplied with the data subject's personal information.[1400]

As outlined before, consent[1401] is only one of the grounds for the lawful processing of personal information. Due to its specific definition, it is also the trickiest ground to use as a justification to lawfully process personal information. This discussion follows.

(ii) The issue of consent

The discussion on consent is important to note, in light of the right to be forgotten, although the right to be forgotten will not necessarily be used in instances where consent is the ground for the processing of personal information, it is still important to keep in mind, due to the specific definition that it conveys. The reason for dealing with consent in some detail is due to the misconceptions that surrounds it. One such misconception is that data subjects are under the impression that personal information may only be processed where they have provided their consent.[1402] However, using POPI as a good example, there are six justifications that provide for the lawful processing of personal information, consent is only one of them.[1403] The other misconception is a "myth" that surrounds "consent", and this relates to "blanket consent" where responsible parties are often under the impression that once consent is granted to process the data subject's personal information for a specific purpose, that consent will apply to a new purpose, in other words, they have carte blanche to process the personal information as and how they please.[1404] This is not true, as a brief discussion on the elements of consent will show.

[1396] Section 11(1)*(b)* of POPI.
[1397] Section 11(1)*(c)* of POPI.
[1398] Section 11(1)*(d)* of POPI.
[1399] Section 11(1)*(e)* of POPI.
[1400] Section 11(1)*(f)* of POPI.
[1401] Section 11(1)*(a)* of POPI.
[1402] BJ Koops 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250 at 251.
[1403] Section 11(1) of POPI, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 189 – 199. There are countries in which consent is the primary justification for the processing of personal information, ie France, Greece, Portugal and Italy, or one of two primary requirements, ie Germany and Austria, all other justifications amount to an exception to consent. See SALRC (Project 124) *Report on Privacy and Data Protection* (2009) para 4.2.58.
[1404] See PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 at 4 for an example of "blanket consent". The author details where the consent given is merely the click of an "OK" button, data subjects are often unaware that the companies treat this consent as a form of "blanket consent" and their personal

De Stadler *et al* lament the fact that responsible parties tend to use consent as their "go-to" justification when processing personal information. Consent should be the last resort to justify the processing of personal information, and consent should be used only if no other justification is present.[1405] Thus, consent is a challenging concept, especially when drafted into legislative instruments concerning the right to privacy.[1406] In foreign jurisdictions phrases such as "unambiguous" or "manifest, free and enlightened"[1407] have been paired with the requirement of consent, and in many instances, it may be the only or only one of two conditions for the processing of personal information.[1408]

In POPI, the definition of consent provides that it is a "voluntary, specific, and informed expression of will". These elements are important when evaluating whether there was true consent or not, and are discussed briefly, as follows:

1. "Voluntary": The data subject must be able to elect, ie they must have a "genuine choice", to have their personal information processed.[1409] The choice must not be linked

information is being processed or being shared with third parties outside of what they consented to. DW Woods & R Böhme 'The commodification of consent' (2022) 115 *Computers & Security* 102605 1 – 12 contains a similar discussion where one member of a "coalition of firms" obtains the consent for all members, and third parties, to process the personal data/information of the data subject. The consent is obtained through the use of this is often cookie consents. The authors describe this as the "legal fiction of consent" which "functions to establish a legal right to collect, store, process, and share personal data".

[1405] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 190.

[1406] SALRC (Project 124) *Report on Privacy and Data Protection* (2009) para 4.2.54, and JC Buiterlaar 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 at 177.

[1407] See Article 2*(h)* of Directive 95/46 and Article 4(11) of the GDPR as examples.

[1408] The second condition being processing in terms of a legal obligation. SALRC (Project 124) *Report on Privacy and Data Protection* (2009) paras 4.2.54 – 4.2.66; see Article 7 of Directive 95/46, and s 14 of the Quebec Act Respecting the Protection of Personal Information in the Private Sector, 1993. The SALRC initially seemed to have decided that although important for the processing of personal information – consent is one condition for the lawful processing of personal data (para 4.2.93). In other words, the initial idea was that the legislation would not be "consent-driven". However, in practice the need to obtain consent is vital – most of the conditions for the lawful processing of personal information requires that the data subject's consent is obtained before the personal information is processed – consent runs as a thread through these conditions, although it is only one of the requirements for lawful processing (see sections 11(1)*(a)* (generally for the processing of personal information), 12(2)*(b)* (where collection of personal information is from a third party), 14(1)*(d)* (when records are retained), 14(7) (when stored information is processed), 15(3)*(a)* (where there is a need to further process the personal information), and 18(1)*(a)* where the data subject provides a waiver for the notification stating that their personal information is being processed) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 69.) Note that even in the special conditions (s 27(1)*(a)* of POPI, E De Stadler *et al* at 69) as well in terms of direct marketing (s 69(1)*(a)* of POPI, E De Stadler *et al* at 69), where there is cross-border transfer of the personal information to foreign legal jurisdictions (s 72(1)*(b)* of POPI, E De Stadler *et al* at 69), and when account numbers are disclosed to third partiesp[658[(s 106(1) of POPI, E De Stadler *et al* at 69). Unlike those countries where consent is either the only requirement (SALRC (Project 124) *Report* para 4.2.58: listed the following countries: France, Greece, Portugal and Italy), or one of two requirements (SALRC (Project 124) *Report* para 4.2.58: the countries listed are Germany and Austria, the other criteria for lawful processing is that the processing of the personal data is in terms of a legal obligation), POPI still places a greater emphasis on the requirement of consent, than what was possibly the initial aim of the SALRC.

[1409] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act:*

to any terms and conditions or threat to be shut out of the activity (such as a purchase from an online store). In other words, the data subject must have "the freedom to withhold consent, but still accept the terms and conditions."[1410] Bound to this is the ability to withdraw their consent at any time and "without undue effort" and unfavourable consequences.[1411] There are instances where the idea of voluntary consent is flawed; this is the case where, for example, personal data is processed prior to the formation of a contract, or it is processed in terms of an obligation in terms of the law.[1412]

2. "Specific": The consent must relate to a detailed purpose. A blanket consent will be considered vague and thus invalid. Consent in this instance is "granular", that is consent is required per specified activity, even if the data is collected only on one occasion.[1413]

3. "Informed": This generally means that the data subject has been appraised of the complete circumstances, which includes the consequences of granting or withholding their consent. POPI does not specify, but De Stadler *et al* argue that being informed includes "the use of plain language", with which I agree. If the reason for the collection of the personal information, how it will be used and who will all have access to it, are not set out in a way that the data subject will understand, then the responsible party cannot claim that the data subject has consented to the processing of their personal information.[1414]

The last POPIA book you will ever need (2021) at 66.

[1410] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 66 and 216.

[1411] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 67.

[1412] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 67, 190 – 193, and 333 – 335.

[1413] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 67, and 190, and W Rosenberg 'The mother's right to privacy in infant abandonment cases' (2022) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 92 at 103 – 104.

[1414] MN Njotini 'Preserving the integrity of medical-related information – How "informed" is consent?' (2018) 21 *Potchefstroom Electronic Law Journal* 1 – 20 and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 68: where the authors also argue that "[t]he most important aspect of plain language is that responsible parties must take the target audience (also referred to as the market segment) into account. For instance, if the audience has lower levels of literacy, responsible parties must use simpler language." See also s 22 of the Consumer Protection Act 68 of 2008, which provides consumers with a right to be informed in plain and understandable language, specifically at s 22(2) provides that:

> "a notice, document or visual representation is in plain language if it is reasonable to conclude that an ordinary consumer of the class of persons for whom the notice, document or visual representation is intended, with average literacy skills and minimal experience as a consumer of the relevant goods or services, could be expected to understand the content, significance and import of the notice, document

4. "Expression of will": This element requires clear, positive action by the data subject to express their permission for the processing of their personal information for example a signature.[1415] It cannot be inferred by default or silence. The expression must also be "distinct from other actions such as agreeing to the terms and conditions".[1416]

As stated earlier, it should be as simple to withdraw consent to processing personal information as it is to grant consent.[1417] The reason is that consent is voluntary, depending on the context. However, any processing activities that occurred before the consent was withdrawn remain lawful, and the responsible party must, in terms of the law, keep a record of such processing.[1418]

Section 11(2) of POPI, read with s 11(1)*(a)*, requires that the responsible party bears the burden of proving that they have consent to process the personal information, noting that the consent may be withdrawn at any time. When consent is revoked, the processing before the revocation remains lawful, and need not be deleted where retention of the record is required as per the law. On revocation of consent, the reposnsible party must stop processing the personal information, and may not rely on another justification merely to continue with processing the information.[1419]

(iii) Objecting to the processing of personal information

Important to note is that revoking consent and objecting to the processing of personal information will have different consequences. The data subject may only object to the processing of their personal information in specific instances. The data subject may object to the processing of their personal data at any time in the prescribed form. The responsible party must provide the relevant assistance to the data subject, when necessary, and the objection must

---

or visual representation without undue effort".
See also E De Stadler and L van Zyl 'Plain language contracts: Challenges and opportunities' (2017) 1 *South African Medical Law Journal* 95 at 101, where the authors have opined that contracts that are extremely detailed and not written in ordinary language may lead to consumers experiencing information overload amounting to "a lack of transparency".

[1415] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 334 and D Thalder & B Shozi 'Is open-identity gamete donation lawful in South Africa?' (2022) 112(6) *South African Medical Journal* 409 at 411 – 412.

[1416] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 69.

[1417] Section 11(2) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 574.

[1418] See sections 11(2) and 14(1) of POPI.

[1419] Section 2*(a)* and *(b)* of POPI. A written consent signed by the data subject may be of assistance in this regard, but the consent must add that the data subject may withdraw their consent at any time and that the withdrawing must be as easy as it was to give. See E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 574 – 575.

be without charge.[1420] The objection thereof is provided in s 11(3) of POPI, which reads as follows:

> "(3) 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; or
>
> *(b)* for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69."

Put differently, in terms of s 11(3) the data subject may object to the processing of their personal information where the responsible party processes the personal information: (1) to protect the legitimate interests of the data subject;[1421] (2) where the responsible party is a public body processing the personal information in terms of a public law duty;[1422] (3) where the processing only protects a legitimate interest of the responsible party, alternatively a third party;[1423] and (4) where the personal data is processed in terms of s 69, which relates to processing in terms of direct marketing.[1424]

The legislature did not define "reasonable grounds" in POPI. The necessity of providing "reasons" for administrative decisions has been discussed within the framework of PAJA. Although not directly dealing with "reasonable grounds", the following paraphrased extract is useful to note, detailing adequate reasons and may provide a useful guide where a data subject wants to object to the continued processing[1425] of their personal information, in light of the

---

[1420] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576 – 578.
[1421] Section 11(1)*(d)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576.
[1422] Section 11(1)*(e)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576.
[1423] Section 11(1)*(f)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576.
[1424] There are further sections in POPI which provide that the data subject may object to the processing of their personal data, see sections 28, 32*(b)*(i), 70(2), and 87.
[1425] Note, in this thesis "continued processing" is not the same as "further processing". "Further processing" carries a specific connotation in terms of POPI – see the discussion of s 15, which outlines the requirements for "further processing of personal data". "Continued processing" in this thesis is possibly best explained as follows: A data subject opens an account with a bank. The bank will, either in the form of consent or in terms of a contract, process the data subject's personal information in line with the opening of that account. The data subject transacts through that account, whether via an app or an ATM or in form of a payment in a shop, and the bank connects all these transactions to the original account that was opened by the data subject, this will most likely, it is submitted, be a continuation of the original (consented/contracted) processing of the personal data, as each separate transaction must be linked to that specific account.

factual context:[1426]

> "Depending on the circumstances, the reasons need not always be 'full written reasons'; the 'briefest pro forma reasons may suffice'. Whether brief or lengthy, reasons must, if they are read in their factual context, be intelligible and informative. They must be informative in the sense that they convey why the . . . [objection] . . . is justified. Reasons must, however, not be intelligible and informative with the benefit of hindsight. They must from the outset be intelligible and informative to the reasonable reader thereof who has knowledge of the context of the [processing]. If the reasons refer to an extraneous source, that extraneous source must be identifiable to the reasonable reader."

Hence, the "reasonable grounds" required for an objection, based on the data subject's own personal circumstance, must be set out in sufficient detail to justify the objection.

The Regulations[1427] relating to POPI set out the prescribed form which the data subject must complete where they are objecting to the processing of their personal information. In terms of the Regulations, the responsible party must provide reasonable assistance to the data subject, free of charge, when filling in the form.[1428] The reasons for the objection, as with the withdrawal of consent, must be based on the data subject's own circumstances. The responsible party must stop processing the data subject's personal information once they have received the objection and it is determined to be reasonable.[1429] However, where the continued processing of the data subject's personal information is required by legislation or a court order, the responsible party may refuse to accede to the objection.

Note, as discussed above, in terms of s 38(1), the responsible party may refuse to accept an objection by the data subject, where the responsible party is processing personal data in

---

[1426] *Commissioner, South African Police Service & others v Maimela & another* 2003 (5) SA 480 (T) at 480C-E (ie the headnote) and 485G – 486G. The headnote has been quoted with approval by the Constitutional Court in *Koyabe & others v Minister for Home Affairs and others (Lawyers for human rights as amicus curiae)* 2010 (4) SA 327 (CC) para 64, *Gavric v Refugee Status Determination Officer & others* 2019 (1) SA 21 (CC) para 68, and *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 34.

[1427] Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018.

[1428] Regulation 2 of the Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018 reads:

> "Objection to the processing of personal information. — (1) A data subject who wishes to object to the processing of personal information in terms of section 11(3)*(a)* of the Act, must submit the objection to the responsible party on Form 1.
>
> (2) The responsible party, or a designated person, must render such reasonable assistance as is necessary, free of charge, to enable the data subject to make an objection on Form 1."

See also form 1 of the Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018.

[1429] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 576.

order to discharge a "relevant function".[1430] "Relevant function" in terms of s 38(2), refers to those functions that are carried out by a public body or are "conferred on any person in terms of the law". These functions are performed to protect the general public from unscrupulous behaviour or conduct in the financial and banking sectors, or in "the management of bodies corporate"; or from deceitful, abusive, wrongful or inept behaviour by professional individuals.[1431] The data subject is also able to withdraw their consent in terms of direct marketing.[1432]

One of the first cases dealing with s 11 of POPI, namely, *Divine Inspiration Trading 205 (Pty) Ltd v Gordon,*[1433] unfortunately, did not discuss "reasonable grounds", nor did it deal with the right to be forgotten. However, it does provide some guidance with regard to the application of s 11 of POPI.

(iv) Divine Inspiration Trading 205 (Pty) Ltd v Gordon

(aa) Facts and contentions

The issue before Hockey AJ was whether POPI would apply in justifying the non-production of documents, specifically medical records, where a subpoena *duces tecum* is served. Uniform rule 38 requires that the receiver of a subpoena *duces tecum* must hand over certain documents to the registrar of the court in respect of pending court proceedings. The possessor of the documents may be called as a witness in the pending court proceedings. The receiver of the subpoena may claim legal privilege as a defence for not producing the documents.[1434]

In *Divine Inspiration*, the documents requested were medical records. The applicants, Divine Inspiration Trading 205 (Pty) Ltd (Divine Inspiration) and The Alphen Farm Estate (Pty) Ltd (Alphen Farm), requested the records in terms of a damages claim that was launched against them by the first respondent, Ms Katherine Gordon (Ms Gordon). Ms Gordon had sustained injuries in an accident whilst on the applicants' premises during October 2015.[1435] Ms Gordon was treated by the second and third respondents who are both medical practitioners,

[1430] See in this chapter the discussion under the heading "(d) Exemptions/exclusions/exceptions".
[1431] Section 38(2) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 577.
[1432] Sections 69 – 71 of POPI.
[1433] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 30ffg.
[1434] Rule 38 of the Uniform Rules of Court; *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 17. See also *Trust Sentrum (Kaapstad) (Edms) Bpk and another v Zevenberg and another* 1989 (1) SA 145 (C) and D Harms *Civil Procedure in the Superior Courts* (August 2023 – Service Issue 77) para B38.4.
[1435] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 2.

namely, a general practitioner, Dr Katherine Lewis, and a psychiatrist, Dr Giselle Rausch, respectively. The two medical practitioners may not, in terms of the National Health Act 61 of 2003, disclose the medical records of Ms Gordon, unless there is "a court order or any law that requires that disclosure".[1436] Ms Gordon opposed the subpoena *duces tecum* on a number of grounds, but only those relevant to POPI will be discussed.[1437]

(bb) The court's findings and conclusions

Ms Gordon's ground of opposition in terms of POPI was based on s 11(3), where she contended that she may object where her personal information is being processed in terms of s 11(1)*(c)* and *(f)*.[1438] Hockey AJ dismissed Ms Gordon's opposition in terms of s 11(1)*(c)* of POPI, but upheld her contention in terms of s 11(1)*(f)*, Hockey AJ explained that a data subject's right to object to the processing of personal information in terms of s 11(3) applies only where the personal information is processed in terms of s 11(1)*(d)* to *(f)*, in this instance s 11(1)*(f)*. Hence, the objection does not apply to personal information that is processed in terms of s 11(1)*(c)*. Hockey AJ dismissed the opposition based on POPI, based on the following (somewhat cryptically discussed) reasons:

In terms of s 11(1)*(c)*, personal information may be processed where a responsible party must comply "with an obligation imposed by law". Hockey AJ held that the medical practitioners were responsible parties as they were private bodies that determined "the purpose of and means for" the processing of the medical records, ie the personal information of Ms Gordon. Therefore, in light of s 11(1)*(c)* the medical practitioners were required to adhere to the subpoena *duces tecum* (ie an obligation in terms of law) and submit the documents to the registrar. [1439]

Hockey AJ acknowledged that Ms Gordon's opposition in terms of s 11(1)*(f)* of POPI was successful. Section 11(1)*(f)* POPI provides for the processing of personal information where this is in line with the legitimate interests of the responsible party or a third party, to whom the information may be supplied. In *Divine Inspiration* the medical practitioners, as

[1436] Section 14(2)*(b)* of the National Health Act 61 of 2003.
[1437] POPI was not the only issue, reliance against handing over the medical records was also placed on s 14 of the National Health Act 61 of 2003, the Health Professions Act 56 of 1974 and the Ethical Rules of Conduct for Professionals, and the privacy of the first respondent (plaintiff in the main), amongst others.
[1438] Section 11(1)*(c)* requires that personal information be processed by the responsible party must be in terms of a legal obligation. Section 11(1)*(f)* provides for the processing of personal information where this is in the interests of the responsible party or on behalf of a third person.
[1439] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) paras 30 – 37. See SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.6.25.

responsible parties, were required to supply the personal information to the applicants. Hockey AJ didn't elaborate on what the legitimate interest of the applicants were, but one can assume, in terms of the facts, that they needed the information as a part of their defence in terms of Ms Gordon's damages claim in the main action. Although, in terms of s 11(3) Ms Gordon does have a right to object to the provision of her medical records (her personal information), by the medical practitioners (as responsible parties) to the applicants. However, Hockey AJ held that the argument ultimately failed due to the obligation placed on the medical practitioners to supply the medical records in terms of the subpoena *duces tecum*, which is a legal obligation, as provided in s 11(1)*(c)*, and the medical records had to be handed to the registrar of the court, pending the main court proceedings.[1440]

However, in the concluding remarks and findings, Hockey AJ still added a further ground to dismiss the opposition based on POPI to the subpoena *duces tecum*, namely s 12(2)*(d)*(iii) allows for the collection of personal information from an alternative source, and not directly from the data subject where this is "for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated".[1441] Furthermore, POPI also allows for the further processing of personal data, and in terms of s 15(3)*(c)*(iii) where the "further processing is necessary" in aide of "the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated".[1442]

Hockey AJ concluded that the drafters of POPI did not intend for it to be in conflict with the procedural rules and regulations of courts and tribunals, where personal information is being processed in terms of the rules relating to discovery procedures or where it is collected as evidence in terms of a subpoena. Hence the procurement of evidence with the use of a subpoena *duces tecum* is compatible with the conditions relating to the lawful processing of personal information.[1443] Therefore, Ms Gordon's objection to the subpoena *duces tecum* based on POPI failed.

Interestingly, *Divine Inspiration* is silent regarding the requirements for the processing of special personal information, which includes health records.[1444]

[1440] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 37.
[1441] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 38, also s 12(2)*(d)*(iii) of POPI.
[1442] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) para 38.
[1443] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC) paras 38 – 39. Compare with *M & another v M & another* [2022] ZAGPJHC 1025 para 17.
[1444] Section 31, read with s 26 of POPI.

(d) Section 24

Section 24 provides for the correction of personal information, but also for the deletion[1445] thereof as one of the rights of the data subject. Briefly, it provides that personal information may not be retained for longer than is reasonably needed, or as provided for in terms of any law, and access thereto may be restricted. This right ties in with the requirement of information quality (ie s 16), the principle of minimality (ie s 10),[1446] and also that information should not be retained longer than is necessary (s 14(1)). The relevant part of s 24 reads[1447]

> "(1) 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
>
> *(b)* destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14."

Section 24(2) provides that the responsible party must take reasonably practical steps to attend to the data subject's request, and where this is not possible, and with the agreement of the data subject, a notification must be attached to the personal information stating that an amendment was requested, which "has not been made". Furthermore, where steps have been taken in terms

---

[1445] The legislature uses the words "destroy or delete" – perhaps this is for emphasis, but it is not apparent from POPI.

[1446] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 570.

[1447] The rest of s 24 is as follows:

> "Correction of personal information. — (1) . . .
> (2) On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable—
> *(a)* correct the information;
> *(b)* destroy or delete the information;
> *(c)* provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or
> *(d)* where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
> (3) If the responsible party has taken steps under subsection (2) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.
> (4) The responsible party must notify a data subject, who has made a request in terms of subsection (1), of the action taken as a result of the request."

Section 24 of POPI must also be read with regulation 3 and Form 2 of the Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018. See generally E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 570 – 574.

of s 24(2), then the responsible party needs to notify, where reasonably practicable, and where these changes have an effect on decisions regarding the data subject, other responsible parties, third parties, etc., as to which steps had been taken.[1448] The process for the deletion or correction of information as outlined in s 24 of POPI is reliant on the data subject providing some form of identification (eg an identity document (ID) or driving licence or birth certificate, etc.) to confirm that the personal information is theirs in order for it to be deleted or altered.[1449] Once again, the legislature stipulates that the responsible party must keep the data subject informed of the outcomes of the request to correct or delete their information.[1450]

When making any of these requests (namely correction or deletion), the data subject will be required to "provide documentary evidence in support of their request", which should be attached to the relevant form with or without an affidavit (depending on the circumstances).[1451] The data subject will need to specify whether they are seeking a correction or deletion of their personal information. The responsible party, where they refuse the request to correct or delete must also provide "credible evidence" in support thereof.[1452] Where the data subject is contesting the accuracy of their information, the responsible party must restrict the processing thereof until accuracy has been verified, alternatively, corrected.[1453]

(e) Defining the right to be forgotten in South Africa

(i) Introductory remarks

Before starting to define a possible "South African right to be forgotten", it will be useful to keep the following in mind as a background to the discussion, namely that search engines are considered to be "responsible parties", and that the right to be forgotten is an internet based right.[1454] A search engine processes personal information that is published by third parties, for

[1448] Section 24(3) of POPI.
[1449] Section 24 must be read with s 23(1) of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 547 – 549.
[1450] Section 24(4) of POPI.
[1451] Regulation 3 and Form 2 of the Regulations relating to the Protection of Personal Information Act, GN R 1383, *GG* 42110 of 14 December 2018.
[1452] Section 24(2)*(c)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 571 and 574.The data subject has a right to make representations in instances where an automated decision has legal consequences, these representations need to be carefully considered by the responsible party – see De Stadler *et al* at 572 – 573.
[1453] Section 14(6)*(a)* of POPI. E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 572.
[1454] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014. See also J Kerr 'What is a search engine? The simple question the Court of Justice of the European Union (CJEU) forgot to ask and what it means for the future

example, articles published by a publisher or media house. Thus, the form of processing personal information is different from that of the publisher or media house, taking into account their differing functions.[1455] In other words, as best explained by the Article 29 Data Protection Working Party,[1456] the processing carried out by search engines "is additional to that carried out by publishers of third-party websites".[1457] Search engines generate profits derived from the data processing activities, the profits being "inextricably linked to" the data processing activities.[1458] These data processing activities include the processing of personal information of data subjects.

Put differently, a search engine's business is the processing of large volumes of data, personal or otherwise, in order to make it available within the country in which it operates. The search engine funds its operations through the selling of advertising space. The adverts shown to a particular user will often be based on the information that they searched for. Hence, search engines process personal information for economic gain. The economic gain being the profits made from the sale of advertising space, combined with the ability to target adverts to individual internet users, based on their searches.[1459]

---

of the right to be forgotten' (2016) 17(1) *Chicago Journal of International Law* 217 at 226 – 227. Both the CJEU and ECtHR have kept the definitions or descriptions of search engines wide. In *Liberty & others v United Kingdom* [2008] ECHR 568 para 43 the ECtHR describes a search engine as "An automated sorting system or search engine, operating under human control, selected communications containing specific search terms or combinations thereof." In *Google France SARL & Google Inc. v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA & Luteciel SARL; Google France SARL v CNRRH SARL, Pierre-Alexis Thonet, Bruno Raboin & Tiger* SARL EU:C:2010:159 paras 22, the CJEU stated: "When an internet user performs a search on the basis of one or more words, the search engine will display the sites which appear best to correspond to those words, in decreasing order of relevance." See also the Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. and Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) EU:C:2013:424, delivered on 25 June 2013 para 34, and the Opinion of Advocate General Kokott in *Opinion procedure 2/13 initiated following a request made by the European Commission* EU:C:2014:2475, delivered on 13 June 2014 para 224 as a general reference that even a website's internal search engines provides a similar function as internet based search engines. See also *Interflora Inc & another v Marks and Spencer Plc (Rev 1)* [2014] EWCA Civ 1403; *Cochrane Steel Products (Pty) Ltd v M-Systems Group (Pty) Ltd & another* 2016 (6) SA 1 (SCA) para 4, and *Yuppichef Holdings (Pty) Ltd v Yuppie Gadgets Holdings (Pty) Ltd* [2016] ZASCA 118 para 7ffg.

[1455] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014.

[1456] As stated in the Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014.

[1457] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2.

[1458] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and Article 29 Data Protection Working Party *Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain* adopted 16 December 2015 at 4.

[1459] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 56, 81, 97 and 99, L Kugler 'The war over the value of personal data' (2018) 61(2) *Communications of the Association for Computing Machinery (ACM)* 17 – 19, G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal

However, the term "responsible party" is not confined to search engines and the right to be forgotten may also be applied to the original publishers of the article containing the personal information.[1460] Search engines, before completing a request for the right to be forgotten may also contact the original publisher, where this is necessary in the circumstances, to obtain their views, alternatively require that they "forget" the information by altering the highlighted keywords, etc.[1461]

It is important to keep in mind that although the personal information is being legitimately processed in terms of the purpose provided to the data subject,[1462] the personal information still remains the data subject's property. In light of objecting to the processing of personal information, as well as correcting, transferring, etc., it is the data subject who decides as it is their personal information. In other words, a responsible party (or an operator) cannot claim ownership over the data subject's personal information.[1463]

(ii) How Google Spain defined the right to be forgotten

It is important to remember as mentioned above that POPI is based on Directive 95/46, as can

---

data' (2018) 34 *Computer Law & Security Review* 289 – 303, and Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479.

[1460] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), and *Biancardi v Italy* [2021] ECHR 972.

[1461] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 3.

[1462] See sections 9 and 13 of POPI. This is not limited to the data subject consenting to the processing.

[1463] See *Discovery Ltd & others v Liberty Group Ltd* [2020] ZAGPJHC 67 paras 88 – 89. The judgment was decided on 15 April 2020, before POPI was enacted, however, the discussion on who owns the personal information is very instructive. The issue at hand was the use of the Vitality status by Discovery' members, and whether these could be used in an application for an insurance policy with another insurer. The court made it clear in para 89, that it may be used in an application (or for any other reason) as the Vitality status remained the personal data of the data subject. For a comprehensive discussion of the judgment see RM Shay & NI Moleya 'Discovering the value of liberty in intellectual property adjudication: A methodological critique of the reasoning in *Discovery Ltd v Liberty Group Ltd* 2020 4 SA 160 (GJ)' (2021) 4 *Potchefstroom Electronic Law Journal* 1 – 33. See also A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Review* 62 at 65 – 66.

Note: in Europe there is a debate regarding the ownership of data/information. The Charter contains a right to data protection, the question that arises is whether, based on this right, data is capable of being owned by the data subject or, due to the right, it is inalienable. The complete debate is beyond the scope of this thesis, unless there is a need to mention it in terms of the right to be forgotten. See the following on this debate: N Purtova 'Default entitlements in personal data in the proposed regulation: Informational self-determination off the table . . . and back on again?' (2014) 30 *Computer Law & Security Review* 6 – 24, H Zech 'Information as property' (2015) 6 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 192 – 197, W Kerber 'Governance of data: Exclusive property vs. access' (2016) 47 *International Review of Intellectual Property and Competition Law* 759 – 762, V Janeček & G Malgieri 'Commerce in data and the dynamically limited alienability rule' (2020) 21 *German Law Journal* 924 – 943, and B Custers & G Malgieri 'Priceless data: Why the EU fundamental right to data protection is at odds with trade in personal data' (2022) *45 Computer Law & Security Review* 105683.

be seen by the many similarities that can be found between the two pieces of legislation.[1464] This means that the South African courts are likely to draw similar conclusions as those in Europe.[1465] As discussed in Chapter 3, the CJEU in *Google Spain*[1466] used the combination of Articles 12*(b)*[1467] and 14*(a)*[1468] of Directive 95/46 as the basis for the right to be forgotten.[1469] *Google Spain*, acknowledged that there are instances where the two sub-articles may be used alone, however, in terms of the right to be forgotten they will be used in combination. These sub-articles form the basis for the direct communication between the data subject and the controller.[1470] The court pointed out that in combination the data subject is able to object to the continued processing of their personal information, irrespective of whether consent was provided or not, and, thereafter the de-linking (de-indexing/de-referencing) of the personal information may be requested, even in the same application.[1471] Together these provisions

---

[1464] A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 3.

[1465] SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).

[1466] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. Note: *Google Spain* is covered in much more detail in Chapter 2, this is merely a summary to provide a short background for this discussion. See generally AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 49ffg.

[1467] Article 12*(b)* of Directive 95/46 states as follows:

> "Right of access
> 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 . . ."

Article 12*(b)* finds its equivalent in s 24 of POPI.

[1468] Article 14*(a)* of Directive 95/46 states:

> "The data subject's right to object
> 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 . . ."

Article 14*(a)* finds its equivalent in s 11(3) of POPI.

[1469] Note it is now Article 17 of the GDPR. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, and came into effect in 1995. It was later replaced by the General Data Protection Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, was published on 4 May 2016, and entered into force on 25 May 2018. All organisations were required to meet the GDPR's minimum standards. See A Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected "content principles"' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* #7985 1 at 1.

[1470] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 77. Directive 95/46 defines "controller" in Article 2 to mean "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". In *Google Spain* the court held that an operator of a search engine is a controller in terms of Directive 95/46. A "controller" is possibly the equivalent of a responsible party in terms of POPI.

[1471] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 77. The request may, instead of de-linking or de-referencing, require that the information be destroyed, deleted or removed.

provide a valuable personal remedy for the effective protection of the data subject's personal information, without needing the offending text to be removed completely.[1472] In *Google Spain*, the data subject was objecting to the search engine's legitimate interest (in this case an economic interest), to process his personal information.[1473] The processing done by the search engine was in addition to the processing done by the publishers of the newspaper. Also, the data subject could not request that the newspaper remove the legal notice, as it was published in "compliance with a legal obligation to which the controller is subject",[1474] and could not be removed from their website. Also, the rights of publishers to pursue their own legitimate interests when publishing information, including personal information, must be taken into account where the right to be forgotten is being considered.[1475] Hence, the court in *Google Spain* did not require the data subject to first approach the publishing house as the original publisher of the article or notice that contained the personal information.[1476] The search engine fitted the definition of "controller", which is equivalent to the definition of "responsible party" in POPI.[1477] Importantly, the CJEU recognised that lawfully published information may become unlawful overtime. Publication on the internet is not a once off act, it is continuous. The right to be forgotten provides a solution against the continuous publication.[1478]

[1472] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 99.

[1473] The CJEU held that the data subject's protection of their personal information will always take precedence over the economic interests of the responsible party – see *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317paras 80 and 81.

[1474] Article 7*(c)* of Directive 95/46. The POPI equivalent is s 11(1)*(b)*.

[1475] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 63.

[1476] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 39 did note that publishers are able to signal to search engines whether or not information on their website may be indexed by the search engine with the use of codes. In this instance the court acknowledged that a website could use "exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive'" so as to indicate whether articles or notices should "be wholly or partially excluded from the search engines' automatic indexes". However, if the new agency or publisher of the newspaper does not indicate to the operator of a search engine to not automatically index the information, it does not mean that the search engine "is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity".

[1477] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2. The definition of "controller" in Directive 95/46 is:

> "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."

Specifically, a "processor" means

> "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

[1478] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 94. Compare with *Botha v Smuts and another* 2025 (1) SA 581 (CC) para 193.

(iii) Why is a right to be forgotten necessary?

Noting that the right to be forgotten is an internet-based right, what is the essence thereof? The essence of the right to be forgotten (although, strictly speaking, a misnomer) is merely to have the personal information de-linked or de-indexed or de-referenced from the data subject's name.[1479] Generally, the aim is not to delete or destroy or alter the information, but to merely make it more difficult to find, ie internet users will need to use a different search term and not the name of the data subject in order to find the information.[1480] The use of an individual's name is generally the easiest way to obtain the information. There may be circumstances where deleting, or destroying[1481] or even altering (often this is in the form of anonymising the information)[1482] the personal information will be more appropriate. What the right to be forgotten allows, where the information is only de-linked or de-indexed, is for the continued unaltered access thereof, even though it is obtained via another search term, which ultimately makes it trickier to find.[1483]

The reason for invoking a right to be forgotten is to encourage, either a responsible party, the Information Regulator, or a court to find a suitable balance between the rights to privacy and freedom of expression. The CJEU and the ECtHR explored various options where they balanced the rights of privacy and freedom of expression.[1484] The next step to decide is which option should be considered in light of the facts before the court? A possible solution to this question is using a sliding scale or continuum, such as the one formulated in *Bernstein v Bester*,[1485] as an effective starting point in considering whether or not to implement the right to

[1479] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1480] For a complete discussion, see Chapter 2 of this thesis. See *Hurbain v Belgium* (European Court of Human Rights) unreported application no 57292/16 (22 June 2021) – specifically the dissenting opinion of Pavali J. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 259 – 260.
[1481] See *Biancardi v Italy* [2021] ECHR 972.
[1482] See *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021).
[1483] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See also Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2.
[1484] In some instances, the balancing of rights included the economic interests of some of the parties involved, as well as other relevant considerations, depending on the circumstances before the court. See *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 18.
[1485] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC): the sliding scale or continuum consists of two extremes, on the one is the truly personal sphere of privacy, which includes the truly intimate or private aspects of an individual's life, and where there should be no interference from anyone, including the State. On the other extreme end of the continuum, or sliding scale are interactions of individuals within the public sphere, and due to the nature of these interactions cannot be considered private, ie making a public announcement cannot be considered private.

be forgotten, or anonymise the personal information or to delete the information. Each of these options has an impact on the right to freedom of expression and information, some to a higher degree and others to a lesser degree. First, on the one extreme end, the right to "forget", or delete information would be refused – this has the least impact on the right to freedom of expression, the information remains as is and unaltered, and can be found using any keywords that one chooses.[1486] *Recht auf Vergessen II* did not state this directly, but the right to be forgotten would not be applied where the data subjects interact within the public sphere, in light of their employment, etc. and where the right to freedom of expression and information of internet users would take precedence. These instances would include where the data subject consents to an interview, or where the information forms part of a current topical debate, irrespective of how old the information is.[1487]

On the opposite end of the continuum would be the complete deletion, also referred to as the destruction, of the personal information. The personal information is of such an intimate or sensitive nature, that the continued access thereof on the internet by the general public does more harm to the data subject, and the only means to protect the data subject's rights and freedoms, especially the right to privacy, is to permanently delete the personal information. This was the case in *Biancardi v Italy*,[1488] where the ECtHR held that, although the press are entitled to report on crime and criminal activity, they are not immune from de-linking or de-referencing requests, no matter how recent the events are and no matter how accurate the news article may be. In *Biancardi*, the data subjects had been involved in an assault at a restaurant. The ECtHR was not making any findings as to whether the data subjects were guilty or not, ordered that the information be deleted, due to the passage of time, the data subjects were not famous persons, and the criminal court was yet to find them guilty or acquit them.[1489] The problem with the article was that they were silent on whether the trial had commenced or not, and whether the data subjects had been found guilty or not. This led the court to decide that it would be best if the information was deleted.[1490] Deletion has the greatest impact on the right

[1486] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141, *Bernstein & others v Bester NNO & other*s 1996 (2) SA 751 (CC) paras 74 and 78, *Fayed v The United Kingdom* Series A No 294B; Application No 17101/90; (1994) 18 EHRR 393, 34 *BVerfGE* 238 – *Tonband* Part B II para 3.
[1487] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 134 and 141, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.
[1488] *Biancardi v Italy* [2021] ECHR 972.
[1489] *Biancardi v Italy* [2021] ECHR 972 paras 65 – 70.
[1490] *Biancardi v Italy* [2021] ECHR 972 para 70. Regarding the benefits and implications of deleting or "forgetting" see PA Bernal 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 – 18.

to freedom of expression and information, as the information is no longer available, no matter which keywords are used. In light of the terminology used in the GDPR, the information would be "erased".[1491] Another solution, related to deletion, was devised in *Waldis v Von Ulmenstein*.[1492] The court held that due to the unique nature of a blog post, ie it is not a physical newspaper, it is easy to delete the parts that are offensive, and retain that which causes no offense or harm to the reputation of the data subject.[1493] When considering whether the information should be deleted, and depending how it is distributed, and depending on all the relevant facts and circumstances, it may be possible to retain a part of the article, and only remove/delete that which is truly offensive to the data subject.

In-between the two extremes, there are other possibilities on the continuum. Some of these will be located toward the privacy end of the sliding scale and others toward the freedom of expression end of the continuum. Starting with an aspect closer to the protection of privacy, namely anonymization of personal information, ie placing a letter or letters (eg the initials of the data subject's name, or simply an "X") where the name of the data subject would appear. Granted the impact on the right to freedom of expression and information is less severe than complete "erasure" or deletion of the information, as the information remains available, however, in altered form. The personal information can thus no longer be allocated to a specific person, due to the mere appearance of a letter (or letters) in place of the name. This is not taking into account persons that actually know the data subject, who is "hidden" behind that letter.[1494]

Lastly, moving towards the opposite end of the continuum, namely towards freedom of expression, and the placement of the right to be forgotten on the sliding scale: As described at

---

[1491] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *Biancardi v Italy* [2021] ECHR 972. See also Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2, E Politou, E Alepis & C Patsakis 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) *Journal of Cybersecurity* tyy001 at 10, J Connolly 'The right to erasure: Comparative perspectives on an emerging privacy right' (2021) 46(1) *Alternative Law Journal* 58 – 63, and C Docksey 'Journalism on trial and the right to be forgotten', *VerfBlog*, 9 March 2022. *https://verfassungsblog.de/journalism-rtbf/*, DOI: *10.17176/20220309-121127-0* (Accessed: 14 March 2022). Note also Article 17 of the GDPR.

[1492] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).

[1493] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 48. See the discussion in *Dimension Data (Pty) Ltd v Pearton* [2021] ZAECPEHC 54 in light of information placed onto a website.

[1494] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *M.L. & W.W. v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), and *Hurbain v Belgium* (European Court of Human Rights) unreported application no 57292/16 (22 June 2021). BJ Koops, JH Hoepman & R Leenes 'Open-source intelligence and privacy by design' (2013) 28 *Computer Law & Security Review* 676 at 681, and L Bolognini & C Bistolfi 'Pseudonymization and impacts of big (personal/anonymous) data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation' (2017) 33 *Computer Law & Security Review* 171 at 177 – 178.

the beginning of this segment, the right to be forgotten, being a misnomer, provides for information to be de-linked or de-referenced or de-indexed from the data subject's name. This means that where the data subject's name is used as the search term in an internet search engine tool, the information will not appear on the results page.[1495] The only impact on the right to freedom of expression and information is that the information will not be found when using the data subject's name, and the information is left intact, ie there is no alteration. That means that whereas not granting the request for information to be forgotten has the least impact on the right to freedom of expression, by comparison the right to be forgotten, although it leaves the information intact, will still impact on the right to freedom of expression, because, the most convenient search term, the data subject's name, will no longer be linked to the information that an internet user may be looking for.[1496] This is useful where the information may not be altered or anonymised or it may not be deleted due to the nature thereof, ie, in *Google Spain* the information that they were seeking to have de-linked or de-referenced was a legal notice. Legal notices may not merely be anonymised or deleted, they must, for future reference, be available to the internet users who may have in interest an the information, irrespective of the reason for the interest. De-linking thus serves two purposes, the information remains intact, but to protect the data subject, the information is more difficult to locate when an internet search engine is used and the data subject's name is the search terms.

To answer the question at the start of this segment, ie "Why is a right to be forgotten necessary?", POPI contains, as a part of the justifications for the lawful processing of personal information, that personal information may be processed to comply "with an obligation imposed by law on the responsible party".[1497] Examples of what amounts to "an obligation imposed by law" include: enforcing legal claims, for the prevention of crime, in terms of legislation, the common law, customary law, the Constitution, and court orders.[1498] In matters where newspapers have complied with court orders and published legal notices, such as sales in execution, notices informing creditors of impending insolvency proceedings, or changes in

[1495] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. For a complete discussion, see Chapter 2 of this thesis. See *Hurbain v Belgium* (European Court of Human Rights) unreported application no 57292/16 (22 June 2021) – specifically the dissenting opinion of Pavali J. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 259 – 260.
[1496] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1497] Section 11(1)*(b)* of POPI.
[1498] *Welch v Commissioner for the South African Revenue Service* 2005 (4) SA 173 (SCA) paras 44 – 49 (majority judgment), *Divine Inspiration Trading 205 (Pty) Ltd and another v Gordon and others* 2021 (4) SA 206 (WCC), and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 59 – 60, 75, and 192.

matrimonial status, these notices cannot be modified by anonymisation or deletion. Recently, the Constutional Court, although dealing with privacy, but not the right to be forgotten, pointed out that online publication does not consist of a singular act. Online publication is a continuous process. The court explained that as[1499]

> "online publication remains online, it continues to be published to third parties to whom the publication is accessible on the internet. Therefore, when the lawfulness of online publication is assessed, a court cannot confine its focus to the moment of initial publication. Online publication that originally may have been lawful, can become unlawful if the statement or document originally published continues to be published online despite changed circumstances that affect the lawfulness of ongoing publication."

In modern society, maintaining our privacy and autonomy in an online environment is one of the many challenges that data subjects must face. Hence, a right to "forget" information would serve the purpose of protecting the data subject's privacy, and ensuring that the current circumstances of the data subject are portrayed, where a search is conducted using the data subject's name as the search terms.

Whether the data subject will be successful in obtaining a request for have information de-linked/de-referenced, ie "forgotten", or anonymised or completely deleted, or whether the data subject will be unsuccessful, it will be necessary to balance all parties' rights, freedoms and interests.[1500] The CJEU, the European Court of Human Rights and the Bundesverfassungsgericht have pointed out in the cases, discussed in Chapter 3 of this thesis, that it includes the rights, freedoms and interests of the general public, in the form of internet users, search engines and publishers.

The next aspect to determine is whether South Africa has a right to be forgotten and what it would look like.

(iv) What could a South African right to be forgotten look like?

Burn and Burger-Smidt and De Stadler *et al* in their respective texts provide a different concept of a possible South African right to be forgotten. Burns and Burger-Smidt suggest that s 24(1)

[1499] *Botha v Smuts and another* 2025 (1) SA 581 (CC) paras 193, see also para 240 of Chaskalson AJ's judgment.
[1500] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*. See also *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 18.

alone is sufficient to establish the right to be forgotten within the South African context.[1501] However, the legal position is not that clear, POPI does not, like the General Data Protection Regulation or GDPR, contain a section titled "the right to be forgotten". POPI is based primarily on Directive 95/49 and not on the current GDPR.[1502] Article 17 in the GDPR provides for the right to be forgotten or the right of erasure. Article 17 is far more direct and comprehensive in its wording with the protection that it provides, where a request for the destruction, deletion, erasure or removal of personal information is made.[1503] De Stadler *et al*, looked at the right to be forgotten, by focussing on the principles set out in *Google Spain* as well as the legislative developments in the EU.[1504] Hence, it can be argued that POPI does not include a right to be forgotten.

The following provides a background to the discussions that follow, especially in light if the internet and search engines. Directive 95/46 was one of the main texts that inspired vast sections of POPI.[1505] Directive 95/46 was drafted at a time when the internet was not as advanced as it is today. In other words, the drafters of Directive 95/46 focused on protecting privacy and personal data in light of paper documents, which includes the requisite filing systems and archives for storing paper documents. If someone wanted to obtain the information from these archives in the past, they would have to physically travel to the archive and, in some instances, actually, personally look through the papers and/or the index cards in order to find the information that they were after. Now with the digitisation of those archives, an internet user may obtain the information from the comfort of their own home.[1506]

Even though, the drafters of POPI would have had the opportunity to see the

---

[1501] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 78 – 79. Note, s 24(1) of POPI provides data subjects with the right to have personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully" corrected or deleted, depending on the circumstances in terms of which the request is made. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 162 and 573.

[1502] SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).

[1503] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 79 – 80, and A Naude & S Papadopoulos 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 213 at 228.

[1504] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 259 – 260 and 574.

[1505] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 259, and AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 44.

[1506] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 36, see also Y Poullet 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 at 212 – 216.

development of Article 17 of the GDPR, ie the drafting of "the right to erasure (right to be forgotten)", and how the EU was striving for new solutions to protect personal information in online resources and archives, the drafters pointed out that POPI was mainly based on Directive 95/46, and not the GDPR. During the enactment of POPI, there would have been a possibility to make the relevant amendments, however, the legislator did not do so. Hence, in POPI there is no specific section, as with Directive 95/46, which sets out the right to be forgotten – the specific right to erasure or right to be forgotten was first drafted in the GDPR.[1507]

Turning to define a "South African right to be forgotten", by comparing the relevant articles from Directive 95/46 with the relevant sections in POPI: Sections 11(3), and 24(1) of POPI are very similar to Articles 12*(b)* and 14*(a)* of Directive 95/46.[1508] Articles 12*(b)* and 14*(a)* provide the data subject with the right to object to the processing of data, in certain instances, and have the information de-linked or de-indexed,[1509] alternatively, deleted, destroyed or altered. Section 11(3) specifically requires that the objection must be in the "prescribed manner, on reasonable grounds relating to [the data subject's] particular situation". Note too, s 11(4), which states that where there is an objection to the processing of personal information, the information may no longer be processed. Section 24(1) provides a possible guide to the data subject as to what are "reasonable grounds" for correcting, deleting or destroying personal information that is under the control of a responsible party,[1510] namely, where it is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully." The argument that follows will discuss, analyse and promote the use of this combination of sections from POPI, similarly to how the CJEU structured the right to be forgotten, and this will form the right to be forgotten in South Africa.

[1507] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 259, and AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 44.

[1508] Directive 95/46. The drafters of POPI would have had initially used Directive 95/46 as a base from which to develop POPI. However, POPI was only assented to during 2013. Before that, the drafters of the GDPR had communicated their intent to reform Directive 95/46 during 2010. Hence, the drafters of POPI eventually had the benefit of both legislative documents – although, POPI does tend to have a closer resemblance to Directive 95/46. See also AS Basson *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis, University of Pretoria, October 2015) at 44ffg.

[1509] POPI speaks of de-identifying, I have kept the international term of de-linking or de-indexing or de-referencing the information to the name of the data subject, this is also in line with the wording of *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 and the discussion in Chapter 2 of this thesis.

[1510] It may or may not be the responsible party, eg a newspaper that prints a legal notice in terms of a court order or a social media web page where information has been shared or posted and the ability to obtain it needs to be restricted.

(v) POPI

Section 11(3) sets out under what circumstances[1511] a data subject may object to the processing of their personal data, or withdraw/revoke consent,[1512] with the emphasis that the personal data may no longer be processed as set out in s 11(4). Section 24(1) deals with the request to, not only correct, but also delete personal information that is being or has been processed. It should be noted that "processing" includes the storage (retention) of personal information.[1513]

There will be instances where a data subject will be required not merely to apply for the de-linking, deletion or destruction of the processed personal information, for the application to be successful, but also to object to the processing, or to withdraw their consent to the processing, of their personal information before or simultaneously with the request to de-link, delete or destroy the personal information.

Where a data subject objects to the processing of their personal information in terms of s 11(3), but also in terms of s 11(2), they may simultaneously request in terms of s 24(1) that their personal information be deleted. This approach[1514] will likely be the preferred method to use where personal information in the form of an account, ie social media accounts, or in store accounts, etc. are deleted with responsible parties. Put differently, and in light of the objections provided in s 11(3), this will include where personal information is processed[1515] in terms of a legitimate interest, irrespective if it is in the data subject's[1516] or responsible party's or a third party's[1517] interest, or in terms of a public body's obligation.[1518] A similar approach, although not specifically mentioned within POPI, may be used where a data subject ends the contractual relationship between themselves and a responsible party.[1519] Most of these require that the consent for the processing or that there is an objection where consent was not required,

[1511] Note as set out above, a data subject may object to where their information is being processed to protect the data subject's legitimate interests (s 11(1)*(d)*), or (s 11(1)*(e)*) it is necessary to process the personal information for the "proper performance of a public law duty by a public body", or (s 11(1)*(f)*) the processing is in terms of a responsible party's (this includes a third party's) legitimate interests.
[1512] Note s 11(2)*(b)* provides that a data subject may withdraw their consent "at any time", where consent was necessary for the lawful processing of personal information.
[1513] See s 1 of POPI. See also the discussion earlier in this chapter.
[1514] Note this was the preferred approach of the CJEU in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88.
[1515] Section 11(3) of POPI.
[1516] See s 11(1)*(d)* of POPI.
[1517] See s 11(1)*(f)* of POPI.
[1518] See s 11(1)*(e)* of POPI.
[1519] Section 11(1)*(b)* of POPI provides for the processing of personal information in order to conclude or perform concerning contractual duties. See S van Deventer 'Regulating substantively unfair terms in online contracts' (2021) 32(2) *Stellenbosch Law Review* 518 at 526 – 527, and S van Deventer 'Problems relating to the formation of online contracts: A South African perspective' (2021) 138(2) *South Africa Law Journal* 219 – 257.

including continued processing, be withdrawn. [1520] It is only then possible to request that the responsible party de-links, anonymises, deletes or destroys the personal information – depending on the circumstances of each individual matter. A right to be forgotten request will generally be uncontroversial in such an instance, as it is based either on a ground in terms of POPI (ie withdrawal of consent or an objection to the processing of personal information) or the termination of a contractual relationship.

The problem that a data subject faces is where their personal information is processed in terms of "an obligation imposed by law". [1521] As pointed out in *Divine Inspiration*, "an obligation imposed by law" refers to acts of parliament and their accompanying regulations and rules.[1522] A further "obligation imposed by law" would be a court order.[1523] POPI does not offer a direct remedy where a data subject can object to the processing of their personal information in terms of "an obligation imposed by law". This is where the right to be forgotten may assist. As stated earlier, the right to be forgotten is an internet based right.[1524] Often the issue does not lie with the responsible party's processing of the personal information in terms of their obligation imposed on them by the law, but where the information is processed in addition to that by another responsible party in terms of a legitimate interest.[1525] This occurs, for example, where a notice for the winding-up or sequestration of an insolvent estate is published in both the *Government Gazette* as well as in a national and/or local newspaper. The *Government Gazette* as well as most publishers of newspapers have an online presence, and in many instances, they do not only have a web page, but also a social media account. The legal notices are often indexed and archived on these websites with the use of specific keywords, which include the names of individuals/data subjects, so as to make them easily available for those looking for the information. Over time, these notices become "inaccurate, irrelevant, excessive, out of date, incomplete, misleading" and to some degree the continued processing

[1520] See s 11(1)*(a)* of POPI. It is submitted that consent is also required in the conclusion of a contract because the data subject agrees to be bound by the terms of the contract – s 11(1)*(b)* of POPI.
[1521] See s 11(1)*(c)* of POPI.
[1522] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon &others* 2021 (4) SA 206 (WCC). Examples of "obligations imposed by law" include maintenance obligations, tax obligations in terms of the Income Tax Act 58 of 1962, etc., see the majority judgment in *Welch v Commissioner for the South African Revenue Service* 2005 (4) SA 173 (SCA) paras 44 – 49.
[1523] See the majority judgment in *Welch v Commissioner for the South African Revenue Service* 2005 (4) SA 173 (SCA) paras 44 – 49, and *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC).
[1524] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014.
[1525] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 83.

thereof is also unlawful.[1526] In keeping with the example, an insolvent may be rehabilitated. The preferred solution in circumstances where there has been a reasonably long period of time has passed (ie passage/effluxion of time) and the fact that the personal information no longer reflects the current situation of the data subject, and the inability to permanently remove or delete such information that has been published in terms of a court order or other legal obligation, to de-link or de-index the information.[1527] Similar grounds or arguments were used by the CJEU to substantiate the creation of the right to be forgotten.[1528]

The data subject when objecting to the processing, including the continued processing, of their personal information, needs to state that the information is either inaccurate, and/or irrelevant, and/or excessive, and/or out of date, and/or incomplete, and/or misleading and/or obtained unlawfully, with any further explanation that may be necessary, for example, that their current circumstances are not reflected by the processed information.[1529]

In terms of the stringent definition of consent in POPI, and the requirements that the consent must be "an expression of will" means that data subjects would need to take a positive act in providing their consent for the processing of their personal information.[1530] Search engines would therefore not be able to argue that because data subjects have posted their personal information in a public online space, ie without privacy restrictions on social media, that data subjects have given implied consent for the processing of their personal

[1526] See s 24(1) of POPI. See also *Botha v Smuts and another* 2025 (1) SA 581 (CC) paras 193 and 240.
[1527] This was the solution best suited for such an instance in *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and the subsequent cases that followed, the information was not destroyed, but through the use of a change in the search algorithm, the information became more difficult to find.
[1528] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1529] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. Briefly, and without wanting to repeat anything unnecessarily, the facts of *Google Spain* are: Mr González was sequestrated for failing to pay his social security taxes. A prominent regional newspaper published the sale of his property in execution for the payment of the debt. When the newspaper began digitising its archives, the two notices for the sale were also digitised. When an internet search using Mr González's name as the keyword was done, the notices ranked high in the search results. Mr González complained, that even though these notices were related to legal proceedings, their continued availability or the processing of that information was excessive in that it prevented Mr González from integrating into society as a rehabilitated insolvent. See also Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2, and E De Stadler, IL Hattingh, P Esselaar & J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 69.
[1530] Section 1 of POPI. See also *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *GC & others v CNIL* EU:C:2019:773 paras 61 – 62. See also I Cofone '*Google v. Spain*: A right to be forgotten?' (2015) 15(1) *Chicago-Kent Journal of International and Comparative Law*. *https://scholarship.kentlaw.iit.edu/ckjicl/vol15/iss1/1* (Accessed: 23 January 2023) 1 at 6, K O'Hara 'The right to be forgotten: The good, the bad, and the ugly' (2015) July/August *The Digital Citizen* 73 at 25, and J Pushka 'The applicability of the Personal Information Protection and Electronic Documents Act to de-indexing internet search engine results' (2019) 19 *Asper Review of International Business and Trade Law* 175 at 182. One could argue that data subject's give search engines a form of tacit consent – however, tacit consent is not, in terms of POPI or Directive 95/46 or the GDPR, enough – it must be explicit consent.

information.[1531] Data subjects expect that even where they post personal information, ie photos, anecdotes, etc., without privacy restrictions, that such information will still be private, and only made available on the social media website.[1532]

Search engines, as noted in the CJEU, do not necessarily obtain the data subject's consent to process their personal information, but process information in light of a legitimate interest.[1533] As noted above, in terms of POPI, the responsible party (in this case the search engine) may process a data subject's personal information in terms of a legitimate interest.[1534] The search engine's legitimate interest is an economic one.[1535] Search engines process all information irrespective of whether it is personal or not with the assistance of web crawlers.[1536] These web crawlers search and index the information that is placed on the (open) internet so that it may be retrieved and displayed on a results page based on the keywords typed into the search tool by internet users.[1537] Search engines, such as Google, when operating within a specific country,[1538] do not merely provide a free online search tool, but also sell advertising space to local companies. Search engines will, based on the internet user's keywords, show these adverts amongst the search results. The adverts shown will match the search terms used in the search tool.[1539] In terms of s 11(3), a data subject may object to the processing of their personal information where it is processed in terms of a legitimate interest. In this example, and as stated above, the legitimate interest is an economic one.[1540] Simultaneously a request in terms of s 24(1) may be lodged. Section 24(1) provides for inaccurate, irrelevant, dated, incomplete, or misleading information to be corrected or deleted. However, where the information is processed in terms of s 11(1)*(c)* which is an "obligation imposed by law",[1541]

[1531] G Xiao 'Bad bots: Regulating the scraping of public personal information' (2020) 34(2) *Harvard Journal of Law & Technology* 701 at 711.
[1532] G Xiao 'Bad bots: Regulating the scraping of public personal information' (2020) 34(2) *Harvard Journal of Law & Technology* 701 at 711.'
[1533] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 69.
[1534] Section 11(1)*(f)* of POPI.
[1535] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 56, 81 and 97. See also *Interflora Inc & another v Marks and Spencer Plc (Rev 1)* [2014] EWCA Civ 1403; *Cochrane Steel Products (Pty) Ltd v M-Systems Group (Pty) Ltd & another* 2016 (6) SA 1 (SCA) para 4, and *Yuppichef Holdings (Pty) Ltd v Yuppie Gadgets Holdings (Pty) Ltd* [2016] ZASCA 118 para 10.
[1536] The *Merriam Webster Dictionary* defines a web crawler as "a computer program that automatically and systematically searches web pages for certain keywords" – Merriam-Webster 'Web crawler' *Merriam-Webster.com Dictionary*. *https://www.merriam-webster.com/dictionary/web%20crawler* (Accessed 5 March 2024). See also D Stevanovic, A An & N Vlajic 'Feature evaluation for web crawler detection with data mining techniques' (2012) 39 *Expert Systems with Applications* 8707 at 8707, footnote 1.
[1537] P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627.
[1538] Also referred to as a domain.
[1539] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 43.
[1540] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1541] Section 11(1)*(c)* of POPI.

POPI does not include a provision which allows for the correction or deletion of such information, and neither does the law generally provide such a provision. A responsible party, including a search engine, will not be able to delete (nor correct) such information.[1542] Search engines will only be able to "delete" the link between the information and the data subject's name – hence, the only option available is to "re-code" (ie "re-write")[1543] the algorithmic codes to exclude (ie de-link) that particular information that when the data subject's name is typed into the search engine tool that the inaccurate, irrelevant, dated, incomplete, or misleading information is not displayed on the results page.[1544] The information will still be available, but it will no longer be found using the data subject's name as the keywords. An internet user looking for the specific information that is no longer linked to the data subject's name, will have to use a different search term or keywords to find it.[1545] Hence, the search engine's economic interest will be balanced with the rights and interests of the data subject where a decision is considered to have the personal information de-linked/de-indexed.

As briefly mentioned above, an important factor in consideration where there is an application for information to be de-linked, de-referenced or de-indexed is what are the current circumstances of the data subject, often considered in light of the passage of time. POPI provides that personal information should be corrected or deleted where the data subject is able to prove that that information is "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully".[1546] In *Google Spain*, the court pointed out that the data subject could request that the information be de-linked from the data subject's name, even though the processing was in terms of a court order. The focus was on the further processing undertaken by the search engine, ie Google, in terms of their economic interest (which was held to be a legitimate interest). The data subject was a rehabilitated insolvent.[1547] Similar

[1542] This will also be true for the responsible party that posted the information on their web page, ie in keeping with the example from *Google Spain*, South Africa's Government Printing Works publishes the *Government Gazette*, in which notices regarding the impending sequestration of a data subject must appear. This is in terms of the relevant statute as well as a court order. Both these are examples of where the responsible party (ie the Government Printing Works) must process the personal information in terms of "an obligation imposed by law".
[1543] J Burrell 'How the machine "thinks": Understanding opacity in machine learning algorithms' (2016) 3(1) *Big Data & Society* 1 at 3, and P Bell 'Algorithms: The intellectual capital of the internet' (2001) July/August *Ivey Business Journal* 44 – 48, note also the comments of S Abiteboul & J Stoyanovich 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation' (2019) 11(3) *Journal of Data and Information Quality* 1 at 6.
[1544] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1545] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1546] Section 24 of POPI.
[1547] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

considerations in *NT1 v Google LCC*[1548] and *Recht auf Vergessen I*,[1549] where the convictions were either automatically expunged, or where the former accused had completed their prison sentence, respectively. Similarly, in terms of POPI, and the relevant South African legislation specifying when an individual is rehabilitated or their criminal record expunged (this is elaborated on in the next chapter), courts, in light of the "conditions for lawful processing of personal information" in Chapter 3 of POPI, especially in terms of section 11(3) and 24(1), would draw a similar conclusion against search engines.

(vi) Remedies provided in POPI

POPI does not provide specifically for the option to de-link or de-index or de-reference – the closest, but this has more to do with anonymising the personal information, is de-identification in terms of s 14(4). De-linking or de-indexing or de-referencing is a remedy that the courts, in light of the competing constitutional rights of freedom of expression, specifically the right to impart and receive information, and privacy, could implement.[1550] The reason for this is that it was the court in *Google Spain* that came up with this solution, as there was no provision in Directive 95/46 that provided for this option.[1551] Alternatively, the legislature would need to amend POPI to provide for this option, as was the case in the GDPR.[1552] De-linking or de-indexing or de-referencing provides that the information is no longer directly associated with the data subject. The main limitation on the right to impart and receive information is that the information will be harder to find.[1553] The member of the public looking for the information on the data subject – for whatever reason – will need to use other keywords, or search terms to find it and not the data subject's name. However, the information will generally be unaltered and, in most cases, will still contain the name of the data subject. But other remedies may be considered depending on the specific circumstances of the data subject – in some instances altering the information, by anonymising the name of the data subject will be appropriate, this

[1548] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB).
[1549] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.
[1550] Note, specifically the higher courts have an inherent power to develop and moderate their own processes, see s 173 of the Constitution of the Republic of South Africa, 1996. As an example, see *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See also Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2.
[1551] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1552] See Article 17 of the GDPR.
[1553] Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12* adopted 26 November 2014 at 2.

would amount to de-identification as provided for in s 14(4) of POPI. In other instances, the complete destruction or deletion of the information in terms of s 24(1) read with s 14 will be best. But these solutions or remedies should be considered, at the end – namely, the complete destruction of the information is final in effect and that means that information is no longer available – this should be a measure of last resort, and would infringe far more drastically on freedom of expression, than merely de-linking/de-indexing/de-referencing, alternatively, altering the information would. It may be the middle ground that keeps both the public in general and the data subject satisfied.

(f) Conclusion

The right to be forgotten can be used to forget (de-link/de-index/de-reference), anonymise, delete or destroy information, or, where the information is processed in terms of a legal obligation the information may be de-linked from the data subject's name. Personal data that is processed in terms of an obligation in terms of the law, as set out above, cannot simply be deleted or anonymised. Hence, de-linking/de-referencing the information provides the data subject to not only keep such information private, but also ensures that the information displayed in the search results page, on a search done using the data subject's name, portrays the data subject's current circumstances. A right to be forgotten would guarantee the further accessibility of the personal information, but the data subject's name will no longer be the keyword or term that may be used to find it.[1554] The basic principle from *Google Spain*, which finds an echo within the South African Constitution and POPI, is that the rights of all concerned must be balanced to find the best possible solution, when de-linking, destroying or deleting the personal information of the data subject.

VIII CONCLUSION

POPI is very comprehensive in achieving the aim at protecting personal information during and even once the processing thereof is completed. The data subject – as outlined in the discussions above – has various remedies at their disposal where personal information is not processed in terms of the conditions for lawful processing. The conditions provide the minimum standards required to ensure that the personal information is not processed beyond the original consent and what is necessary or relevant or is inaccurate in order for the responsible party to fulfil the required purpose. The legislature in drafting POPI has certainly

[1554] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.

made every effort to balance the constitutional rights of privacy and freedom of expression, however, due to the main aim of POPI, to protect personal information, POPI favours privacy over freedom of expression.[1555] However, the right to privacy is not absolute, and must, as detailed in Chapter 4, be balanced against freedom of expression – this too is alluded to in the Preamble of POPI, with the words that POPI regulates "the processing of personal information [and] gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests."

Although not specifically set out in POPI, there is a possibility for the data subject to request that their personal information be de-linked or de-indexed from their name, as the search term or keyword used. As argued above, it makes the information more difficult to find, but generally leaves it intact or unaltered – unlike where the information is directly deleted or destroyed. The right to be forgotten finds a middle ground between the general public's right to receive and impart information, in light of the right to freedom of expression, as well as meeting the data subject's right to privacy.

In the next chapter – based on the discussion and defining the right to be forgotten within South Africa, what are the lessons South Africa can learn from countries where the right to be forgotten is more established, and how these can be applied in light of the current legal principles.

[1555] F Coetzee 'The press and POPI: Media law' (2014) 14(4) *Without Prejudice* 69 at 70. See also *Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others* [2022] ZAECMKHC 42 para 18.

CHAPTER 6

FORGETTING: LESSONS FOR SOUTH AFRICA

I INTRODUCTION

In the last few years, there have been numerous headlines dealing with data breaches/leaks,[1556] and revelations of what data/information is actually being collected by big data companies such as Apple, Google, and Meta.[1557] It raises questions about how much control these big data companies already have over the personal data/information of their users. Moreover, how well are these companies shielding personal data/information from outside interference? It is the possibility of abusing collected personal data/information that has led to the promulgation of data protection legislation, as discussed in the previous chapters. The aim of this legislation is to promote the protection of human rights, specifically the right to the privacy. South Africa (SA), following the Europe Union (EU), and many other countries, has acknowledged that there is a need to actively protect the personal data/information of data subjects with the passing of the Protection of Personal Information Act 4 of 2013 (POPI).

The cases discussed in Chapter 3 illustrated the importance of balancing conflicting rights where personal data/information is publically available or shared, especially the competing rights of the data subject and the controller/responsible party.[1558] The case discussion in Chapter 3 focused on how the Court of Justice of the European Union (CJEU), the European Court of Human Rights (ECtHR) and the national courts applied the right to be forgotten whilst balancing the rights and interests of all parties involved. These judgments have created a body of legal principles and rules the South African legislature and courts may use and develop, taking into account the Constitution and how the courts have balanced the rights

[1556] A Kulkarni (ed) 'Data of 500 million WhatsApp users leaked, up for sale online: Report' *NDTV*, dated 28 November 2022. *https://www.ndtv.com/world-news/whatsapp-data-leaked-data-phone-numbers-of-500-million-whatsapp-users-leaked-up-for-sale-online-report-3558403* (Accessed: 30 November 2022), P Handley 'Snowden leaks: 10 years later, US intelligence still collects huge amounts of information' *Mail & Guardian*, 5 June 2023. *https://mg.co.za/world/2023-06-05-snowden-leaks-10-years-later-us-intelligence-still-collects-huge-amounts-of-information/* (Accessed: 29 January 2024).

[1557] D Curran 'Are you ready? Here is all the data Facebook and Google have on you' *The Guardian*, 30 March 2018. *https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy* (Accessed: 29 January 2024), H Labuschagne 'Apple vs Google vs Facebook —this is who tracks the most personal data types' *My Broadband*, 26 August 2022. *https://mybroadband.co.za/news/internet/ 458095-apple-vs-google-vs-facebook-this-is-who-tracks-the-most-personal-data-types.html* (29 January 2024). A Karan, N Balepur & H Sundaram 'Your browsing history may cost you: A framework for discovering differential pricing in non-transparent markets' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 717 – 735.

[1558] See Article 2*(d)* of Directive 95/46, Article 4(7) of the GDPR, and s 1 of POPI.

to privacy and freedom of expression in past cases.[1559]

It is worth remembering that the right to be forgotten is merely a species of the right to privacy and is a statutory right.[1560] This is important, as the South African Constitution does not have a hierarchy of rights, and all rights must be applied equally to natural and juristic persons. However, certain limitations may apply, especially where rights are being balanced against each other.[1561] As is stated in the preamble of POPI, this means that the right to privacy (ie the right to be forgotten) must be balanced with the other rights in the Constitution, especially the right to freedom of expression. The cases, as discussed in Chapter 3, held that the interests, rights and freedoms of the data subject must be balanced against those of third parties seeking the information (ie the general public or internet users). Where competing rights are balanced, the South African courts have held that an important factor to consider is whether the limitation of the conflicting rights is proportionate to the result that the aggrieved party wishes to achieve or whether there is another less restrictive and just as effective means of achieving that result.[1562] The right to be forgotten achieves this aim, as merely de-linking or de-referencing the information from the name of the data subject does not delete the information completely, it simply makes it harder to find. Therefore, as mentioned in the previous chapters, privacy (including the right to be forgotten) assists with the development of an individual's (or data subject's) personality.[1563]

The purpose of this chapter is to directly compare POPI with 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 (Directive 95/46), as this was the main piece of legislation used in drafting POPI.[1564] Since May 2018,

---

[1559] See Chapter 4 of this thesis.

[1560] NNG de Andrade 'Oblivion: The right to be different … from oneself: Reproposing the right to be forgotten' (February 2012) 13 *IDP. Revista de Internet, Derecho y Política* 122 at 125, and A Slane 'Search engines and the right to be forgotten: Squaring the remedy with Canadian values on personal information flow' (2018) 55 *Osgoode Hall Law Journal* 349 at 352.

[1561] Sections 7. 8 and 36 of the Constitution.

[1562] *S v Manamela & another (Director-General of Justice intervening)* 2000 (3) SA 1 (CC) para 66, and *Primedia Broadcasting (a division of Primedia (Pty) Ltd) & others v Speaker of the National Assembly & others* 2017 (1) SA 572 (SCA) para 31. Section 36 of the Constitution is referred to as the "limitations clause" and provides the factors to be considered when balancing competeting rights in SA. Note also the discussion in Chapter 4 of this thesis titled "Balancing of privacy and expression in the case law".

[1563] 34 *BVerfGE* 238 – *Tonband* Part B II para 3, M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 209 – 211, S Singleton 'Balancing a right to be forgotten with a right to freedom of expression in the wake of *Google Spain v. AEPD*' (2015) 44 *Georgia Journal of International and Comparative Law* 165 – 194, F Zufall 'Challenging the EU's right to be forgotten: Society's right to know in Japan' (2019) 5 *European Data Protection Law Review* 17 at 19 and K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157.

[1564] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act:*

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, known as the General Data Protection Regulation (the GDPR), repealed and replaced Directive 95/46. The CJEU, in certain decisions just after the enactment of the GDPR, in order to provide guidance thereto, made its rulings in terms of both Directive 95/46 and the GDPR.[1565] Some of the cases discussed in Chapter 3[1566] focused only on Directive 95/46, as these were decided and heard before the GDPR was fully enacted. Where these earlier cases are discussed, relevant aspects of the GDPR will also be mentioned.

The discussion in this chapter will mirror a part of Chapter 3, ie the topics covered by the cases that developed the right to be forgotten will be set out herein, in a similar order. The differences in the approaches between Europe and South Africa will be highlighted, any possible issues will be detailed, and potential solutions will be provided. The broad topics covered in Chapter 3 where the right to be forgotten was applied are the following: first, the territorial jurisdiction of the right to be forgotten, second, the right to forget a crime and criminal trials, third, statements, interviews, etc, made in a professional capacity, fourth, the processing of special categories of data, and last, the anonymisation and deletion of archives. The topics and considerations from the cases in Chapter 3 will be compared with the approaches from the superior courts, especially the Constitutional Court, as described in Chapter 4, as well as the relevant discussions in light of POPI, as illustrated in Chapter 5.

The topics covered in Chapter 3, as listed above, include areas where the balancing of the competing rights will be more straightforward, and a solution will be easier to ascertain than in other instances. The more difficult topics are anoymisation and deletion, especially since the consequences of such an order have a greater impact on freedom of the expression, in comparison to merely requiring that the information appears on the search page in chronological order. However, the courts and the relevant data protection officers and

The last POPIA book you will ever need (2021) at 47 – 48.

[1565] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772 paras 40 – 41. See M Zalnieriute '*Google LLC v. Commission nationale de l'informatique et des libertés* (*CNIL*)' (2020) 114(2) *The American Journal of International Law*' 261 at 262, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[1566] Whether in the text or the footnotes, see *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* EU:C:2017:197, *Google Netherlands B.V, Google Inc.* NL:HR:2017:316 *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II*. Although *Recht auf Vergessen I* and *Recht auf Vergessen II* were decided after the enactment of the GDPR, they mainly focus on law is in terms of Directive 95/46, because the cases had started well before Directive 95/46 was repealed.

authorities will need to carefully consider the facts before them when considering what would amount to the best order in the circumstances of the matter.

The chapter will also include other possible factors that the courts (or data protection officers, or information regulators) should consider in applications for the right to be forgotten – these factors have featured in the comments from academics, discussing the case law from the CJEU and the ECtHR. The chapter will close with a final conclusion for the thesis.

II JURISDICTION

(a) Introduction

The reason for not labelling this section "territorial application" is because this is not a controversial issue within the scope of this thesis, although it is important. Directive 95/46 does not have a specific article dealing with its territorial application.[1567] However, the CJEU in *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (*Google LLC v CNIL*)[1568] confirmed the territorial application of the right to be forgotten, in terms of Directive 95/46, as being limited to only within the EU. In coming to this conclusion, the CJEU also referred to Article 3 of the GDPR, which provides for the territorial application of the right to be forgotten is limited to the territory of the EU. The GDPR, as stated before, was the first time that the right to be forgotten was actually drafted.[1569] Hence, the right to be forgotten is applicable only within the territorial jurisdiction of the EU, as the GDPR is silent on how personal data/information that is found within a domain outside of the EU should be treated. This includes countries where a similar right to be forgotten exists.[1570] The reason for the regional approach is based on the fact that all Member States of the EU have signed and are thereby required to enact the principles of the GDPR within their individual territories.[1571] The

[1567] Article 3 of Directive 95/46 sets out the scope and Article 4 the applicability of national law. Note also Recital 65 of Directive 95/46 which calls for uniformity of application. See also B Van Alsenoy & M Koekkoek 'Internet and jurisdiction after *Google Spain*: the extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120.

[1568] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.

[1569] See Chapter 2 of this document.

[1570] *Google LLC v CNIL* EU:C:2019:77 para 61 and 63. Note, the Supreme Court of Canada, in *Google Inc. v Equustek Solutions Inc.* 2017 SCC 34, held that it is possible, depending on the harm suffered, to implement a global de-indexing order – however the request was made on an interlocutory application, pending trial. The Supreme Court of Canada was not dealing with the right to be forgotten per se, merely a request from one company (ie Google) to temporarily de-index the web page of another.

[1571] This is in terms of the following treaties and their subsequent amendments: Treaty on the Functioning of the European Union (Consolidated 2016) (TFEU), formerly Treaty Establishing the Economic Community, signed at Rome, on 25 March 1957 (formerly known as the Treaty of Rome, see Article 358 of the TFEU), and Treaty on European Union (Consolidated 2016) (TEU) (formerly the Treaty of Maastricht). Note the TFEU and the TEU were consolidated in Lisbon in 2007, see the Treaty of Lisbon amending the Treaty on European Union and the

GDPR, unlike Directive 95/46, requires that there is uniformity and consistency in its application. Hence, the right to be forgotten, where granted in an individual Member State, should be applied throughout the EU.[1572] Although there is not a specific provision stipulating for an application throughout the EU, the CJEU has encouraged data protection authorities to work together and bring about uniformity and that the right to be forgotten where applied in one country should apply in all Member States.[1573]

Unlike the various Member States of the EU, South Africa has not implemented a regional data protection statute, ie one from the African Union. Instead, South Africa has implemented its own domestic legislation in the form of POPI, which is based on the EU as well as other international standards.[1574] POPI does not contain a specific section regarding the territorial limits thereof, however South African law does have the presumption that South African statutes do not apply extraterritorially.[1575] Hence, the right to be forgotten will be applicable only within South Africa. There is no controversy with respect to this topic.

However, it is not unusual for data protection legislation to have wider jurisdictional scope, in comparison to its territorial application. This was canvassed in Chapters 2 and 3 (in terms of Directive 95/46 and the GDPR) and in Chapter 5 (in terms of POPI). Hence, what is dealt with herein is how the various data protection legislative instruments, through the definitions and case discussions, have defined their jurisdictional scope. The essence of the jurisdictional scope will be set out below for the EU and South Africa, followed by possible suggestions for South Africa to follow or consider where a similar case is heard and decided in the courts.

Treaty establishing the European Community (2007/C 306/01), signed at Lisbon, on 13 December 2007 (Treaty of Lisbon). The treaty of Lisbon was consolidated, as set out above, in 2016.

[1572] *Google LLC v CNIL* EU:C:2019:77 para 66 – 68. In para 70 the CJEU pointed out that the data subject's rights and freedoms are to be protected throughout the EU.

[1573] *Google LLC v CNIL* EU:C:2019:77 paras 64, 66 and 72. See generally F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 155 – 156. See generally A Johnston & H Unberath 'Law at, to or from the Centre? The European Court of Justice and the Harmonization of Private Law in the European Union' In F Cafaggi (ed) *Collected Courses of the Academy of European Law* (2006) at 149 – 190.

[1574] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 47 – 48.

[1575] See *Competition Commission v Bank of America Merrill Lynch International Ltd & others* 2020 (4) SA 105 (CAC) paras 36 – 44, *Director of Public Prosecutions, Western Cape v Kouwenhoven* 2021 (1) SACR 579 (WCC) para 40, M Van Staden 'A comparative analysis of common-law presumptions of statutory interpretation' (2015) 26(3) *Stellenbosch Law Review* 550 at 564 - 567, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 86 – 87. Note also sections 1, 14 and 23 of the Companies Act 71 of 2008, and specifically the definition for 'resident' in s 1of the Income Tax Act 58 of 1962.

(b) Summary of the CJEU case discussion and legal principles

Directive 95/46 and the GDPR placed their jurisdictional reach on the data subject, irrespective of whether the data is being processed within the EU or not.[1576] Hence, both Directive 95/46 and the GDPR have a limited global jurisdiction. The aim of this limited global jurisdiction is to ensure the complete protection of the data subject's rights, especially the rights to privacy and data protection.[1577] The Article 29 Data Protection Working Party (Article 29 WP)

[1576] Recital 65 and Articles 3 and 4 of Directive 95/46, and Recitals 14 and 122 and Article 3 of the GDPR, see also Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 at 10, B Van Alsenoy & M Koekkoek 'Internet and jurisdiction after *Google Spain*: The extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120, Y Poullet 'Is the general data protection regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774, M Zalnieriute '*Google LLC v. Commission nationale de l'informatique et des libertés* (*CNIL*)' (2020) 114(2) *The American Journal of International Law*' 261 – 267, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[1577] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 38. Compare with the Canadian Supreme Court in *Google Inc. v Equustek Solutions Inc Google Inc. v Equustek Solutions Inc.* 2017 SCC 34 (*Google v Equustek*) where in a "global content takedown order" was dismissed and the order against Google was upheld. This was severely criticised for a number of reasons in the academic commentary. One of the main criticisms is as follows: the CJEU held that generally the right to be forgotten can only be implemented either within a country's borders, alternatively only within the EU (or similar regional grouping). The CJEU did acknowledge that the right to be forgotten may have a wider jurisdictional reach. However, the CJEU confirmed that the EU's right to be forgotten does not generally apply extraterritorially, because not all countries have a similar right or remedy. Similarly, South African courts have confirmed that there is a presumption that South African legislative instruments do not have extraterritorial reach. Interestingly, the CJEU pointed out that if the right to be forgotten were to be applied extraterritorially, then this would need to be considered and drafted into the relevant legislation by the legislature. Although a number of jurisdictions may recognise similar intellectual property rights, not all jurisdictions recognise a right to be forgotten or a similar order (in this instance a takedown order), even if the order is only temporary. The Canadian Supreme Court focused on the EU because it recognises the right to be forgotten, thereby justifying the global approach to the takedown order. However, in the US, a Californian court summarily decided that the Canadian order was unenforceable. One of the main reasons cited by the Californian court was that the Equustek had not appeared in that court. However, the problem with the Canadian order is that it requires Google to apply the takedown in countries that have not made a similar order. Generally, for a foreign order to apply in another jurisdiction, the party seeking its enforcement must make the requisite application to that jurisdiction's courts. Although, it is generally acknowledged that data legislation may have a wider jurisdictional reach in comparison to other legislative instruments, it is still limited to the parties directly involved in the matter, and the jurisdiction in which the matter was heard, ie the jurisdictional or geographical borders of a country. Put differently, where the right to be forgotten is ordered against a foreign company that has an online presence in a specific State's jurisdiction, the order to implement the de-indexing/de-linking/de-referencing will still be limited to within that State's borders and does not impact on any other State where the company may have an online presence. See also generally, *Google LLC v CNIL* EU:C:2019:772, *Competition Commission v Bank of America Merrill Lynch International Ltd & others* 2020 (4) SA 105 (CAC) paras 36 – 44, *Director of Public Prosecutions, Western Cape v Kouwenhoven* 2021 (1) SACR 579 (WCC) para 40, M Van Staden 'A comparative analysis of common-law presumptions of statutory interpretation' (2015) 26(3) *Stellenbosch Law Review* 550 at 564 - 567, V Goswami 'Algorithms, expression and the Charter: A way forward for Canadian Courts' (2017) 7(1) *Western Journal of Legal Studies* Article 2 at 1 – 15, B Sookman 'US Court thumbs its nose at Supreme Court of Canada: *Google v. Equustek*' (2018) 30(3) *Intellectual Property Journal* 375 – 405, J Berryman 'Equity in the age of the internet: *Google Inc. v. Equustek Solutions Inc*.' (2019) 31 *Intellectual Property Journal* 311 – 326, R Diab 'Search engines and global takedown orders: *Google v Equustek* and the future of free speech online' (2020) 56(2) *Osgoode Hall Law Journal* 231 – 270, C Ryngaert & M Taylor 'The GDPR as global data protection regulation?' (2020) 114 *AJIL Unbound* 5 – 9, M Zalnieriute '*Google LLC v. Commission Nationale de l'informatique et des Libertés* (*CNIL*)' (2020) 114(2) *The American Journal of International Law*' 261 – 267, OJ Gstrein & AJ Zwitter 'Extraterritorial application of the GDPR: Promoting European values or power?' (2021) 10(3) *Internet Policy Review* 1 – 30, and V Gagrani 'The right to be forgotten:

emphasised this approach as necessary in order to protect the EU's interests extraterritorially where the need arises.[1578] Put differently, the data subject may access a website of an online store (ie a controller) within the EU that is based, for example, in the United States (US). If the data subject purchases something off that website, they will need to provide a certain amount of personal data. The controller) will need to comply with the EU data protection principles even if the personal data is processed within the US.[1579] Furthermore, both Directive 95/46 required, and the GDPR requires that a controller, where they wish to conduct business within the EU with EU citizens, must be situated within the EU's territory, especially where legal action is taken against the controller for contraventions of the relevant data protection legislation.[1580] Where the information, including personal data, is merely passing through servers situated within the EU, the EU data protection legislation will not apply. The current principles are set out in the GDPR, since the repeal of Directive 95/46.

(c) South Africa

South Africa has placed its emphasis on the activity of processing the data/information, rather than the data subject.[1581] This is emphasised in the definition of "responsible party", because they determine (whether alone or with others) the reason for the processing of personal information and how such information will be processed. Where the equipment, eg servers, computers, and any other technological tools, used to process the data/information, is situated will not determine the territorial application of POPI, put differently, is the equipment physically situated in South Africa, or in Namibia or Europe.[1582] If the information is merely

A need or a way to deviate misdeeds?' (2022) 30 *Supremo Amicus* 85. Note B Sookman 'US Court thumbs its nose at Supreme Court of Canada: *Google v. Equustek*' (2018) 30(3) *Intellectual Property Journal* 375 at 394 – 395 – provides a summary of further cases where a global right to be forgotten was ordered, including from Australia: *CG v Facebook Ireland Ltd & another* [2016] NICA 54, *Douez v Facebook Inc*. 2017 SCC 33, *Autorité des marchés financiers v. PlexCorps* 2017 QCTMF 88, *X v Y & Z* [2017] NSWSC 1214, *X v Twitter Inc* [2017] NSWSC 1300, and *Google Inc v Duffy* [2017] SASCFC 130. See also M Douglas 'The exorbitant injunction in *X v Twitter* [2017] NSWSC 1300' (2017) 36(4) *Communications Law Bulletin* 11 – 12.

[1578] Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 at 10.

[1579] Article 29 Data Protection Working Party *Opinion 8/2010 on applicable law*, adopted on 16 December 2010 at 10.

[1580] Article 4(2) of Directive 95/46. See also R Wong 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 at 232, B Van Alsenoy & M Koekkoek 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120, and L Chemlali 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

[1581] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 86 – 87.

[1582] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87 – 88.

passing through servers situated in South Africa, as that is the most convenient route for transfer, then South Africa will not have jurisdiction, similar to the EU legislation. Hence, POPI will only find application if one of the responsible parties is situated within South Africa or is a South African natural/juristic person or is using equipment that is situated within South Africa to process the personal data/information, irrespective of where they are situated.[1583]

(d) Comment

South Africa should consider making the focus more on the data subject, and not on where and by whom the personal data/information will be processed. The responsible party gains the most by transacting with the data subject, in that they receive the data subject's personal information, and depending on the transaction, a profit, eg through the sale of goods. The data subject stands to lose where their personal data/information is, even unintentionally, leaked or the safeguards breached. However, this will require a change in the legislation, aiming to make POPI more centred on the data subject, and their personal data, and not on the responsible party.

Where this is considered, s 3 of POPI would need to be amended along the lines of making the data subject, where they are a South African citizen, or where they are domiciled in South Africa, the focal point of the processing procedures and not the responsible party. This would be similar to the GDPR.[1584] This amendment would ensure better protection of a South African data subject's rights, as well as that the collection, processing, and storage of the personal data/information meets the standards as provided in POPI.

III THE RIGHT TO FORGET CRIMES AND CRIMINAL TRIALS

(a) Introduction

Once a sentence is served or the fine is paid, most people want to leave their criminal past behind them and start over, start anew, without the crime hanging over their heads. However, where the crime and subsequent trial made the headlines, especially in online platforms, combined with the internet's inability to forget, this is sometimes trickier than expected,

[1583] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87 – 88. Note the principles for interpretation in *Natal Joint Municipal Pension Fund v Endumeni Municipality* [2012] ZASCA 13 para 18, although this case dealt with the interpretation of contracts, the relevant principle was applied in *Nimble Investments (Pty) Ltd v Malan & others* [2021] ZASCA 129 para 69 for interpreting statutes.

[1584] Article 3 of the GDPR. See also E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 87 – 88.

especially where the press reports on the crime at regular intervals.

In the case discussion in Chapter 3, three aspects were highlighted, namely, first, forgetting expunged or spent criminal convictions,[1585] second, considerations of access to contemporary historical events,[1586] and, third, a family member applying for the right to be forgotten.[1587] Although some of the considerations discussed were relatively universal, these issues came about in terms of data subjects applying to have their (or a family member's) criminal convictions and sentence de-listed/de-indexed/de-referenced, ie forgotten.

(b) Summary of the EU and national high court case discussion and legal principles

Article 8(5) of Directive 95/46 and Article 10 of the GDPR provide that processing in terms of criminal investigations or convictions may be carried out only by the authorised State organ/s, alternatively by another authorised person on their behalf. Directive 95/46 provides that personal data/information may be processed during the course of criminal investigations and prosecutions, as well as after conviction, in line with the relevant legal principles, and by the relevant authority. This includes the keeping of registers in which a record is kept of who committed a specific crime, ie a sexual offenders register. Interestingly on the same day that the GDPR commenced, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (also referred to as the Law Enforcement Directive)[1588] commenced. This directive, together with the GDPR, provides for the processing of personal data in criminal matters. The Law Enforcement Directive is not discussed, as it is beyond the scope of this thesis.

Only one of the three cases extensively discussed and applied Directive 95/46, namely *NT1 & another v Google LLC & another* (*NT1*),[1589] which was heard before the GDPR was enacted. *Recht auf Vergessen I* acknowledged both Directive 95/46 and the GDPR as well as the Charter, noting that that matter had begun under Directive 95/46, but merely used Directive 95/46 and the Charter as the background during its discussions.[1590] *Recht auf Vergessen I* based its focus on the Basic Law and argued that it provided the same level of protection as the

[1585] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB).
[1586] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.
[1587] *ML v Slovakia* [2021] ECHR 821.
[1588] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[1589] See generally, *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 13, 22, 27, 29, 31 – 37, 52, 82, 85, 95, 101, 103 – 105, 107, 110 – 115, 131 – 133, 145, 147, 150, 161 – 162, 166, 170, and 223.
[1590] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.

Charter. Hence, the focus of the Bundesverfassungsgericht was on the equivalent national German legislation, and not solely a discussion on the EU legislative instruments. The ECtHR in *ML v Slovakia*[1591] focused on the various rights involved, not just that of the son, but also that of the family, and whether the family may apply for the information to be de-indexed/de-listed/de-referenced.

In all three judgments the courts, irrespective of the national courts of the UK[1592] or Germany[1593] or the ECtHR,[1594] faced the same issue, namely that all of the data subjects wanted their past criminal convictions and sentences to be removed or de-indexed/de-listed/de-referenced (ie forgotten) from online archives. In all three cases the courts emphasised that the relevant rights, freedoms and interests of the parties involved must be balanced to find a fair outcome in light of the circumstances before them.[1595]

The three cases emphasised the passage/effluxion of time as an important factor.[1596] Further considerations included, whether or not the crime was expunged (spent), alternatively whether the data subject had served their sentence, and whether they had lived crime free.[1597] Rehabilitation and re-integration were also considered important; the data subjects should be able to form new acquaintances without their past being constantly brought up.[1598] A further consideration was whether the data subjects brought attention to their plight.[1599]

The courts also pointed out that de-indexed/de-listed/de-referenced the unwanted links to the names of the data subject is a less restrictive method in comparison to complete removal – especially since certain crimes form a part of a country's contemporary history.[1600] In all

[1591] *ML v Slovakia* [2021] ECHR 821
[1592] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB)
[1593] BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*.
[1594] *ML v Slovakia* [2021] ECHR 821.
[1595] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I.*
[1596] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I, GC AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773 and *ML v Slovakia [2021] ECHR 821*.
[1597] *NT1 & another v Google LLC & another r* [2018] EWHC 799 (QB), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I, Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), *ML v Slovakia* [2021] ECHR 821, and *Biancardi v Italy* [2021] ECHR 972.
[1598] *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB), BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I, Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), and *Biancardi v Italy* [2021] ECHR 972.
[1599] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), and BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I.*
[1600] *GC & others v CNIL* EU:C:2019:773, BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I*, and *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22

three cases, the courts ordered that the links on the results page be de-indexed/de-listed/de-referenced where the name of the former accused was used as the search terms in order to obtain the information.

(c) South Africa

In light of criminal records, the stigma within communities remains. However, that does not mean that a data subject should not be able to start again. With regards to the issue of whether criminal records may be "forgotten" ie de-indexed/de-listed/de-referenced, POPI provides some initial guidance. In terms of s 6(1)*(c)*(ii) of POPI does not apply to public bodies where personal data /information is processed for the purposes of preventing, detecting, identifying what has amounted to the unlawful proceeds of crime (such as money laundering), investigating offences generally, prosecuting offenders, as well as executing sentences, and in light of security measures.

In terms of s 26(2) of POPI, there is a general prohibition that responsible parties may not process data/information relating to criminal behaviour. In terms of the criminal behaviour of the data subject the data/information includes, the offence, and the subsequent result of the trial, ie whether the data subject was sentenced to a period of imprisonment, or was fined, or was acquitted. However, s 26(2) of POPI must be read with sections 27(1)*(f)* and 33. Section 27(1)*(f)* states that the prohibition in s 26(2) will not apply where the data/information is processed in compliance with sections 28 – 33 of POPI.[1601] For the purposes of this discussion, s 33 provides that the prohibition on processing of the data subject's criminal behaviour does "not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law", ie those involved in the investigation, prosecution and subsequently the correctional service authorities.[1602] Section 33 to an extent mirrors s 6(1)*(c)*(ii), detailed above.

June 2021) – see the separate dissenting opinion of Pavali J.

[1601] Section 33 of POPI provides for the authorisation for the processing of the data subject's criminal behaviour and biometric information. Biometric information is used in criminal investigations and often forms a part of the evidence, this includes fingerprints, DNA samples as well as any other physical features that form a part of the identity of the data subject, see M Smith & S Miller *Biometric Identification, Law and Ethics* (2021) at 1 – 3. See P Mzila 'Protection of personal information in South Africa: A framework for biometric data collection security' In *Proceedings of INTERNET 2016: The Eighth International Conference on Evolving Internet* (13 – 17 November 2016, Barcelona, Spain) 1 – 6 for a discussion involving biometric information collection in light of POPI.

[1602] Criminal Procedure Act 51 of 1977 is the main piece of legislation that governs criminal proceedings, it includes sections dealing with investigations, but also the presentation of evidence in court. Note that in respect of child offenders the Child Justice Act 75 of 2008 is the legislative instrument that governs criminal proceedings as well as the possible sentences that child offenders, where they are found guilty, may receive.

An important legislative instrument which provides for the collection and presentation of information for criminal trials, as well as controls both the keeping of registers and the expungement of criminal records, is the Criminal Procedure Act 55 of 1977.[1603] The Criminal Procedure Act provides for imprisonment, suspension of imprisonment sentences which are connected to community service initiatives, as well as fines. These initiatives are designed to encourage offenders (ie data subjects) to rehabilitate and not commit a crime again. There are also correctional service facilities that assist in rehabilitating offenders, where these receive a sentence of imprisonment.[1604]

In relation to the expungement of criminal records, certain previous convictions will no longer be relevant during the sentencing phase of a trial after a period of 10 years, they are automatically expunged, provided the person has lived crime free.[1605] Sexual offences, including the keeping of a public register of sexual offenders, are specifically dealt with in the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007. The Criminal Law (Sexual Offences and Related Matters) Amendment Act provides what must be recorded in the register, and further matters pertaining thereto.

Especially in light of the balancing of respective rights, the data subject's privacy and their interest to be fully rehabilitated into society will be balanced against the public's right to know. A very important consideration is how the matters were reported on – if the news amounts to gossip, not only may the data subject have a claim based in defamation, but the information will most likely be de-linked.[1606] Although the press may claim that the public has a right to know, this will be balanced against how the content of the article was written.[1607] The press, or any individual, cannot hide behind a press statement that clearly amounts to a defamatory remark.[1608] Journalists must show respect towards those that they are reporting on, and reports must be factual.[1609] The South African Constitutional Court pointed out that

[1603] See also the Expungement of Criminal Records GN 513, *GG* 32205 of 6 May 2009.
[1604] In relation to children, see the Child Justice Act 75 of 2008. Furthermore, *Centre for Child Law & others v Media 24 Ltd* 2020 (4) SA 319 (CC) requires that the names and identities of child victims, witnesses and offenders are not disclosed where these are involved in criminal matters – see also the amendments to s 154(3) of the Criminal Procedure Act 51 of 1977.
[1605] Section 217A of the Criminal Procedure Act 51 of 1977. Note s 217B provides that those convicted of sexual offences may not have their criminal records expunged, unless they have had their names removed from the national register of sexual offenders in terms of s 51 of the Criminal Procedure Act. Note, murder, although categorised as a serious offence is treated the same as other minor offences – see *The Citizen 1978 (Pty) Ltd & others v McBride* 2011 (4) SA 191 (CC) paras 69 – 72.
[1606] See *NT1 & another v Google LLC & another* [2018] EWHC 799 (QB) paras 82 – 87.
[1607] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).
[1608] *EFF & others v Manuel* [2020] ZASCA 172.
[1609] *Khumalo & others v Holomisa* 2002 (5) SA 401 (CC).

although records are expunged, that does not affect the truthfulness of the published statements, and certainly does not erase history.[1610]

(d) Comment

South African law caters for instances where the data subject's right to privacy is balanced against either the press or the general public's right to freedom of expression and information. South Africa, similarly to the EU, provides for the expungement of criminal records (whether automatically after a lapse of time or on application). This will be one of the guiding factors as to whether the information should be forgotten or not. Furthermore, has the data subject served their sentence and lived crime free since leaving prison, put differently, rehabilitation and re-integration into society are further important considerations.[1611] The data subject should not unnecessarily be held back by their past, especially where the rights of the data subject are found to outweigh the rights of the general public. Where the press randomly draws unwanted attention to the data subject, and the reports or articles are laced with gossip, the courts should not hesitate to either apply the right to be forgotten, ie to de-index/de-list/de-reference the information, alternatively, and depending on the complete circumstances of the matter before the court, the anonymisation or the complete removal of the information. It will also depend on what would amount to the best protection of the data subject's rights. These remedies are available over and above the civil compensation remedies (such as defamation) within the South African legal system.

Regarding the prohibition on the processing of criminal behaviour, as provided for in POPI, Directive 95/46 and the GDPR – the provisions are similar because it has been generally accepted that the criminal behaviour of a data subject will require specific safeguards during the processing of their personal information, and that these must be provided by the relevant authorities tasked with the investigation, prosecution and those equipped to deal with the sentence received by the data subject at the end of the trial. In light hereof, it is submitted, that South Africa has followed the standards currently being applied in Europe.[1612]

[1610] *The Citizen 1978 (Pty) Ltd & others v McBride* 2011 (4) SA 191 (CC) para 69 – 72. Note also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* paras 109 – 115, and 148.

[1611] Note, the South African sentencing regime places an emphasis, depending on the age of the data subject (accused at the trial) and the seriousness of the crime, and the needs of society, on mercy towards an accused. See *S v Zinn* 1969 (2) SA 537 (A), *S v V* 1972(3) SA 611 (AD) at 614 and *S v Rabie* 1975 (4) SA 855 (AD) at 862G-H. Note, that where there is a prescribed minimum sentence, mercy in conjunction with all the factors considered to be substantial and compelling circumstances, will be taken into account – see *S v Malgas* 2001 (1) SACR 469 (SCA). However, this discussion is beyond the scope of the thesis.

[1612] SALRC Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005) para 3.7.2, Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 83 – 99 and E De Stadler,

In this instance, apart from a few extra considerations, eg living crime free, South African law is well equipped to protect, and balance, the various rights and freedoms that will be affected by a request to de-index/de-list/de-reference the past criminal activities of the data subject.

IV STATEMENTS, ETC. MADE IN A PROFESSIONAL CAPACITY

(a) Introduction

During an individual's career, depending on the functions that form a part of their employment, an individual may agree to make a statement on behalf of their employer. Put differently, the employee, where this is a part of their duties, will be making statements in their professional capacity on behalf of their employer. The issue in this instance is whether such statements may be forgotten, even where they form a part of a current public debate, because the individual who had made those statements no longer wants to be associated with them, as this may minimise their chances of finding other employment.

(b) Summary of the German case discussion and legal principles

The Bundesverfassungsgericht in *Recht auf Vergessen II* held, in a situation similar to this, that the relevant rights, freedoms and interests of all persons affected will need to be weighed against each other, before a decision may be made.[1613] Instead of focussing on Germany's data protection legislation, the Bundesverfassungsgericht made their decision based on the rights and freedoms protected within the Charter.[1614] All rights within the Charter are accorded equal value. The rights of the complainant (or the data subject or individual or employee) will be balanced against those of the content providers.[1615]

In *Recht auf Vergessen II*, the data subject had approached the courts to request that the

---

IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 207 – 215.

[1613] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 141, note also the discussion in para 63ffg and later summarised in para 121. See also See also BVerfG, Beschluss des Ersten Senats vom 06.11.2019 – 1 BvR 16/13 – *Recht auf Vergessen I* para 170, *Von Hannover v. Germany (no. 2)* [2012] ECHR 228, *Węgrzynowski and Smolczewski v Poland* (European Court of Human Rights) application no. 33846/07 (16 July 2013) para 56, and *Delfi AS v Estonia* [2015] ECHR 586 (for a comment on *Delfi AS v Estonia* see N Cox, '*Delfi v. Estonia*: Privacy protection and chilling effect', VerfBlog, 2015/6/19, *https://verfassungsblog.de/delfi-v-estonia-privacy-protection-and-chilling-effect/* (Accessed: 18 July 2022)).

[1614] Charter of Fundamental Rights of the European Union (2012/C 326/02).

[1615] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 120 – 122 and 141. See also *Fuchsmann v Germany* [2017] ECHR 925 para 32ffg. See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 266 – 267.

search engine remove the link to an interview that she gave in her professional capacity. The rights in this instance were the data subject's right to privacy (Article 7) and protection of personal data (Article 8) as set out in the Charter, and the search engine's right to pursue its business interests (Article 16).[1616] The Bundesverfassungsgericht emphasised that the rights of the unspecified public to information and the rights of the content providers to freedom of expression (especially since this was a media company) must also be included as they are often the most affected by a de-indexing/de-listing/de-referencing request, but also the data subject's right to free expression was included in the balancing exercise.[1617] Likewise, the search engine had a right to conduct its business that was specific to the German market.[1618] The passage of time was also a factor, as well as the continued interest and relevance of the topic of the interview.[1619] The Bundesverfassungsgericht held that the time between the interview and the date of judgment was seven years – this was not a long period of time to conclude that such information had become private, especially in light of the interest that it still had within German society. The data subject, too, had a right to freedom of expression, which could not be overlooked. The data subject had consented to the interview. In light of these factors, the application was dismissed.[1620]

(c) South Africa

Recht auf Vergessen II focused on the rights and freedoms as provided in the Charter. These were the right to privacy and data protection, as provided for in Articles 7 and 8, respectively, as well as the right to freedom of expression (Article 11) and the right of the search engine to conduct a business (Article 16). In terms of the South African Constitution, the right to privacy is protected in s 14, s 16 provides for the right to freedom of expression and information, and s 22 specifies that persons have the right to freedom of trade, occupation and profession.[1621]

[1616] CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.

[1617] The right to freedom of expression and information is found in Article 11 of the Charter. BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 120 – 122 and 141. See also *Fuchsmann v Germany* [2017] ECHR 925 para 32ffg. See also CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 266 – 267.

[1618] Article 16 of the Charter.

[1619] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 134, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.

[1620] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 134, 141 – 142, and CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 267 – 268.

[1621] Section 22 of the Constitution reads as follows: "Every citizen has the right to choose their trade, occupation or profession freely. The practice of a trade, occupation or profession may be regulated by law."

In South Africa, a data subject may over the period of their employment, depending on the duties that are a part of their work, make certain public statements on behalf of their employer. The work that the data subject does may be in marketing, or public relations, and inevitably they may be called upon to deal with queries from the press.

The issue that will arise is where the interview or statement that was made regarding an employer's particular employment practice or policy that the employee no longer wishes to be associated with, especially where they wish to obtain new employment. The question is: will the data subject be able to have the information de-indexed/de-listed/de-referenced? And further, what are the considerations that will guide the South African courts in such a request?

In terms of *Bernstein v Bester*,[1622] the Constitutional Court provided that privacy exists along a continuum.[1623] In terms of the continuum, there will be aspects of an individual's life that they wish to keep private, as these are found in the truly intimate sphere; however, the more an individual interacts with third parties outside of that intimate sphere, the less likely privacy will find application.

In light of the facts of *Recht auf Vergessen II*, the data subject made the comments in an interview on behalf of their employer within their official capacity. Where a data subject acts within their official capacity, they are interacting within the public sphere, and are, based on the principles of *Bernstein v Bester*,[1624] unable to claim that privacy will find application. *Bernstein v Bester*[1625] pointed out that those who are actively involved with the affairs of a company cannot expect that their actions will not be criticised by the press.[1626] It is submitted, that this will include where they are merely airing the companies' position, even if the data subject does not agree with same. The statements may affect the data subject's social sphere, but they do not affect the data subject's private sphere. These considerations are echoed where the employee has a legitimate expectation of privacy – certainly for their completely private affairs, but not in terms of the affairs of the company, especially where the data subject consents to the interview.[1627] It is only within the inner sanctum where a true expectation of privacy may

[1622] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC).
[1623] See the discussion in Chapter 4 – all three aspects have been fully elaborated and discussed in terms of the South African case law.
[1624] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC).
[1625] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC).
[1626] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC) para 74. Note this discussion does not include vicarious liability of an employer for the actions of an employee, whilst the employee is performing a duty in terms of their employment, for a discussion on vicarious liability and POPI see D Millard & EG Bascerano 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *Potchefstroom Electronic Law Review* 1 – 38.
[1627] Note the arguments of the SCA in *Smuts & another v Botha* [2022] ZASCA 3.

be expected.[1628] The data subject in consenting to defend the company on a topical issue must be prepared to receive the criticism, where this is fair, in light of the debate within society.[1629]

Further considerations such as the continued interest in the topic, as well as the passage of time will be contemplated by the court hearing the matter. The continued interest of a specific topic, such as employment practices by various companies, is something that often interests society as a collective.[1630] Employees generally want to work for companies where their needs and interests are also of concern to the company and not merely the amount of work that each employee produces for their salary. The topic may determine whether the passage of time will play a role or not – it may be that certain topics will remain for longer periods in the public debate compared with others. Those that are contentious, and only for a short period of time, may well be forgotten quicker, such as the identity of a witness in a high-profile trial, whose identity does not add to the public debate.[1631] By comparison, chief executive officers that make statements in terms of the companies that they work for, their names, in light of the statements and circumstances may remain in the public debate, and those statements will not be de-index/de-list/de-reference in searches where their names are the search terms used. Employees, especially chief executive officers, and public relations or marketing managers, and sales personal, are often considered to be the "face of the company".[1632] Lastly, the data subject has a right to freedom of expression, and by consenting to the interview, or to make the

[1628] *Bernstein & others v Bester NNO & others* 1996 (2) SA 751 (CC).
[1629] Compare with *Smuts & another v Botha* [2022] ZASCA 3.
[1630] Compare with *Smuts & another v Botha* [2022] ZASCA 3.
[1631] Note, in defamation cases, see especially the considerations set out in *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) regarding the defence of truth and public interest, one of the defences that the "wrongfulness of a defendant's conduct will be rebutted if he or she proves that the defamatory remarks are true and in the public interest". The defendant is required to ensure that the comments are substantially true and not literally true, put differently that "the sting of the charge is true". What this amounts to will depend on "the time, the manner and the occasion of the publication", as well as the convictions of the community. Recent comments of possible defamatory statements are not excluded from the defence of truth and public interest (See *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) paras 41 – 42; *EFF & others v Manuel* [2020] ZASCA 172 para 37; *Independent Newspapers Holdings Ltd & others v Suliman* [2004] 3 All SA 137 (SCA) para 47 and *Kemp & another v Republican Press (Pty) Ltd* 1994 (4) SA 261 (E) at 265B – F). In light of the defence of fair comment, Davis J added that an obvious wrongful publication may be rebutted where the defendant proves that the publication amounts to fair comment, or the facts are true and in the public interest. For this rebuttal the following four factors are considered: The defamatory statement (1) amounts to a comment and not to a mere "assertion of an independent fact"; (2) the statement must be fair; (3) the facts on which it is based are true; and (4) it is indeed in the public interest (*Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 43; *EFF & others v Manuel* [2020] ZASCA 172 para 38). It is likely that similar considerations are possible in cases where the statements that are made by the data subject form a part of the public debate, and due to this, will mean that the information/data will remain "completely" available, ie the data subject's name will not be de-linked/de-referenced from the information.
[1632] KL Keller & K Richey 'The importance of corporate brand personality traits to a successful 21st century business' (2006) 14 *Journal of Brand Management* 74 at 81, and N Denner, N Heitzler & T Koch 'Presentation of CEOs in the media: A framing analysis' (2018) 33(3) *European Journal of Communication* 271 at 273.

statement on behalf of the company, they are exercising their right to freedom of expression, which, in light of a democratic society, is a valuable right.

(d) Comment

It is likely that in terms of both jurisdictions, based on the facts of *Recht auf Vergessen II*, the data subject will be unable to have the information de-index/de-list/de-reference. The considerations in each jurisdiction are fairly similar, although the approaches may be different. In South Africa, emphasis will most likely be placed on how privacy operates on a continuum – the more the person interacts with society, the less likely will the right to privacy be applicable. Where a person acts solely in their professional capacity, their interactions will most likely be placed on that part of the continuum that is within the public sphere, and where privacy will find very little, if any, application. In both instances, it is not merely the public's right to information that is an important consideration, but also the data subject's right to freedom of expression – especially where such expression is voluntary and the data subject has consented to the interview, as this is a part of their official duties.

Content providers, especially news outlets and particularly those news outlets that conducted the interview and host the content on their webpages, have a right to freedom of expression, specifically the freedom to impart information. This forms an important aspect when considering whether such information should remain accessible, or not. In circumstances where the information forms a part of the current public debate, such employment practices in companies, the scales may tip in favour of having the information permanently available, with the ability to find it using any keyword, including the data subject's name, and the information should not be de-index/de-list/de-reference.

However, it is not only the data subject's rights to privacy and freedom of expression, and the public's right to information that are important to weigh up. Search engines' have a right to trade, and this is another further important consideration in the balancing exercise. Search engines are data driven, which means that they use data/information (including personal data/information) to make a profit, it is the base of their business model. In such instances, the business interests of a company are usually outweighed by the privacy of the data subject (ie the employee).[1633] However, where the information is found within the public domain, and

[1633] BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* para 105, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317, and *GC & others v CNIL* EU:C:2019:773 para 85.

remains connected (ie indexed/linked/referenced) to the data subject's name, the search engine will be able to use the data/information to further its business interests, generally in the form of advertising space, based on searches conducted by an internet user looking for that information.

This last-mentioned consideration, when deciding whether the right to be forgotten is applicable, is a newer consideration when a court balances the data subject's (ie employee's) right to privacy against the content provider and the general public's right to freedom of expression and information. Generally, the right of a search engine to trade, is not found in this specific balancing mix.[1634] The South African courts are able to use *Recht auf Vergessen II* as suitable guidance for that debate.

V PROCESSING SPECIAL CATEGORIES OF DATA/INFORMATION

(a) Introduction

Special data/information, sometimes referred to as sensitive data/information, is a category of data/information that refers to "religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, or biometric information", and includes the data subject's criminal record, and civil judgments (eg sequestration).[1635] Most individuals do not want their special or sensitive data/information divulged. Hence, the data protection legislative instruments in Europe and South Africa all contain specific provisions that deal with the processing thereof. In Europe it is referred to as special data/information and in South Africa as special personal information. Nothing turns on the different terms, they refer to the same type of data/information.

(b) Summary of the CJEU case discussion and legal principles

The processing of special data/information was dealt with in *GC & others v CNIL*.[1636] In this case, the court had to consider three key issues. First, the duties of search engine operators and/or controllers in terms of Directive 95/46 (and subsequently the GDPR); second, de-linking/de-referencing/de-listing in light of the legislative exceptions; and third, displaying

[1634] Generally, the rights to privacy and freedom of expression and information will be the concern of the balancing exercise. The concept that the right to privacy will outweigh the economic interests of search engine providers (and possibly companies or organisations in general), is fairly new in terms of South African constitutional law.
[1635] Section 26 of POPI, see also Article 8 of Directive 95/46 and Article 9 of the GDPR.
[1636] *GC AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773. ED's matter was covered in the section on forgetting in criminal matter, discussed above.

links in chronological order.

Article 8(1) of Directive 95/46 states that it is prohibited to process special data/information that "reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of data/information concerning health or sex life."[1637] Article 8(2) provided for exceptions to the prohibition against the processing of special data/information.[1638]

The facts stemmed from four separate applications that were combined into one matter, for a preliminary hearing at the CJEU. Briefly, in the first application, GC was a candidate campaigning to be elected as the mayor of a town in France. During the campaign, a photomontage was uploaded onto YouTube which falsely depicted GC as having an affair with the previous mayor with whom she had worked. GC claimed that the montage had negatively impacted her career.[1639] In the second application, AF was a former employee of the Church of Scientology. During the course of his employment, AF liaised with the media with regard to a suicide committed by one of the Church's members and his comments appeared in the press. After AF left the Church, he no longer wished to be associated with it.[1640] In the third application, BH was implicated with other businessmen and politicians in a political party funding scandal. BH was charged with various offences related to the scandal, but was acquitted at the end of the trial. The trial was reported in the press, but these reports did not

[1637] *GC & others v CNIL* EU:C:2019:773 para 39. Article 9 of the GDPR is worded as follows:

> "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

[1638] *GC & others v CNIL* EU:C:2019:773 para 41. Note Article 8 was incorporated into the GDPR, with some variations as Articles 9 and 10. The relevant parts of Article 8(2) of Directive 95/46 read as follows:

> "2. Paragraph 1 shall not apply where:
>
> *(a)* the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
>
> . . .
>
> *(e)* the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
>
> . . .
>
> 5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
>
> Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority."

[1639] *GC & others v CNIL* EU:C:2019:773 para 25.

[1640] *GC & others v CNIL* EU:C:2019:773 para 26.

reflect the final outcome for BH.[1641] In the last application, ED, like BH, wanted links to articles in the press regarding his criminal conviction and sentence for sexual offences of minors be forgotten, especially since one of the articles reported on delicate details about ED that had been revealed during the trial.[1642]

The first issue that arose before the CJEU was what are the duties of and how should search engines comply with Article 8 of Directive 95/46 where content that has been indexed was obtained and processed from a third-party website. The CJEU answered this issue by stating that search engine operators (as well as controllers) must comply with Directive 95/46 and the GDPR. Data/information, as the CJEU pointed out in *Google Spain*, does become incompatible of over time, and, consequently, search engine operators must de-list or de-reference a data subject's name from the search results, where the data subject's name is used as the search term. The reason for the de-listing or de-referencing is based on the fundamental right to privacy and personal data/information. The CJEU held that in terms of Article 8, search engine operators may not process sensitive (special) data/information, longer than is necessary, even where this is contained on a third-party website.[1643] The CJEU emphasised that those who are involved with the processing of personal data/information, ie controllers and operators of search engines, must adhere to the prohibitions and restrictions in terms of both Directive 95/46 and the GDPR.[1644]

The second issue dealt with the processing of personal data/information, specifically special data, in light of de-indexing/de-listing/de-referencing and exceptions. The issue had three parts to it. First, in light of the exceptions, must operators of search engines de-index/de-list/de-reference webpages that contain personal data/information which is covered by the provisions of Article 8(1) and (5)? Second, this had a further two sub-questions: (a) how must Article 8(2)*(a)* and *(e)* be interpreted in light of the responsibilities, powers and capabilities of the operator? And (b), may an operator refuse to carry out a de-indexing/de-listing/de-referencing request where the data/information on the third-party's website falls under Article 8(1), but is included in the exceptions under Article 8(2)*(a)* and *(e)*? Third, if the data/information was published in light of the journalistic exceptions contained in Article 9, would the search engine operator be able to refuse the de-linking request, in terms of

[1641] *GC & others v CNIL* EU:C:2019:773 para 27.
[1642] *GC & others v CNIL* EU:C:2019:773 para 28.
[1643] *GC & others v CNIL* EU:C:2019:773 paras 46 – 47.
[1644] *GC & others v CNIL* EU:C:2019:773 para 42.

Article 9?[1645]

In light of the issues raised, the CJEU held, first the operator must accede to the de-linking request, as provided for generally in Article 8 of Directive 95/46, in light of the relevant exceptions.[1646] Second, if the data/inforamtion to be de-indexed/de-listed/de-referenced falls into one of the exceptions in Article 8(2), the search engine operator/controller may refuse the de-indexing/de-listing/de-referencing request, provided that the refusal "satisfies all the other conditions of lawfulness" in terms of Directive 95/46. However, if the data subject has rights and interests that are protected in terms of Article 14 of Directive 95/46, they may still object to the processing of their personal data/information, depending on their personal circumstances, in terms of that Article.[1647] Third, the CJEU held, depending on the facts of each matter, that the operator of a search engine must, where there is an application to de-index/de-list/de-reference, take into account the impact that the continued processing has on the data subject's rights to privacy and data protection, against the general public's right to information and expression, in order to decide if the link is strictly necessary on the results page, where the data subject's name is the keyword.[1648]

The CJEU emphasised its earlier judgment in *Google Spain*, that in terms of Articles 12*(b)* and 14*(a)* of Directive 95/46, an operator must comply with the de-indexing/de-listing/de-referencing, requests, even if the data is not, or only later, or simultaneously removed by the third party. This, in terms of the right to be forgotten includes lawfully published information.[1649]

(c) South Africa

The preamble to POPI highlights that the constitutional "right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information". This means that all mentioned role players in POPI, namely, data subjects, responsible parties, operators, Information Officers and the Information Regulator, must apply

[1645] *GC & others v CNIL* EU:C:2019:773 para 31.
[1646] *GC & others v CNIL* EU:C:2019:773 para 69.
[1647] *GC & others v CNIL* EU:C:2019:773 para 69.
[1648] *GC & others v CNIL* EU:C:2019:773 para 69. See also Articles 7 (privacy), 8 (data protection) and 11 (freedom of expression and information) of the Charter.
[1649] *GC & others v CNIL* EU:C:2019:773 para 52, *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 88. Note *GC v CNIL* in paras 54 – 55 stated as follows with regard to Article 17 of the GDPR, (ie "The right to erasure (right to be forgotten"), as with the combined Articles 12*(b)* and 14*(a)* of Directive 95/46, provides that data may only be published for as long as it is strictly necessary, and thereafter the controller must remove same, without due delay.

POPI, bearing in mind the need to protect the privacy of data subject.

The processing of sensitive data/information is provided for in Part B of Chapter 3 in POPI.[1650] Section 26, defines what is "special personal information",[1651] as well as prohibiting the processing thereof, unless one of the exceptions provided for in s 27 is applicable. Section 27 of POPI[1652] allows for special personal data/information to be processed where the responsible party has obtained the data subject's consent to the processing;[1653] the data subject has deliberately made the data/information public;[1654] the processing is necessary to establish, exercise or defend a legal right or obligation;[1655] the processing is necessary to comply with an international law obligation;[1656] or the processing is necessary for historical, statistical or research purposes, but only to the extent that the purpose serves a public interest or it is impossible or very difficult to obtain consent to process the data/information.[1657]

Special personal data/information may be processed where the responsible party has applied for prior authorisation from the Information Regulator. Alternatively, the Information Regulator may, grant a responsible party prior authorisation through the *Government Gazette*.[1658]

Briefly, as mentioned in Chapter 5, special personal data/information is divided into broad categories, in sections 28 to 33 of POPI, which grant prior authorisation for the processing of the special personal data/information. In light of the facts of *GC & others* the relevant categories are as follows:[1659] First, in relation to GC, her political persuasion/relationship status;[1660] second, in relation to AF, his religious and philosophical beliefs;[1661] and, third, in relation to BH and ED, their criminal behaviour.[1662]

In respect of the processing of special personal data/information, the data subject must give their prior consent thereto, unless one of the further exceptions in s 27 applies.

[1650] Sections 26 – 33 of POPI.
[1651] See the introduction to this section for what amounts to special personal information in terms of POPI.
[1652] These principles are restated for ease of reference.
[1653] Section 27(1)*(a)* of POPI.
[1654] Section 27(1)*(e)* of POPI. Compare with *Smuts & another v Botha* [2022] ZASCA 3 paras 8, 9, 18, 19, 20 and 31.
[1655] Section 27(1)*(b)* of POPI.
[1656] Section 27(1)*(c)* of POPI.
[1657] Section 27(1)*(d)* of POPI.
[1658] Section 27(1)*(f)* of POPI.
[1659] The other categories are in sections 29 (race of ethnic origin of the data subject); 30 (the data subject's trade union membership) and 32 (the data subject's health or sex life).
[1660] Section 31 of POPI.
[1661] Section 28 of POPI.
[1662] Section 33 of POPI. Section 33 also includes the biometric information of the data subject.

Furthermore, this data/information is generally processed by the administrative structures of the organisations to which the data subject is a member, or where they further the aims of the organisation. Again, in light of the facts of *GC & others*, GC was a part of a political party and her personal data/information would have been processed as a result of her participation in an electoral campaign; AF was a member of a religious or philosophical group and his personal data/information would have been processed as a result of his membership of the Church; and BH's criminal investigation, trial and the subsequent outcome, in terms of POPI, it was an accused person in a criminal trial and his personal data/information would have been processed by the police (or any specific investigating unit), the prosecution, and the court staff. ED was also an accused person in a criminal trial and his personal data/information would have been processed for the same reasons as that of BH.

GC's matter was somewhat unique. She and the previous mayor had worked closely together after he was first elected to the position of mayor. Following his term of office, GC was selected as her party's candidate for election to the position of mayor. The montage, which was posted on YouTube during GC's campaign, depicted her and the previous mayor in such a way that it suggested that they were having an affair. GC claimed that this montage ruined her political career. The persons with whom individuals have relationships, be they friendship or more intimate, is certainly personal information in terms of POPI. While a data subject's sex life is listed as a special personal data/information, together with health,[1663] a data subject's other relationships are not. However, this does not mean that such information falls outside of the category of sensitive or special personal data/information. Data/information about the persons with whom one has a relationship, especially an intimate relationship, should not be processed, unless there is a lawful justification for doing so. The processing of personal data/information that involves personal relationships should be processed only where the data subject has given their consent. The montage, according to GC, was not true. Depicting an individual in relationship with another, has the ability to ruin their credibility and reputation. In such a circumstance, the individual may have a claim for damages in terms the principles of defamation.

Special personal data/information is not automatically de-indexed/de-linked/de-referenced from online databases, where this is discovered. This means that a data subject will need to make the relevant request in terms sections 11(3) and 24(1) of POPI, to have the special

[1663] Section 32 of POPI.

personal data/information "forgotten".[1664]

(d) Comment

Both Article 8 of Directive 95/46 and s 26 of POPI advance a comparable definition of special personal information or sensitive data. However, POPI has taken this a step further in providing certain prior authorisations, as described above, for specific organisations to process special personal information or sensitive data/information, where the data/information is needed to further the aims of the organisation or alternatively where the data subject is member of the organisation. Article 8(2) of Directive 95/46[1665] and s 27 of POPI both list exceptions to the general rule that special personal information or sensitive data is not to be processed.

In light of the responsibilities of search engines as responsible parties, this means that they may not process special personal information or sensitive data that is found on a third-party website, unless one of the exceptions apply or the necessary prior authorisations have been received either from the data protection authorities or from the legislative instruments. However, this will generally not be the case, as an authorisation, especially a prior authorisation, is generally given specifically to an organisation that is going to use the special personal information or sensitive data to further its aims, such as a political party campaigning during an election. Search engines may process the special personal information or sensitive data where they have received the necessary consent from the data subject, but this will be unlikely, as a request would need to be made to every individual, who is a potential data subject, possibly world-wide, and this, as rightly pointed out by the CJEU in *GC & others*, is impossible.

Responsible parties in terms of POPI, like controllers in terms of Directive 95/46, must comply where special personal data/information has been processed, and the data subject objects thereto. Even though special personal data/information may not be processed, unless there is prior authorisation or the data subject has given their explicit consent, search engines with the use of their algorithms,[1666] will automatically process the data/information, irrespective of whether one of these two grounds to justify the processing is present. The data subject will need to, based on their personal circumstances, explain why the information must be de-indexed/de-listed/de-referenced. Only thereafter will the information be de-indexed/de-

[1664] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 paras 87 – 88.
[1665] See Articles 9 and 10 of the GDPR.
[1666] P De Hert & V Papakonstantinou '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 at 627.

listed/de-referenced, alternatively, deleted. The reason is because, as stated above, search engines, as responsible parties, must adhere to the requisites of POPI (as well as Directive 95/46), which is aimed at the protection of the right to privacy, and this includes the protection of personal data/information. The fact that the data subject objects, is an important factor to prove that they no longer wish search engines to process their data.

VI ANONYMISATION OR DELETION OF ARCHIVES

(a) Introduction

This discussion went to the heart of the right to freedom of expression, especially press freedom. Although it was argued, in the ECtHR as one of their functions, the press maintains and provides access to reports recording contemporary history, and makes these reports available to interested members of the public through their archives, both online and offline. These archives serve as a vital collective memory for society.[1667] The courts in South Africa and Europe (including the EU) have emphasised the important functions that both the rights to privacy and freedom of expression play within democratic societies. Privacy allows for the development of self and the protection of a person's reputation. Freedom of expression, in which is included the right to receive and impart information, allows society to remain informed. Striking a balance between these two rights is never easy, especially where the media or press are involved. The cases discussed in Chapter 3 under this heading detailing the CJEU and ECtHR approaches, as well as the discussion in Chapter 4, which covers in detail the South African approach to balance these two rights, affirms this fact.

(b) Summary of the ECtHR case discussions and legal principles

The three European judgments all originated from the ECtHR, namely *ML & WW v Germany* (*ML & WW*),[1668] *Hurbain v Belgium* (*Hurbain*)[1669] and *Biancardi v Italy* (*Biancardi*).[1670] In each of these three cases, the European Court had to decide whether merely applying the right to be forgotten, ie de-indexing/de-linking/de-referencing, would be sufficient, or was the impact on the rights of the data subject so great that anonymisation or deletion was the only

[1667] *Hurbain v Belgium* [2023] ECHR 948 para 182 (see also para 26 of Ranzoni J's dissenting opinion).
[1668] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).
[1669] *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021), this is a judgment from the ECtHR's Third Chamber, which was upheld by the Grand Chamber in *Hurbain v Belgium* [2023] ECHR 948.
[1670] *Biancardi v Italy* [2021] ECHR 972.

alternative available to protect the infringed rights.

The main principles from the three cases were the balancing of the relevant rights, freedoms and interests of all parties involved.[1671] In this instance, the rights under consideration were Article 8 (the right to respect for private and family life) and Article 10 (freedom of expression) in the European Convention on Human Rights (Convention).[1672] The ECtHR also considered the interests of internet users during the balancing exercise. The ECtHR's Grand Chamber in *Hurbain*[1673] summarised the main factors to be considered in an application where a data subject or individual claims the right to be forgotten as follows:[1674]

> "(i) the nature of the archived information; (ii) the time that has elapsed since the events and since the initial and online publication; (iii) the contemporary interest of the information; (iv) whether the person claiming entitlement to be forgotten is well known and his or her conduct since the events; (v) the negative repercussions of the continued availability of the information online; (vi) the degree of accessibility of the information in the digital archives; and (vii) the impact of the measure on freedom of expression and more specifically on freedom of the press."

One factor mentioned by the Chamber Courts of the ECtHR, which was cited, although not directly applied, by the Grand Chamber, was that individuals cannot claim privacy and protection of their personality rights, including the loss of reputation, where the damage is as a result of their own behaviour or actions.[1675]

[1671] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 87 – 88, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 93, 101 – 103, *Hurbain v Belgium* [2023] ECHR 948 paras 105, 219 – 257, and *Biancardi v Italy* [2021] ECHR 972.

[1672] Article 8 is sometimes referred to as the right to privacy and includes the protection of personality rights. See *Flinkkila & others v Finland* [2010] ECHR 446 para 75, and *Saaristo & others v Finland* [2010] ECHR 1497 para 61.

[1673] *Hurbain v Belgium* [2023] ECHR 948.

[1674] *Hurbain v Belgium* [2023] ECHR 948 para 205, see the discussion and application in paras 212 – 257. See *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) para 95, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 105 – 107, and *Biancardi v Italy* [2021] ECHR 972. See also *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 para 165, *Axel Springer SE and RTL Television GmbH v Germany* [2017] ECHR 793 para 42, and *Falzon v Malta* (European Court of Human Rights) application no 45791/13 (20 March 2018) para 55. The court also applied *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317. See E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 263.

[1675] *Hurbain v Belgium* [2023] ECHR 948 para 189, *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018) paras 87 – 88, 95 and 100, *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 105 – 109, and *Biancardi v Italy* [2021] ECHR 972. See also *Österreichischer Rundfunk v Austria* [2006] ECHR 1043 para 68, *Axel Springer AG v. Germany* [2012] ECHR 227 para 83, *Axel Springer SE & RTL Television GmbH v Germany* [2017] ECHR 793 para 42, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017] ECHR 607 paras 163 and 165, *Falzon v Malta* (European Court of Human Rights) application no 45791/13 (20 March 2018) para 55, and *Denisov v Ukraine* [2018] ECHR 1061 para 98. The Grand Chamber also discussed *Google Spain SL, Google Inc.*

The ECtHR noted the *Google Spain* judgment and the right to be forgotten and recognised that *Google Spain* provides a solution which it applied. The ECtHR does not refer to it as the "right to be forgotten", and preferred to say that the data/information should be de-referenced. Although, this is essentially what the right to be forgotten entails, the ECtHR does not apply the EU legislation, but expects the governments and courts from its Member States to apply domestic and EU laws through the prism of the Convention, ie the application and implementation of domestic and EU laws must be in line with the rights provided for in the Convention. It is worth noting that not all members of the Council of Europe (and the ECtHR) are members of the EU (and the CJEU).[1676]

The ECtHR refused to grant an order to de-index/de-list/de-reference personal data/information in *ML & WW*.[1677] The reason for not granting the order was that the data subjects in that matter had been in constant contact with the press in relation to their "plight".[1678] Unlike in *Hurbain* where the ECtHR specifically emphasised that the data subject wished to remain out of the media's "spotlight", as he did not make contact with the press, and truly wanted to have the trial, conviction and sentence "forgotten".[1679] Another factor considered in *Hurbain*, and which swayed the decision in favour of anonymisation rather than de-indexing/de-listing/de-referencing, was that the information was easily retrievable when using both an internet as well as the publisher's search tool.[1680] *Hurbain* stressed, depending on the facts before each court, that the least restrictive limitation of freedom of press must be considered and implemented.[1681] In *Biancardi*, the ECtHR went one step further and ordered that the information be removed completely from the online database, due to the sensitivity

v AEPD, Mario Costeja González EU:C:2014:317. Note also E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 263.

[1676] *Jeunesse v The Netherlands* [2014] ECHR 1036 para 110, Articles 19 and 32(1) of the Convention, and S O'Leary 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 at 5.

[1677] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).

[1678] See generally *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018), as this point was something that the ECtHR kept on coming back to. See also E Corcione 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 at 263 – 265.

[1679] *Hurbain v Belgium* [2023] ECHR 948 paras 227 – 229.

[1680] *Hurbain v Belgium* [2023] ECHR 948 para 234 and *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) paras 126 – 127, and 132.

[1681] *Hurbain v Belgium* [2023] ECHR 948 para 242 and *Hurbain v Belgium* (European Court of Human Rights) application no 57292/16 (22 June 2021) para 19 (of the separate dissenting judgment of Pavali J). Note apart from anonymization, in *Hurbain v Belgium* [2023] ECHR 948 para 14 of Krenc J's concurring opinion considered other options to take into account apart from anonymization, such as "the de-indexing of the article . . . its alteration . . . or the addition of a notice" (case references omitted).

thereof, as well as the fact that the criminal trial had not begun, and the data subject's innocence or guilt had not been determined.[1682]

(c) South Africa

Once again, as with most of the discussions in this chapter, the rights of privacy (s 14) and freedom of expression (s 16) in the Constitution will need to be balanced with one another. A useful "tool" includes the sliding scale, as detailed in Chapter 5, that specifically considers whether the data/information should remain available or whether the data/information should be de-indexed/de-linked/de-referenced ("forgetting") or whether anonymisation will be enough, or whether the data/information is so sensitive that the data/information should be deleted. In this regard, similar considerations as those of the privacy continuum, enunciated in *Bernstein v Bester*[1683] will be useful to keep in mind, especially since one of the considerations relates to the public interactions of data subjects. In *Smuts v Botha*[1684] the Supreme Court of Appeal (SCA) held that where a data subject has already posted pictures of himself and his family on social media and the address of his farm was available in the Deeds Registry, which is a public document, the data subject cannot claim that the data/information is private where it is posted by another in a statement. However, the Constitutional Court in *Botha v Smuts*[1685] did not deal with the issue of whether personal data/information that is available in the Deed Registry means that the data subject cannot claim that the data/information may amount to personal data/information and therefore should be deleted, etc. Although the issue was dealt with in the high court judgment, it was held that the parties had not addressed this issue in their papers, and that there was no need to make a finding on this point.[1686] The Consitutional Court

[1682] *Biancardi v Italy* [2021] ECHR 972.
[1683] *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC).
[1684] *Smuts & another v Botha* [2022] ZASCA 3. Mr Smuts published a post on social media severely criticising the manner in which Mr Botha treated the wild animals present on his farm. The post identified Mr Botha by name and included pictures of him. In addition, it also included the name and location of his farm. Following Mr Smut's post, a barrage of further criticisms were levelled against Mr Botha by members of the general public. Mr Botha then applied to the high court for an interdict prohibiting Mr Smuts from publishing defamatory statements about him. The high court held that while Mr Smuts was entitled to comment on and post pictures of the animals, he was not entitled to post Mr Botha's name or picture. He was also not entitled to post the name and location of the farm. This information was personal and was protected by Mr Botha's right to privacy. After the high court granted the interdict, Mr Smuts appealed to the Supreme Court of Appeal (SCA). The SCA found in favour of Mr Smuts and upheld the appeal. In arriving at this decision, the SCA held that the information was not personal because Mr Botha had already posted pictures of himself and his family on social media and the address of his farm was available in the Deeds Registry, which is a public document. Mr Botha has appealed the judgment, and the matter is to be heard on 9 November 2023 at the Constitutional Court, see Constitutional Court of South Africa 'Herman Botha v Bool Smuts and another'. *https://collections.concourt.org.za/handle/20.500.12144/38290* (Accessed: 23 October 2023) – the judgment has not been handed down.
[1685] *Botha v Smuts & another* 2025 (1) SA 581 (CC).
[1686] *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 125 of Kollapen J's judgment.

held that a data subject's personal data/information, even if published on the internet, will carry a reasonable or legitimate expectation of being protected, unlike data/information relating to their business or public life.[1687] The more the data subject interacts with the public, the less likely, applying the continuum in *Bernstein v Bester*,[1688] will the data subject have a legitimate expectation that such data/information will remain truly private. These considerations are easily applied to the right to be forgotten – the more personal the data/information is and the more readily available this information is, the less likely it is that their personal data/information will be "forgotten", anonymised or deleted. A factor that could influence the decision, as to whether a data subject will have a legitimate expectation to keep personal data/information private, is the position that the data subject holds within the public sphere, ie whether the person is a politician or famous personality. A possible reason for this is where the data/information relates to the data subject's integrity, an important aspect where a data subject holds public office, the data/information may not be "forgotten", anonymised or deleted. This will depend on the circumstances of the matter before the courts, and whether it is necessary, for the office held by the data subject, that similar standards are displayed throughout both the personal and public life.[1689]

The SA courts have acknowledged that the internet or social media posts have an incredibly wide reach, and are easily accessible, crucial factors that cannot be down played, when considering whether a person's privacy has been infringed.[1690] Interestingly, in *Waldis v Von Ulmenstein*[1691] the court did not order the complete removal of the blog post or article, and made an order that only the offensive parts of the blog post be removed, the rest could remain as it "did not breach the laws of defamation" and, in light of freedom of speech could be kept and available for interested internet users to access.

[1687] *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 1.
[1688] *Bernstein & others v Bester NNO &other*s 1996 (2) SA 751 (CC).
[1689] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 81 and *TU, RE v Google LLC* EU:C:2022:962 para 62.
[1690] *EFF & others v Manuel* [2020] ZASCA 172 para 31, *Heroldt v Wills* 2013 (2) SA 530 (GSJ), *Netshipise v Munnick & others* [2018] ZAGPJHC 547 para 6, and *Botha v Smuts & another* 2025 (1) SA 581 (CC) para 193. See also D Iyer 'An analytical look into the concept of online defamation in South Africa' (2018) 32(2) *Speculum Juris* 124 at 125, D Sive & A Price 'Regulating expression on social media' (2019) 136(1) *South African Law Journal* 51 – 83, P Gabriel 'The Protection of Personal Information Act 4 of 2013 and children's right to privacy in the context of social media' (2019) 82 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 605 – 620, and M Malahleka 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 1 at 14 – 15.
[1691] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC) para 48. See the discussion in *Dimension Data (Pty) Ltd v Pearton* [2021] ZAECPEHC 54 in light of information placed onto a website.

(d) Comment

Once again, the South African courts and the ECtHR have many similarities when balancing the rights of privacy and freedom of expression. These include where the data subject is directly responsible for the release of their personal information, and therefore does not have a legitimate expectation of privacy, such as in *Smuts v Botha*.[1692] The Constitutional Court limited this exectation to only the data subject's business or public life, as that thrives on being available or accessible on the internet, however, a legitimate expectation of privacy still exista in relation to the data subject's personal information.[1693] The same reasoning is used where the data subjects have drawn attention to their "plight", as was the case in *ML & WW*,[1694] in contrast in *Hurbain*[1695] Dr G kept a low profile. The more the data subject interacts with the public, the less likely, as stated above in the discussion of *Recht auf Vergessen II*, will their personal data/information be "forgotten", anonymised or deleted.

South Africa, apart from in *Waldis v Von Ulmenstein*,[1696] has only recently considered the effects of publication on the internet,[1697] but specifically has considered the complete deletion or removal, alternatively the anonymisation of personal data/information on a blog post. The considerations as enunciated in *Hurbain*[1698] are a still useful to take into account with the various factors that the South African courts have accepted in the cases that deal with defamation, and more recently, the publishing of a home address on the internet as was the issue in *Botha v Smuts*.[1699] These include the permanency of the internet, the accessibility of the data/information on the internet, the passage of time, the behaviour of the data subjects, as well as the negative impact that the continued availability of the information has on the data subject, whether there is an interest in the data/information remaining available, and the impact that such an order granting anonymisation or deletion will have on freedom of expression.[1700] Newer considerations are possibly the passage of time between when the information was posted and when the data subject applies for the data/information to be anonymised or deleted; whether the person is well known, ie an actor or actress, etc.; and whether the information will

[1692] *Smuts & another v Botha* [2022] ZASCA 3.
[1693] *Botha v Smuts & another* 2025 (1) SA 581 (CC).
[1694] *ML & WW v Germany* (European Court of Human Rights) application nos. 60798/10 & 65599/10 (28 June 2018).
[1695] *Hurbain v Belgium* [2023] ECHR 948 paras 227 – 229.
[1696] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).
[1697] *Botha v Smuts & another* 2025 (1) SA 581 (CC).
[1698] *Hurbain v Belgium* [2023] ECHR 948 paras 227 – 229.
[1699] *Botha v Smuts & another* 2025 (1) SA 581 (CC).
[1700] See generally Chapter 4.

have an impact on the data subject holding a public office, ie a politician. However, these last-mentioned considerations are factors that the courts can easily take into account, as they are, especially in light of archived information, important to keep in mind when coming to a solution that has the least impact as possible on freedom of expression. A further consideration that should be considered, and was used by the Consitutional Court, was the nature of the data/information, and what that data/information related to, ie whether it was regarding the data subject's business interests.[1701] *Waldis v Von Ulmenstein*[1702] is a good example of only partially deleting information, and leaving the rest intact, where this is not offensive. However, as has been mentioned throughout, this will depend on the particular circumstances and facts before the court deciding the matter.

VII GENERAL REMARKS AND FURTHER CONSIDERATIONS

(a) Introduction

As seen from the above discussion, the right to be forgotten plays in developing a data subject's personality. In summary, the right to be forgotten allows data subjects more control over their personal data/information by limiting access to data/information that has become "inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully".[1703] These are very important considerations in protecting a data subject's personality, which includes keeping personal data/information private, protecting the data subject's reputation, and providing the data subject with an opportunity to have their information corrected, etc. However, there are certain other considerations that may also need to be included during the balancing exercise that have not been discussed or have been minimally discussed by the courts in the above examples. These further considerations include the decommodification of personal data/information and the ability to combat surveillance capitalism; the eternal memory of the internet; and, specifically in light of anonymisation, whether there are vulnerable family members that need to be afforded protection by having the article anonymised, or whether the data subject was merely an innocent bystander when the incident reported on occurred. Lastly, there will be a brief discussion on the right to be forgotten and artificial intelligence (AI). The reason for adding this discussion is due to the rapid development that AI has experienced since the start of actually writing this thesis.

[1701] *Botha v Smuts & another* 2025 (1) SA 581 (CC).
[1702] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).
[1703] Section 24(1) of POPI.

The considerations mentioned here are not a closed list; there are certainly more, depending on the circumstances of the matter before the relevant data authority or court. Some of these considerations may even fit into the listed considerations discussed above, but will not feature in every matter that comes before a State's data protection authority, or the courts, when deciding whether the data/information should be "forgotten" or not.

Each of these considerations will be briefly discussed hereunder and how they influence whether the right to be forgotten will be granted or not. The considerations for anonymisation will be dealt with together and not under separate headings, as many of the points overlap.

(b) Decommodification of personal data/combatting surveillance capitalism

Although alluded to in the discussions above, this is a novel consideration in SA, ie the balancing of the rights to trade[1704] and privacy.[1705] In *Google Spain*, the CJEU held that this involved balancing a search engine's economic interests, ie the search engine's right to trade, against the data subject's request to have their data/information "forgotten". An important question to ask, but will likely only be answered with time, is whether the South African courts will tip the scale in favour of a natural data subject's privacy. And does this consideration mean that the right to privacy will always have the upper hand when these two rights are being balanced?

The reason for this is that data/information, especially personal data/information, equals money, sometimes also referred to as power (especially in controlling what products, services, etc. are offered on the market, etc.).[1706] The selling of personal data/information is a lucrative market, especially for big data companies such as Google,[1707] Facebook,[1708] X (formerly

[1704] Section 22 of the Constitution.
[1705] Section 14 of the Constitution.
[1706] G Malgieri & B Custers 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303, M Botes, A Olckers & M Labuschaigne 'Data commercialisation in the South African health care context' (2021) 24 *Potchefstroom Electronic Law Journal* 1 – 36, Y Jooste 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 at 478 – 479, DW Woods & R Böhme 'The commodification of consent' (2022) 115 *Computers & Security* 102605 1 – 12 and LJ Hoffmann 'Commodification beyond data: Regulating the separation of information from noise' (2023) 2 *European Law Open* 424 – 433. For a complete discussion and how surveillance capitalism also amounts to both power and money, see Y Jooste 'Surveillance capitalism as white world-making' (2021) 53 (1) *Acta Academica* 44 – 67.
[1707] Google LLC is a US company owned by Alphabet Inc. For a discussion on how the GDPR directly impacts Alphabet and Apple economically, see M Ucar & A Yalcintas 'GDPR and digital protectionism in the EU: The cases of Android and iOS' (2023) 57(4) *Journal of Economic Issues* 1079 – 1094.
[1708] Facebook is owned by Meta Platforms Inc. For a discussion on what the change from Facebook Inc. to Meta Platforms Inc. had on the overall business model, see S Kraus, DK Kanbach, PM Krysta *et al* 'Facebook and the creation of the metaverse: Radical business model innovation or incremental transformation?' (2022) 28(9) *International Journal of Entrepreneurial Behavior & Research* 52 – 77.

Twitter),[1709] Apple.[1710] A search engine, such as Google, sells advertising space to businesses so that when data subjects type into a search tool any of the keywords that match those of an advertisement, then links to these advertisements are displayed on the results page.[1711] One reason why data subjects are increasingly interested in protecting their personal data is because of what has been termed the "Snowden revelations".[1712] Thus, the right to be forgotten is not only about controlling a person's identity and allowing for self-development; it is also an important mechanism in the fight against the commodification of personal data and the threat of surveillance capitalism. The right to be forgotten may play an important public interest/policy role when it comes to striking a balance between privacy and data protection, on the one hand, and freedom of expression, on the other hand. Freedom of expression is an important factor to remember because big data companies may argue that individuals/data subjects have the right to freely impart their personal data/information. It is how this personal data/information is collected and used, ie processed, that is where the problem lies.[1713]

Companies are continuously looking for more and more personal data/information in order to find innovative ways of keeping data subjects interested in their products. The right to be forgotten (and, by implication, anonymisation and deletion) provides data subjects with a remedy to protect themselves against the collection and distribution of their personal data/information. Hence, privacy has an impact on the economic ability to make money as well as the economic value of images.[1714] The decommodification of personal data/information will

[1709] For a general discussion of Twitter and the change name to X as well as the business structure, see The Editors of Encyclopaedia Britannica 'X' *Encyclopedia Britannica*, 25 June 2024. *https://www.britannica.com/money/Twitter* (Accessed 26 June 2024).

[1710] For a discussion on how the GDPR directly impacts Alphabet and Apple economically, see M Ucar & A Yalcintas 'GDPR and digital protectionism in the EU: The cases of Android and iOS' (2023) 57(4) *Journal of Economic Issues* 1079 – 1094.

[1711] See generally on the topic of the sale of advertising space, how it works, and the implications to internet users and data protection: D Geradin & D Katsifis 'An EU competition law analysis of online display advertising in the programmatic age' (2019) 15(1) *European Competition Journal* 55 – 96 and D Geradin & D Katsifis '"Trust me, I'm fair": Analysing Google's latest practices in ad tech from the perspective of EU competition law' (2020) 16(1) *European Competition Journal* 11 – 54.

[1712] M Laurer & T Seidl 'Regulating the European data-driven economy: A case study on the general data protection regulation' (2021) 13(2) *Policy & Internet* 257 at 259.

[1713] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 80 – 81, 84 – 85, 97 and 99, *Fuchsmann v Germany* [2017] ECHR 925 para 32ffg, BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17 – *Recht auf Vergessen II* paras 105, 120 – 122, and 141.and *TU, RE v Google LLC* EU:C:2022:962 para 62. See also H Hijmans 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 at 559, 561 – 562, CM Wulff 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 at 266 – 268, and S Schreurs, N van der Kammen & S Oosterhuis 'A Dutch perspective on the "right to be forgotten"' (2022) 30(2) *European Review of Private Law* 315 at 323.

[1714] M Sánchez de Diego 'Right to one's own image in Spain: What it is and what it is not' (2018) 8 *Journal of Information Policy* 401 – 416.

affect the economic interests of both publishers and search engines.[1715]

Insurance companies often want personal data/information in order to analyse the risks of insuring a data subject accurately, even if certain biases may cloud a true or proper reflection.[1716] The results may be, depending on the information available, higher insurance premiums. Alternatively, data subjects are labelled uninsurable.[1717] The right to be forgotten may assist, especially where the person has made a full recovery from a devastating illness, and has not suffered from a relapse for a prolonged period, to access insurance, without the illness being a factor to be considered, leading to higher premiums, or not being insured at all. The following discussion is only one example of where premiums are "loaded" based on a past medical illness, and how the right to be forgotten may assist data subjects when they are completely cured of their illness. The discussion will be kept as brief as possible.

An example of how personal data/information may be decommodified comes from France, in 2016, where the right to be forgotten was introduced as a mechanism for cancer survivors to use when applying for insurance. However, there are certain restrictions. The first restriction pertains to long-term cancer survivors who are defined either as persons 18 years or older at the time of diagnosis who have not suffered a relapse for 10 years "after the active treatment", and persons under the age of 18 years at the time of diagnosis who have not suffered a relapse for 5 years "after the active treatment".[1718] The second restriction pertains to a "pathology and reference table".[1719] The idea behind this table is to prevent insurers from

[1715] M Sánchez de Diego 'Right to one's own image in Spain: What it is and what it is not' (2018) 8 *Journal of Information Policy* 401 – 416. See also S Singleton 'Balancing a right to be forgotten with a right to freedom of expression in the wake of *Google Spain v. AEPD*' (2015) 44 *Georgia Journal of International and Comparative Law* 165 – 194, M Ovčak Kos 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 at 209 – 211, F Zufall 'Challenging the EU's right to be forgotten: Society's right to know in Japan' (2019) 5 *European Data Protection Law Review* 17 at 19 and K Faisal 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157.

[1716] See generally, A Dumas, R Allodji, B Fresneau *et al* 'The right to be forgotten: A change in access to insurance and loans after childhood cancer?' (2017) 11 *Journal of Cancer Survivorship* 431 – 437, and M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 – 127. See also M Laurer & T Seidl 'Regulating the European data-driven economy: A case study on the general data protection regulation' (2021) 13(2) *Policy & Internet* 257 at 258, B Custers 'New digital rights: Imagining additional fundamental rights for the digital era' (2022) 44 *Computer Law & Security Review* 105636 1 at 8 – 9, and C Blease 'Open AI meets open notes: Surveillance capitalism, patient privacy and online record access' (2024) 50 *Journal of Medical Ethics* 84 – 89.

[1717] A Dumas, R Allodji, B Fresneau *et al* 'The right to be forgotten: A change in access to insurance and loans after childhood cancer?' (2017) 11 *Journal of Cancer Survivorship* 431 – 437, and M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 – 127.

[1718] M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 at 123 – 124.

[1719] This table includes not only cancer but also other illnesses and chronic diseases – see M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 at 124. The example in the text uses cancer as an example of an illness that

increasing premiums, or including further warranties, or denying a data subject insurance, merely because the data subject has been diagnosed with cancer. The table is based on the advancement of therapeutic treatment that a data subject may receive, and which may assist in prolonging the data subject's life expectancy, despite the diagnosis.[1720]

The French Government's intention by adding such a right to be forgotten is to force insurance companies to consider, not only the usual risks associated with cancer, but also the progress that medical science has made in successfully treating cancer, when they decide whether to insure a data subject and, if so, the premiums payable,[1721] mainly due to the advancement of medical technology, the latest cancer treatments are becoming more and more available, even through State medical facilities.

This means that data subjects that are cured, and where there has been no relapse for a prolonged period, are often able to enjoy a high quality of life. Data subjects/cancer survivors are stigmatised based on the fact that they have had cancer. The right to be forgotten, even if certain restrictions apply, is able to unburden them of the stigma of having had cancer, and allows them to obtain insurance, irrespective of whether it is short term or long term, and on similar terms as those who have never suffered from the disease before applying for the insurance.[1722]

Although SA does not have an explicit right to be forgotten, similar considerations, may apply, depending on which insurer data subjects choose. In some instances, the type of cancer the data subject had will either have no effect on the cover that they choose, or the data subject will be excluded where the risk is too high. One of the more common "side-effects" that SA data subjects may face is that their premium is "loaded" because they have had cancer.[1723] For

---

has economic consequences for data subjects/cancer survivors.

[1720] Under each of these two restrictions in the application of the right to be forgotten where cancer survivors (data subjects) apply for insurance, there are specific considerations listed, which form part of the insurance analysis, as well as whether the data subject must still declare that they have had cancer or not. Some of these include any complications experienced during the treatment, whether the data subject has HIV, or the type of cancer that the data subject suffered from, etc. M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 at 123 – 126.

[1721] M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 at 125.

[1722] See generally, A Dumas, R Allodji, B Fresneau *et al* 'The right to be forgotten: A change in access to insurance and loans after childhood cancer?' (2017) 11 *Journal of Cancer Survivorship* 431 – 437, and M Mesnil 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 – 127.

[1723] See H Taylor 'Can I get life insurance after a cancer diagnosis?' *FA News*, 18 October 2016. *https://www.fanews.co.za/article/life-insurance/9/general/1202/can-i-get-life-insurance-after-a-cancer-diagnosis/21225* (Accessed: 13 April 2024), MyWayLife 'Can I get life insurance if I have cancer?' MyWayLife Blog, 17 June 2018. *https://www.miwaylife.co.za/blog/can-i-get-life-insurance-if-i-have-cancer/* (Accessed: 13 April 2024). See also AB Kornblith, JE Herndon II, RB Weiss *et al* 'Long-term adjustment of survivors of early-

data subjects that have survived cancer, especially childhood cancer, and have not had a relapse, the right to be forgotten would be an ideal solution. The right to be forgotten would ensure that the data subject would not be discriminated against when applying for an insurance policy, irrespective of whether it is short- or long-term policy. Insurance companies could use similar considerations as those used in France, where a data subject/cancer survivor applies for insurance.

(c) Eternal memory of and the ease of accessing data/information on the internet

This consideration is, although not often fully detailed in the cases discussed above, the main reason why a right to be forgotten (and by application anonymisation and deletion as possible further options) is so important – data subjects want to protect their reputation, and their right to privacy. The introduction to this thesis details the repercussions that the eternal memory has, especially since data/information, including personal data/information, is so easily accessible once it is placed on the internet. Paywalls may block a majority of internet users from accessing data/information placed on a website, including personal data/information, however, the fact that the link to the data/information was displayed on the results page is still a cause of concern for some data subjects.[1724] However, most of the data/information is freely accessible to internet users.[1725]

Ausloos and Veale recognise the need for researchers who use data, especially data that is available through the internet, or via other technological means, must develop a "procedure" whereby the use of personal data/information is contemplated, any ethical questions and legal issues are dealt with.[1726] The reasoning behind the procedure is to safeguard researchers from the overriding safeguards that are available to data subjects within data protection instruments.[1727]

All the cases discussed in Chapter 3 specifically highlighted the importance of the passage of time. The fact that the internet never forgets, coupled with the passage of time as well as the ease that data/information may be accessed, may lead to some very embarrassing situations for a lot of data subjects. It may impact a data subject's ability to obtain suitable

stage breast carcinoma, 20 years after adjuvant chemotherapy' (2003) 98(4) *Cancer: Interdisciplinary International Journal of the American Cancer Society* 679 at 682 – in this article, data was collected in conjunction with the University of Pretoria.

[1724] *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC).

[1725] *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317 para 19.

[1726] J Ausloos & M Veale 'Researching with data rights' (2020) *Technology and Regulation* 136 – 157

[1727] J Ausloos & M Veale 'Researching with data rights' (2020) *Technology and Regulation* 136 at 157.

employment, especially where the data/information, which may include a photo from a celebration with the data subject holding a cocktail, etc., which the data subject thought inconsequential at the time, now has adverse consequences.

Keeping in mind that the internet never forgets, the passage of time between the original event, and the current circumstances of the data subject, the right to be forgotten provides a solution against the eternal memory of the internet. The reason is to ensure that the data subject's latest circumstances are displayed in searches using their name. This is what was ordered in *GC & others*.[1728] As briefly described above, the CJEU, instead of requiring that the data/information be "forgotten", first ordered that where the personal data/information is available on a third party's webpage it may not be processed more than is necessary. Second, the CJEU ordered that the current position of the data subject must be displayed at the top of the search results so as to ensure a chronological flow of the data subject's data/information. In light of this example, it may be argued that the CJEU acknowledged that it might not be necessary to order that the links be removed, but rather that an accurate picture of the data subject must be displayed in the search results.

The SA courts are likely to consider the passage of time as an important factor against the eternal memory of the internet, especially since there is the possibility that the data/information will be taken out of context and that the data subject's current circumstances may not be considered, depending on the facts of each matter. Put differently, a search engine be ordered to display the data/information in chronological order, especially in instances where the courts are of the opinion that displaying the data/information in chronological order would remedy the negative impact of data/information being taken out of context.

One last point to note on this topic. Rosen explained that the internet is designed to not forget.[1729] This theme was carried throughout this thesis. This has been emphasised by numerous academic writers, even those critical of the right to be forgotten.[1730] Thylstrup

[1728] *GC AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773. See *Hurbain v Belgium* [2023] ECHR 948 paras 81 – 84, and N Gumzej 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 at 1674.

[1729] J Rosen 'The web means the end of forgetting' *New York Times Magazine*, 21 July 2010. *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022). See also S Welsh 'Forgetting as a function: When the internet wants to remember, how can we learn to forget?' (2020) 24(2) *Kairos: A Journal of Rhetoric, Technology, and Pedagogy*.

[1730] M Crockett 'The internet (never) forgets' (2017) 19 *SMU Science and Technology Law Review* 151 – 181, E Politou, E Alepis & C Patsakis 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) *Journal of Cybersecurity* tyy001 1 at 9 – 10, and H Kocharyan, L Vardanyan, O

pointed out that the "world's memory is at risk" at being lost.[1731] However, the loss of memory will not be due to the internet being able to forget, but may be caused by natural disasters physically destroying the infrastructure that houses servers or the actual servers themselves that store data/information, or through political decisions, or the decisions of giant profit-making tech-companies, to name a few. Put differently, the internet may "forget" data/information but this will not be caused through its own volition, but by an external source.[1732] The essence remains, the internet does not on its own forget. Mayer-Schönberger indicated that there are links that have disappeared, and servers that are no longer functioning, which has caused data/information to be lost.[1733] But once again, this was due to an outside source, and not from an internal function of the internet.

In essence, the internet does not forget, but outside sources may cause data/information to be lost or destroyed. This may, as Mayer-Schönberger writes, provide a positive opportunity for something new to take its place.[1734]

One last point to note on this topic. Rosen explained that the internet is designed to not forget, ie to always remember.[1735] The same point has been made by numerous other writers, including those who are critical of the right to be forgotten.[1736] Although this statement is factually correct, it is important to note, as Thylstrup memorably puts it, that the "world's memory is at risk" of being lost,[1737] not because the internet will forget, but rather because of natural disasters that physically destroy the infrastructure that houses servers or the actual

Hamuľák & T Kerikmäe 'Critical Views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy?' (2021) 21(2) *International and Comparative Law Review* 96 at 97.

[1731] NB Thylstrup 'The world's digital memory is at risk' *New York Times (Online)*, 21 June 2023. Proquest One Academic. *https://www.proquest.com/?accountid=158225* (Accessed: 26 February 2025).

[1732] NB Thylstrup 'The world's digital memory is at risk' *New York Times (Online)*, 21 June 2023. Proquest One Academic. *https://www.proquest.com/?accountid=158225* (Accessed: 26 February 2025).

[1733] V Mayer-Schönberger 'The internet is rotting – Let's embrace it' *The Conversation: Academic rigour, journalistic flair*, 25 July 2019. *https://theconversation.com/the-internet-is-rotting-lets-embrace-it-116239* (Accessed: 1 March 2025).

[1734] V Mayer-Schönberger 'The internet is rotting – Let's embrace it' *The Conversation: Academic rigour, journalistic flair*, 25 July 2019. *https://theconversation.com/the-internet-is-rotting-lets-embrace-it-116239* (Accessed: 1 March 2025).

[1735] J Rosen 'The web means the end of forgetting' *New York Times Magazine*, 21 July 2010. *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022). See also S Welsh 'Forgetting as a function: When the internet wants to remember, how can we learn to forget?' (2020) 24(2) *Kairos: A Journal of Rhetoric, Technology, and Pedagogy*.

[1736] M Crockett 'The internet (never) forgets' (2017) 19 *SMU Science and Technology Law Review* 151 – 181, E Politou, E Alepis & C Patsakis 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) *Journal of Cybersecurity* tyy001 1 at 9 – 10, and H Kocharyan, L Vardanyan, O Hamuľák & T Kerikmäe 'Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy?' (2021) 21(2) *International and Comparative Law Review* 96 at 97.

[1737] NB Thylstrup 'The world's digital memory is at risk' *New York Times (Online)*, 21 June 2023. Proquest One Academic. *https://www.proquest.com/?accountid=158225* (Accessed: 26 February 2025).

servers themselves, or through the decisions of politicians, or through the decisions of tech companies, to name a few. Put differently, the internet may "forget" data/information, but this will not be as a result of its own volition but rather as a result of an external source.[1738] The key point thus remains: the internet does not forget, but nevertheless, data or information may be lost or destroyed as a result of outside events.[1739]

Even when data is lost or destroyed as a result of outside events, Mayer-Schönberger writes, this may create a positive opportunity for something new to take its place.".[1740]

(d) Anonymisation: Protecting vulnerable family members and innocent bystanders

There are two further aspects regarding anonymisation of personal data/information that have not been specifically discussed in the cases, but are important to note. The reason for this is that depending on the circumstances, these further considerations may be the factor that tips the scales towards anonymising the data subject's identity, eg in a news report. The two considerations are first, the person referred to is a vulnerable person, such as a child, or older person, and their identity must be protected as far as possible. An alternate to this is that the data subject is not a vulnerable person, but there are vulnerable persons in their family and their identities must be protected. Second, the data subject was just an innocent bystander when a particular incident occurred.[1741] It should be noted that this is not a comprehensive list, as there may be other relevant considerations, depending on the facts and circumstances, that will convince a court to issue an order in favour of the right to be forgotten or, specifically, the right to anonymisation.

The first of these mentioned considerations, namely the reference to vulnerable persons, was alluded to in *ML v Slovakia*,[1742] but this was not a consideration explicitly discussed by the ECtHR. *ML v Slovakia* is a good example of how non-anonymised data/information has an impact on vulnerable family members and not just the data subject. The ECtHR focused on the fact that the articles in question amounted to idle gossip, and their publication impacted the

[1738] NB Thylstrup 'The world's digital memory is at risk' *New York Times (Online)*, 21 June 2023. Proquest One Academic. *https://www.proquest.com/?accountid=158225* (Accessed: 26 February 2025).
[1739] V Mayer-Schönberger 'The internet is rotting – Let's embrace it' *The Conversation: Academic rigour, journalistic flair*, 25 July 2019. *https://theconversation.com/the-internet-is-rotting-lets-embrace-it-116239* (Accessed: 1 March 2025).
[1740] V Mayer-Schönberger 'The internet is rotting – Let's embrace it' *The Conversation: Academic rigour, journalistic flair*, 25 July 2019. *https://theconversation.com/the-internet-is-rotting-lets-embrace-it-116239* (Accessed: 1 March 2025).
[1741] F Aldhouse 'Anonymisation of personal data – A missed opportunity for the European Commission' (2014) 30 *Computer Law & Security Review* 403 – 418.
[1742] *ML v Slovakia* [2021] ECHR 821.

feelings of the data subject's mother, the applicant/complainant, in the proceedings. The comments referred to the town in which the data subject's mother lived and also mentioned the data subject's surname. Although the mother was not directly mentioned in these articles, the court found that because she still lived in the same town mentioned in the article and bore the same surname as her son, her reputation and identity were affected as these were intertwined with that of her son. The court acknowledged that the data subject may not have been successful if he had applied for the right to be forgotten because he should have foreseen the consequences of his own actions. However, it was the mother, not the data subject, applying for the right to be forgotten, or rather for anonymisation.[1743] She did not cause the consequences she experienced as a result of the publication of the articles, and consequently she should not be denied the protection of her privacy. Aldhouse, specifically referring to children and other persons in a similar context stated that[1744]

> "privacy and data protection are not the only circumstances in which the courts consider anonymisation. There are cases – typically in family cases and especially those concerning children – in which parties and witnesses are required to be anonymised. The experience of judges in handling these matters must colour their response to questions of substantive anonymisation of personal data in freedom of information and data protection cases."

In SA, since 2019,[1745] the names of children, irrespective if they are a complainant, witness or an accused, may not be published during or after the completion of a criminal trial.[1746] This has often been extended to include the names of parents or other family members associated with a child complainant, witness or accused, so as to protect the child and family from being stigmatised by the community.[1747] Generally, the media may not report on the identity of children, and this may also include the identity of the parents, during and after the completion of divorce proceedings within SA.[1748] Although divorces are generally held in open court, and these hearings may result in published judgments, the right to privacy, which includes keeping family matters private,[1749] should not be intruded on more than is necessary.[1750] Hence, in

[1743] Note, the judgment did state that the son/data subject had committed suicide a few years before the matter came before the courts – see *ML v Slovakia* [2021] ECHR 821 para 6.
[1744] F Aldhouse 'Anonymisation of personal data – A missed opportunity for the European Commission' (2014) 30 *Computer Law & Security Review* 403 at 407.
[1745] *Centre for Child Law & others v Media 24 Ltd* 2020 (4) SA 319 (CC).
[1746] Section 154(3) of the Criminal Procedure Act 51 of 1977.
[1747] *Centre for Child Law & others v Media 24 Ltd* 2020 (4) SA 319 (CC).
[1748] Section 12 of the Divorce Act 70 of 1979.
[1749] Private family matters include finances, infidelity, living arrangements of minor children, etc.
[1750] *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) para 67, *Johncom Media Investments Limited v M & others* 2009 (4) SA 7 (CC), see also *Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others* [2023] ZACC 13, and L Albertus 'Has the balance been struck? The decision

divorce and criminal proceedings initials replace the individual names. It is submitted that similar considerations may easily be applied to older persons, especially where there is a chance that they may be stigmatised by the community in which they live, based on the behaviour of their children.

The second consideration mentioned above, namely that the person is merely an innocent bystander, arises when innocent individuals are implicated in scandalous publications under the guise of initials with just enough information to positively identify the person behind those initials. Aldhouse described this and used the following example: an innocent individual that happens to have the same initials as the perpetrator, and they could be implicated in the scandalous publication instead of the actual "perpetrator". Where these rumours damage the reputation and dignity, as well as harm the innocent person/data subject's private life, then courts will consider it best that the data/information either be de-indexed/de-linked/de-referenced, specifically to the name of the data subject. If that is not possible, then the data/information will be anonymised. In this instance, the rights and freedoms of the "innocent bystander" will be considered more worthy of protection than the public's interest or the media's freedom of expression.[1751]

In SA, where constitutional rights need to be balanced against each other, courts will look at the facts and circumstances of the matter before it, as well as the harm that is suffered where the data/information remains in its current form. In this instance, as with the cases dealing with defamation in Chapter 4, the data subject will need to prove that their privacy, as well as their reputation (or dignity), has been negatively impacted by the publication. The cases in Chapter 4 outlined the various principles and considerations that ought to be taken into account. One important point to note is that it must be established that the person implicated in the article is actually the data subject. It is not enough to assume that the initials refer to the data subject. Furthermore, it must also be established that the data subject's right to privacy

in *Johncom Media Investments Limited v M* 2009 4 SA 7 (CC)' (2011) 14(1) *Potchefstroom Electronic Law Journal* 216 – 234.

[1751] F Aldhouse 'Anonymisation of personal data – A missed opportunity for the European Commission' (2014) 30 *Computer Law & Security Review* 403 at 408. Aldhouse worded this as follows:

> "The publication of a scandalous case under cover of initials, but with hints at the underlying identity, has other foreseeable, but regrettable consequences. The experience of this author in relation to the Flitcroft case was that rumour overtook research and one was assured by normally level-headed lawyers that their 'cousin' employed in the courts or football clubs could positively guarantee that the plaintiff was some named footballer – always other than the person it actually turned out to be. The consequential rumours had the potential to damage perfectly innocent bystanders."

It is submitted, that this connection could be aggravated by the fact that the innocent person and the perpetrator may be family members or close friends.

and dignity has been negatively impacted as a direct result of the inferences drawn by internet users in assuming that the article implicates the data subject.[1752] These will need to be applied to the facts that are before the court at the time of the application.

(e) The right to be forgotten and AI

The reason, as mentioned above for this short discussion is due to the rapid technological advancements that have been documented and reported on. There will be some overlap with the above discussions, but due to the unique challenges that AI presents, these issues will be mentioned again here, and as briefly as possible. AI and machine learning applications come with many positives, which include assistance in quicker medical diagnostics, the ability to automate repetitive tasks, and provide accurate predictions, forecasts and detailed information to governments departments, and companies, and also may be of great assistance when researching a topic. Put differently, AI has the ability to revolutionise the way in which individuals manage basic or simple daily tasks, irrespective of whether these are in line with their work or private life.[1753] However, AI also comes with risks.[1754] AI and machine learning needs data/information, irrespective of whether the data/information is personal or not, to learn and function.[1755] Chapter 1 provided a brief description of what AI entails. The main point to note is that AI is able to act independently as well as when prompted to act on command.[1756] The issue with AI is that it needs data/information to learn, and that the data/information collected, or used in this process may or may not be distorted. An example of data/information being distorted, including images, is a deepfake. A deepfake is described as "content (video, audio or otherwise) that is wholly or partially fabricated or existing content (video, audio or

[1752] *Isparta v Richter & another* 2013 (6) SA 529 (GNP), *Heroldt v Wills* 2013 (2) SA 530 (GSJ), *Waldis & another v Von Ulmenstein* 2017 (4) SA 503 (WCC), and *Netshipise v Munnick & others* [2018] ZAGPJHC 547.
[1753] Specifically in light of legal research, see P Magrath 'The Genie and the Lamp: How can artificial intelligence help us find new case law?' (2022) 22 *Legal Information Management* 114 – 118.
[1754] M Ebers, VRS Hoch, F Rosenkranz, *et al* 'The European Commission's proposal for an Artificial Intelligence Act—A critical assessment by members of the Robotics and AI Law Society (RAILS)' (2021) 4 *J – Multidisciplinary Scientific Journal* 589 at 289. In South Affrica, the KwaZulu-Natal High Court Division, Pieteramaritzburg, recently grappled with the use of ChatGPT in legal research, *Mavundla v MEC Department of Co-Operative Government and Traditional Affairs KwaZulu-Natal* & others [2025] ZAKZPHC 2. See also M Van Eck 'Error 404 or an error of judgment? An ethical framework for the use of ChatGPT in the legal profession' (2024) 4 *Journal of South African Law* 469 – 490 for a summary of some of the csses discussed in Chapter 1, as well as further cases from mainly foreign jurisdictions, and how they compare in to the South African position.
[1755] G Mazurek & K Małagocka 'Perception of privacy and data protection in the context of the development of artificial intelligence' (2019) 6(4) *Journal of Management Analytics* 344 at 349 and 359.
[1756] BJ Copeland 'Artificial intelligence' *Encyclopedia Britannica*, 15 May 2024. *https://www.britannica.com/technology/artificial-intelligence* (Accessed: 16 May 2024). Note, chatbots respond to questions asked by the user thereof – see E Gregersen 'ChatGPT' *Encyclopedia Britannica*, 30 June 2023. *https://www.britannica.com/technology/ChatGPT* (Accessed: 12 July 2023).

otherwise) that has been manipulated."[1757] A complete discussion on the creation of deepfakes is beyond the scope of this thesis.[1758]

The possibility of human rights infringements that may be caused by AI (and deepfake technology) are numerous.[1759] There are number of human rights infringements that could be caused by AI, this is not a closed list: first, there is a chance that personal data/information will be collected and processed in contravention to the GDPR or POPI.[1760]

Second, AI may be able to identify a data subject, even if the personal data/information has been anonymised/de-identified, merely through the patterns that are created within the personal data/information, this may include their spending habits, chat content, web browsing history, etc.[1761]

Third, the personal information collected may be processed to the extent that it creates

---

[1757] B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 1. J Kietzmann, LW Lee, IP McCarthy & TC Kietzmann 'Deepfakes: Trick or treat?' (2020) 63 *Business Horizons* 135 – 146 – provide a useful discussion on how deepfakes are created, the consequences as well as a possible framework as to manage deepfakes. See also S Dack 'Deep fakes, fake news, and what comes next' The Henry M. Jackson School of International Studies, 20 March 2019. *https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/* (Accessed: 5 March 2024), and LA Renier, K Shubham, RS Vijay, *et al*. 'A deepfake-based study on facial expressiveness and social outcomes' (2024) 14 *Science Report* 3642 1 – 12.

[1758] Important to note is that the success that deepfakes have rests on two factors, namely believability and accessibility. Regarding believability, deepfake technology has dramatically improved over the last few years making it more difficult to discern whether an image, audio clip, video clip, etc. is in fact real or not. Second, the technology is alarmingly easy to access thanks to the apps/applications, the availability of the computer codes, etc. all available on the internet. This means that believable deepfake images, videos, etc. can be easily created at little or no cost, without an individual needing the requisite training. J Kietzmann, LW Lee, IP McCarthy & TC Kietzmann 'Deepfakes: Trick or treat?' (2020) 63 *Business Horizons* 135 at 136 – 137, L Whittaker, TC Kietzmann, J Kietzmann & A Dabirian '"All around me are synthetic faces": The mad world of AI-Generated media' (2020) 22(5) *IT Professional* 90 at 94, and K Nagumotu 'Deepfakes are taking over social media: Can the law keep up?' (2022) 62 *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 102 at 106 – 107.

[1759] M Ebers, VRS Hoch, F Rosenkranz, *et al* 'The European Commission's proposal for an Artificial Intelligence Act—A critical assessment by members of the Robotics and AI Law Society (RAILS)' (2021) 4 *J – Multidisciplinary Scientific Journal* 589 at 589.

[1760] This means that based on the data/information, including personal data/information, collected and processed, and the outcome of the processing will have an impact on a data subject's life. A data subject may, in order to get a certain health insurance, be required to wear a smart health device. This may result in the premium being adjusted, depending on the data/information collected by the insurance company. G Mazurek & K Małagocka 'Perception of privacy and data protection in the context of the development of artificial intelligence' (2019) 6(4) *Journal of Management Analytics* 344 at 358, TT Canh 'The right to be forgotten according to European Union law in the face of challenges of artificial intelligence to human's private life' In *Proceedings of the 3rd International Conference on Science, Technology and Society Studies (STS 2022)* (22 July 2022, Ho Chi Minh City, Vietnam) 315 at 316, B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 7, and D Donnelly 'First do no harm: Legal principles regulating the future of artificial intelligence in health care in South Africa' (2022) 25 *Potchefstroom Electronic Law Journal* 1 at 9. See also L Lane 'Clarifying human rights standards through artificial intelligence initiatives' (2022) 71(4) *International & Comparative Law Quarterly* 915 at 924 – 926.

[1761] TT Canh 'The right to be forgotten according to European Union law in the face of challenges of artificial intelligence to human's private life' In *Proceedings of the 3rd International Conference on Science, Technology and Society Studies (STS 2022)* (22 July 2022, Ho Chi Minh City, Vietnam) 315 at 317.

a fake or false individual, ie an individual that does not exist.[1762]

Fourth, there are numerous outstanding ethical issues regarding the use of personal data/information and consent. Consent, as required in the GDPR and POPI must be specific, ie it must relate to the specific processing activity. Jones, Kaufman and Edenberg argue, for AI to function optimally whilst processing personal data/information, a type of "continual consent" will be required.[1763] Although continual consent provides for the opportunity to withdraw or revoke, it may be tricky to manage, depending on the technology or the website or company to whom this consent is given.[1764]

Last, where data/information is processed with the use if AI, the algorithms that are used to process the data/information and the complexity of the network that is built using these algorithms means that the process is opaque.[1765] Furthermore, this opacity does tend to make them difficult to regulate.[1766] Jones argues that it is vital that algorithms used in automated processing or AI are regulated in order to maintain human dignity. The algorithms used and the research outcomes must not lose site of the human individual behind the data/information.[1767]

Both the GDPR and POPI contain provisions that provide for the automated processing of personal data/information.[1768] Both the GDPR and POPI provide that where the automated

---

[1762] This includes the ability to make up a bogus company. The false individual's or bogus company's identity may be created in such a way that mimics a real person or company, and this may cause reputational damage to that data subject. Note, in terms of the GDPR, data subjects can only be natural persons, whereas in POPI data subjects may be both natural or juristic persons. See generally B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 7 – 10. Compare with D Edros 'Dead ringers? Legal persons and the deceased in European data protection law' (2021) 40 *Computer Law & Security Review* 105495 1 – 21.

[1763] ML Jones, E Kaufman & E Edenberg 'AI and the ethics of automating consent' (2018) 16(3) *IEEE Security & Privacy* 64 – 72.

[1764] ML Jones, E Kaufman & E Edenberg 'AI and the ethics of automating consent' (2018) 16(3) *IEEE Security & Privacy* 64 at 67.

[1765] The opacity of AI applications creates opportunities for data/information, including personal data/information to be manipulated. M Busuioc, D Curtin & M Almada 'Reclaiming transparency: Contesting the logics of secrecy within the AI Act' (2023) 2(1) *European Law Open* 79 – 105. This point ties up with the third point mentioned above, but is often mentioned separately as it highlights the specific need for transparency. See B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 7 – 10, and M Busuioc, D Curtin & M Almada 'Reclaiming transparency: Contesting the logics of secrecy within the AI Act' (2023) 2(1) *European Law Open* 79 at 79 – 82.

[1766] ML Jones 'The right to a human in the loop: Political constructions of computer automation and personhood' (2017) 47(2) *Social Studies of Science* 216 at 218.

[1767] ML Jones 'The right to a human in the loop: Political constructions of computer automation and personhood' (2017) 47(2) *Social Studies of Science* 216 – 239.

[1768] Articles 2 and 22 of the GDPR and sections 5(1)*(g)* and 71(1) of POPI. Interestingly, Article 4(4) of the GDPR provides the definition for "profiling" which states:

> "any form of *automated processing* of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests,

processing will produce "legal effect" the data subject may object to the automated processing.[1769]

Specifically regarding the EU, data subjects, in terms of Article 17 of the GDPR have an explicit right to request that their data that is processed via automated means (including AI) be deleted.[1770] Further possible solutions from the GDPR include first, that the minimum amount of personal data/information be collected and processed, ie "data minimisation".[1771] Second, ensuring that the latest innovative technical solutions are applied to personal information that is processed using AI or automated means.[1772]

There are few shortfalls with the GDPR, only two are listed as examples, first, the GDPR only applies to natural persons, and not juristic persons. Second, the GDPR it only applies to an individual that is alive, and not to a deceased's personal data/information.[1773] This first example means that juristic persons are not provided with the same level of protection as natural persons in the protection of their personal data/information. In terms of the second example, the deceased's (ie data subject's) reputation and memory are negatively impacted,

---

reliability, behaviour, location or movements" (my emphasis).
However, a complete discussion on what "profiling" and when personal data/information may be processed by automated means is beyond the scope of this discussion. For information, and a complete discussion on this aspect see: EG González & P De Hert 'Understanding the legal provisions that allow processing and profiling of personal data—An analysis of GDPR provisions and principles' (2019) 19 *ERA Forum* 597 – 621, M Büchi, E Fosch-Villaronga, C Lutz, A Tamò-Larrieux, S Velidi & S Viljoen 'The chilling effects of algorithmic profiling: Mapping the issues' (2020) 36 *Computer Law & Security Review* 105367 1 – 15, K Weideman 'Profiling and (automated) decision-making under the GDPR: A two-step approach' (2022) 45 *Computer Law & Security Review* 105662, and AJ Wulf & O Seizov '"Please understand we cannot provide further information": Evaluating content and transparency of GDPR-mandated AI disclosures' (2024) 39 *AI & Society* 235 – 256.

[1769] Recital 71 of the GDPR and
EG González & P De Hert 'Understanding the legal provisions that allow processing and profiling of personal data—An analysis of GDPR provisions and principles' (2019) 19 *ERA Forum* 597 – 621, and E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 443 onwards. Certain exceptions may apply, see Article 22 of the GDPR and s 71 of POPI. Article 22 provides for the following: first, where the processing is necessary to enter into or for the performance of a contract. Second, where the processing is authorised by the EU or a Member State's law. Third, the data subject has provided their explicit consent to have their personal data/information processed via automated means. Section 71 of POPI provides: first the decision relates to the finalisation and implementation of a contract, and the data subject's requests "in terms of the contract have been met", or the data subject's legitimate interests are protected by appropriate means. Second, the automated decision is made in "governed by a law or code of conduct" and the data subject's legitimate interests are protected by "appropriate measures".

[1770] Ie the data/information is "forgotten". EF Villaronga, P Kiesberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304 – 313, TS Cabral 'Forgetful AI: AI and the right to erasure under the GDPR' (2020) 6 *European Data Protection Law Review* 378 – 389, and L Lane 'Clarifying human rights standards through artificial intelligence initiatives' (2022) 71(4) *International & Comparative Law Quarterly* 915 – 944.

[1771] EF Villaronga, P Kiesberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304 at 311.

[1772] EF Villaronga, P Kiesberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304 at 311.

[1773] B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 7 – 8.

however only where it is proven that the negative impact affects the deceased's family, can the family bring an application for the deceased's personal data/information to be "forgotten".[1774]

The EU has enacted the "Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (EU AI Act) to provide a harmonised approach across the EU, but specifically dealing with AI.[1775] The EU AI Act is in the form of a regulation, because a regulation provides for a uniformed, harmonised and integrated statutory landscape across the EU, whereas a directive may result in a fragmented statutory landscape. Member States, when transposing a directive into their national laws have some freedom to adapt it, most notably through the interpretation of the legal concepts.[1776] A regulation comes into force across the EU on the same day, and no transposition is required, thus promoting uniformity and legal harmony.[1777] The EU AI Act is designed to be applied to the processing of personal data/information, and thereby be applied together with the GDPR,[1778] this results in only the personal data/information of natural persons and not those of juristic persons.[1779] A complete discussion of the EU AI Act is beyond the scope of this thesis, suffice to say that the aim of the EU AI Act is to "promote trustworthy AI that is consistent with [EU's] values and interests", including the accountable, transparent, and non-discriminatory use thereof in data processing.[1780] The EU AI Act is globally the first

---

[1774] *ML v Slovakia* [2021] ECHR 821, and B Van der Sloot & Y Wagensveld 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716 1 at 7 – 10.

[1775] M Veale & F Zuiderveen Borgesius 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97 – 112.

[1776] I Saltzman 'The status of national implementation of Directive 95/46/EC on the processing and free movement of personal data' (1996) 18(12) *European Intellectual Property Review* 680 – 683, F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 155 – 156, and S Hurka & Y Steinebach 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 280

[1777] F Duina 'Explaining legal implementation in the European Union' (1997) 25 *International Journal of the Sociology of Law* 155 at 156, P De Hert & V Papakonstantinou 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 at 132, P De Hert & V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 at 182, Y Poullet 'Is the general data protection regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 at 774, and S Hurka & Y Steinebach 'Legal Instrument Choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 at 278 – 279. Note the comments on uniformity when interpreting EU laws by the CJEU in *UI v Österreichische Post AG* EU:C:2023:370 paras 29 and 48.

[1778] Recital 11 of the EU AI Act.

[1779] M Ebers, VRS Hoch, F Rosenkranz, *et al* 'The European Commission's proposal for an Artificial Intelligence Act—A critical assessment by members of the Robotics and AI Law Society (RAILS)' (2021) 4 *J – Multidisciplinary Scientific Journal* 589 at 594.

[1780] For further information see M Veale & F Zuiderveen Borgesius 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97 – 112, P Hacker 'A legal framework for AI training data — From first principles to the Artificial Intelligence Act' (2021) 13(2) *Law, Innovation and Technology* 257 – 301, E Hickman & M Petrin 'Trustworthy AI and corporate governance: The EU's ethics guidelines for trustworthy artificial

comprehensive legislation regulating AI and machine learning.[1781]

POPI, unlike the GDPR, applies to both natural and juristic persons. Hence, under POPI juristic persons will have a similar protection of their personal information to those of natural persons.[1782]

SA does not have an explicit right to be forgotten, however, the principles for data processing must apply, even where the personal data/information is being processed using automated/AI means. This means, as suggested above, apart from applying for the information to be "forgotten", in terms of sections 11(3) and 24(1) of POPI, as described in Chapter 5.[1783] Similarly, as stated in terms of the GDPR, POPI requires that the minimum amount of personal data/information be collected and processed and that it be processed for the minimum amount of time needed, ie the processing must not be excessive.[1784] Furthermore, the latest technology should be used where data/information is processed using automated means.[1785]

Unlike the EU, SA does not have an AI Act.[1786] However, apart from the EU AI Act, SA has further examples it may follow when contemplating similar AI legislation, including legislative instruments from the Organisation for Economic Co-operation and Development (OECD) and the United Nations Educational, Scientific and Cultural Organisation

---

intelligence from a company law perspective.' (2021) 22 *European Business Organisation Law Review* 593 – 625, RJ Neuwirth 'Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA)' (2023) 48 *Computer Law & Security Review* 105798 1 – 14, M Busuioc, D Curtin & M Almada 'Reclaiming transparency: Contesting the logics of secrecy within the AI Act' (2023) 2(1) *European Law Open* 79 – 105, T Buocz, S Pfotenhauer & I Eisenberger 'Regulatory sandboxes in the AI Act: Reconciling innovation and safety?' (2023) 15(2) *Law, Innovation and Technology* 357 – 389, and L Enqvist '"Human oversight" in the EU Artificial Intelligence Act: What, when and by whom?' (2023) 15(2) *Law, Innovation and Technology* 508 – 535. Note also the discussion in A Calderaro & S Blumfelde 'Artificial Intelligence and EU security: The false promise of digital sovereignty' (2022) 31(3) *European Security* 415 – 434.

[1781] JS Butt 'Analytical study of the world's first EU Artificial Intelligence (AI) Act, 2024' (2024) 5(3) *International Journal of Research Publication and Reviews* 7343 at 7345.

[1782] E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 79 – note the "key point" discussion on that page. See also SALRC (Project 124) *Report on Privacy and Data Protection* (2009) para 3.3.40ffg. Note s 8(4) of the Constitution provides that juristic persons are "entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person." Hence, the right to privacy, of which the right to be forgotten is a part, applies to juristic persons.

[1783] Briefly, the data subject will need to object on reasonable grounds to the processing made using automated means, and then either request that the data/information be corrected or deleted.

[1784] Y Burns & A Burger-Smit *A Commentary on the Protection of Personal Information Act* (2018) at 50 – 51, E De Stadler, IL Hatting, P Esselaar and J Boast *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need* (2021) at 253 – 268, and A Roos 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 at 13 – 14, and 25.

[1785] EF Villaronga, P Kiesberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304 at 311

[1786] SS Ka Mtuze & M Morige 'Towards drafting artificial intelligence (AI) legislation in South Africa' (2024) 45(1) *Obiter* 161 at 167.

(UNESCO).[1787] Both these international organisations have identified certain principles, and these principles overlap with the principles for lawful processing of personal data/information provided in POPI, the GDRP and Directive 95/46.[1788] It will not be necessary to go into too much detail, save to say, that these principles are designed to promote transparency and trust in AI systems, especially since AI has the ability to bring positive transformation into society.[1789]

A possible SA AI Act would need to strengthen POPI, and possibly, as in the EU, be applied in conjunction with POPI. However, POPI requires that responsible parties remain accountable to data subjects when processing personal data/information with the use of automated means. Put differently, the means or decisions made when processing of personal data/information must be transparent and lawful.[1790]

This discussion merely emphasises the importance of and need for an ethical AI framework, either, statutorily regulated or drafted by research institutions. The need to protect human rights is a fundamental aspect that must be taken into account where AI systems are used to process personal data/information and personal data/information must be safeguarded from any unnecessary abuse.[1791]

(f) Conclusion

The above are merely a few extra possible considerations that have come out of the academic commentary with regard to the right to be forgotten. The considerations discussed in this chapter and in other chapters of the thesis are not to be taken as a closed list. The considerations will often be dependent on the facts of the matter before the court or the data protection

[1787] L Enqvist '"Human oversight" in the EU Artificial Intelligence Act: What, when and by whom?' (2023) 15(2) *Law, Innovation and Technology* 508 at 514.

[1788] OECD has identified 5 core principles, many of which overlap with the current principles provided in POPI. Briefly, these 5 principles are (1) "inclusive growth, sustainable development and well-being", (2) "respect for the rule of law, human rights and democratic values, including fairness and privacy", (3) "transparency and explainability", (4) "robustness, security and safety", and (5) "accountability". See the OECD *Recommendation of the Council on Artificial Intelligence* (2024) at 8 – 9, see also SS Ka Mtuze & M Morige 'Towards drafting artificial intelligence (AI) legislation in South Africa' (2024) 45(1) *Obiter* 161 at 164 – 165. UNESCO has provided in its recommendations the following 9 principles: (1) "proportionality and do no harm", (2) "safety and security", (3) "fairness and non-discrimination", (4) "sustainability", (5) "right to privacy, and data protection", (6) "human oversight and determination", (7) "transparency and explainability", (8) "awareness and literacy", and (9) "multi-stakeholder and adaptive governance and collaboration". See UNESCO *Recommendation on Artificial Intelligence*, (adopted 23 November 2021) at 11 – 14.

[1789] UNESCO *Recommendation on Artificial Intelligence*, (adopted 23 November 2021) at 8 – 9. See also SS Ka Mtuze & M Morige 'Towards drafting artificial intelligence (AI) legislation in South Africa' (2024) 45(1) *Obiter* 161 at 164 – 167.

[1790] See Chapter 5 for a complete discussion on the conditions of lawful processing.

[1791] M Milossi, E Alexandropoulou-Egyptiadou & KE Psannis 'AI ethics: Algorithmic determinism or self-determination? The GPDR approach' (2021) 9 *IEEE Access* 58455 – 58466.

authority. The extra considerations added here as may sway the decision maker (ie the presiding officer or the data protection authority) to prefer the protection of privacy instead of the continued availability of personal data/information.

VIII CONCLUSION

(a) The aim of the thesis

Chapter 1 set out the aims of what the thesis was going to achieve, put differently the hypothesis and research questions. The aim of the thesis was to critically analyse whether POPI in its current form makes provision for a right to be forgotten. This was, through analysis and discussions, answered positively. However, unlike the GDPR, POPI does not have a specific section that provides for the right to be forgotten. The reason is that POPI is primarily based on Directive 95/46, and not the GDPR. This was also the primary motive for comparing POPI with the EU legislation, specifically Directive 95/46.

The CJEU had used Articles 12*(b)* and 14*(a)* of Directive 95/46 to devise a solution to the problem where information is placed on the internet in terms of "an obligation imposed by law".[1792] An obligation imposed by law, as discussed in Chapter 5, is where a natural or juristic person is required to perform a duty in terms of a legislative instrument or court order.[1793] *Google Spain* pointed out that this would include the publication of court notices such as sales of execution of immovable property to generate funds in terms of an insolvent estate.

The CJEU in *Google Spain* acknowledged that, first, even though the data subject was a rehabilitated insolvent, and this was later extended to rehabilitated criminal offenders, the notice could not simply be removed from the internet. The reason was that, at the time, the notice was published in terms of a valid legal obligation/duty, and simply because the circumstances of the data subject had changed did not mean that the legal notice was now unlawful or illegal. The information may have been outdated, and was a burden for the data subject. Second, the internet has made it a lot easier to find this information. Previously, such information was stored only in paper archives where individuals seeking a copy of such information would have to travel to where the archive was kept and then search for it with the use of an indexing system. This information is now freely available on the internet and is often accessible to everyone, no matter where an internet user may access the data/information from

[1792] As stated in s 11(1)*(c)* of POPI. *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* EU:C:2014:317.
[1793] *Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others* 2021 (4) SA 206 (WCC).

or when they access this information. Put differently, first, the data/information may be accessed by an internet user from anywhere in the world, provided they have an internet-compatible device and internet access. Second, the information that was once available only in paper-based archives has now been digitised and is often freely and easily accessible years after the event has happened.

Hence, another solution was needed to be found. The CJEU's preferred solution in this instance was to de-link or de-index or de-reference the information from the data subject's name, where the data subject's name is used as a keyword in an internet search. The CJEU, however, did state that the right was limited, either nationally or regionally, nationally referring to the country in which the data subject is based, regionally referring to the EU.[1794]

To conclude this thesis, the research questions posed in Chapter 1, will be set out and briefly answered with reference to the chapter in which they were discussed. This is to provide a summary of the findings and discussions that were made throughout the thesis. The research questions briefly were:

(a) Does POPI, being based on Directive 95/46, and using the arguments of the CJEU in *Google Spain*, make provision for a right to be forgotten?

(b) What is the scope, content, or nature of the right to be forgotten in South Africa, this includes how the EU's Directive 95/46 and GDPR have been interpreted by both the regional and national courts in Europe in defining the right to be forgotten.

(c) What are the considerations that should be taken into account when the right to be forgotten as a species of the right to privacy is balanced against the right to freedom of expression and information?

(d) Are there any further considerations that may be taken into account, where these have not been considered by the courts, and how these will affect the balancing exercise between the right to be forgotten and the right to freedom of expression?

The answer to each will be briefly set out below.

(b) The first question

The first question specifically focused on whether South Africa has a comparable right to be forgotten similar to the EU's Directive 95/46. The CJEU had used Articles 12*(b)* and 14*(a)* of

[1794] See chapter 3 of this thesis.

Directive 95/46 to create the right to be forgotten.[1795] The comparable sections in POPI are sections 11(3), and 24(1). Briefly, Article 14*(a)* of Directive 95/46 provides a data subject with the right to object to the processing of their personal data/information. Section 11(3) of POPI provides a similar right. Similarly, Article 12*(b)* of Directive 95/46 and s 24(1) of POPI both provide that data subjects may request that personal data/information that is incorrect, irrelevant, dated, incomplete, misrepresentative or obtained unlawfully be corrected, deleted, or destroyed.

The reason for this solution is that both Directive 95/46 and POPI do not make provision for how personal data/information that was published in terms of a legal obligation should be dealt with where it has become inaccurate, outdated, irrelevant, or incomplete. The information cannot simply be deleted or destroyed because it has been lawfully published. The only possible remedy is for the information to be de-linked/de-indexed/de-referenced from the data subject's name, where a search engine's search tool is used to obtain the data/information with the use of the data subject's name as the keyword. Although the data/information would not be affected, it will be more difficult to find. Interestingly, the data subject's name will still remain as a search term where the data/information is indexed in a paper archive. The right to be forgotten is thus exclusively an internet-based right and does not influence indexes, etc., that have been created to search for data/information in paper archives. These findings lead to the next research question, namely the definition, scope and content of the right to be forgotten.[1796]

(c) The second question

The second question was in relation to the definition, scope and content of the right to be forgotten in light of the manner in which the courts interpreted and applied this right. The CJEU, the ECtHR and the national courts have, as discussed in the first part of this Chapter and detailed in Chapter 3, not only applied the right to be forgotten as first described in *Google Spain*, to data/information that was published based on an obligation in terms of the law, but have also expanded the right to be forgotten and applied it to news articles, ie articles published by the media dealing with court proceedings, the arrest of data subjects, etc.[1797] The right to be forgotten was originally devised to deal with legal notices, irrespective of whether they are printed in the official national gazette of the State, or in a newspaper's classifieds, etc. News articles tend to become outdated, inaccurate, and misleading with the passage of time based on

[1795] See the discussions in Chapters 2 and 3.
[1796] See the discussions in Chapters 5 and 6.
[1797] Chapter 3 of this thesis.

the current circumstances of a data subject. In certain instances, merely de-linking/de-indexing/de-referencing the data/information will not be enough. Hence, another solution is needed. The courts have expanded the right to be forgotten to include anonymising or deleting the digital versions of archived newspaper articles. The print versions, it was argued by the courts, remain intact; it is only the digital version, and this is also the most accessible version, that is altered. Most internet users only search and read the digital version and will seldom look for the original print version, as this is often more difficult and time-consuming to obtain.

In Chapter 3, as well as above, various broad topics were explored. However, the topics explored did not form a closed list because the right to be forgotten is fairly new, and not all possibilities have come through the courts. There were further considerations discussed above, and will again be summarised below. However, a few of them could easily fit under the topics explored in Chapter 3. The topics that were explored were the following: the territorial application of the right to be forgotten; the application of the right to be forgotten in criminal matters; statements, interviews, etc, made in a professional capacity; the processing of special categories of data; and the anonymisation or deletion of archives.

The courts looked at the impact that each of these topics had on privacy, keeping in mind the right to freedom of expression.[1798] It was the impact on the data subject's privacy and private life that was the focus of the discussions; put differently, the greater the impact, the more likely that the information would be de-indexed/de-linked/de-referenced. The smaller the impact, the less likely that the information would be de-indexed/de-linked/de-referenced from the data subject's name. Instead, it would remain available on all possible keywords. An example of the latter is when a person gives an interview on behalf of a company due to company practices or policy. The courts held that this clearly showed that the interview was on behalf of the company, and not in the data subject's personal capacity. Furthermore, even though a considerable amount of time had passed between the airing of the interview and the current application, the information was still a part of the public debate and, therefore, should be easily found on all possible keywords, including the data subject's name. The right to privacy was only marginally infringed, as it was clear that the data subject was acting in light of their duties to the company and not in their personal capacity. Even though the court's decision to reject the application infringed the applicant's right to privacy, that minor infringement was outweighed by the fact that it promoted the right to freedom of expression.

[1798] This discussion was detailed in Chapters 3, 5 and 6, note also the rights discussion in Chapter 4.

However, the courts did also acknowledge that there were circumstances that required that the information be removed completely, ie deleted. Some of the considerations included the importance of the data/information in light of the current public debate, but the focus was on the impact that the continued accessibility of the data/information had on the data subject's reputation and privacy. This is possible when the article discusses an event, such as an assault, and the matter has not gone to court, and the data subject has not had an opportunity to clear his or her name. This has the greatest impact on freedom of expression and information, but very little to no impact on the right to privacy. The data subject's privacy remains intact, whereas the media and internet users' right to freedom of expression and information is impacted as the data/information is no longer available, especially digitally. There have been instances where the data/information may only need to be partly deleted. Partial deletion of data/information would be ordered where it is published on a blog that has a paywall, and hence, very few readers in comparison to a freely accessible digital newspaper archive. Deletion of the data/information from digital archives, may mean that internet users may not be aware that it is still available in a paper-based archive, including which paper-based archive.

Where the information is still important to the public debate, but the data subject's name does not add anything to the topic, and the continued display thereof or access thereto with the data subject's name causes more harm than is necessary to the data subject, then the data/information is likely to be anonymised, and de-linked/de-referenced/de-indexed completely. This is often the case where there is a need for the information to remain available for research, historical or statistical purposes. For example, the fact that a drunk driver caused the deaths of numerous individuals in a motor vehicle accident, does not need the name of the driver to be known, merely the fact that the accident occurred, and that the driver was convicted and sentenced. The actual name of the driver is not necessary for statistical purposes, etc. Hence, the data subject's privacy and reputation are protected, but the media and internet users' right to freedom of expression and information is negatively impacted on. It is interesting to note that this is only the case on internet platforms; generally, there is no impact on paper archives as the information will be available in its original, non-anonymised form. The only problem is that if an individual wants that original, non-anonymised version of the article, they will only be able to obtain it at some effort and expense to themselves.

Lastly, where information is published based on "an obligation in terms of the law" the data/information cannot be altered or anonymise the data subject's name, and neither can it be deleted, however, the continued availability of the data/information negatively impacts on the

data subject's privacy. In this scenario the courts have ordered that the data/information should be de-linked/de-referenced/de-indexed from the data subject's name. The information is still available, although it will be more difficult to find. This form of de-linking/de-referencing/de-indexing does have an impact on the right of freedom of expression and information as it will be more difficult to find, as an internet user will not be able to find this information using the most convenient search term, namely the data subject's name. The courts have also ordered that the information should merely be de-linked/de-referenced/de-indexed, and not anonymised. This may be used where the impact on the data subject's privacy, and also their reputation, will not warrant that the information be anonymised or deleted.

Note, as with most of these options, it will have an impact only on digital archives, and not on the paper archives of the media house or publisher. In a paper-based archive, the data/information will remain accessible on the most convenient search term, namely the data subject's name.

(d) The third question

The aim of question three was to discuss how the courts balanced the rights of privacy and freedom of expression in considering certain criteria or factors.

In expanding the right to be forgotten, the national courts, the CJEU and the ECtHR applied various criteria or factors, some of these were fairly specific to the matter before the court, and others have universal application. The list of criteria was detailed in chapter 3, and there is no purpose in rehashing the entire list again.[1799] The following factors, it is submitted, could be described as the more universal criteria that were considered and applied by the various courts:

(a) the right to be forgotten is not an absolute right, meaning that the data subject's right to have their personal data/information de-linked/de-referenced/de-indexed must be balanced against the rights, freedoms and interests of search engines, publishers/media/content providers, and internet users;

(b) the passage of time between the original publication and the date of request was an important factor highlighted by all the judgments discussed. Where the publication is not archived, then the context in which it was published will also be important to

[1799] See also *Hurbain v Belgium* [2023] ECHR 948 para 205.

consider;[1800]

(c) the type or nature of the publication, which includes the sensitivity of the published data/information, and any repercussions that the data subject may suffer if it were to remain indexed/linked/referenced to their name;

(d) the public's continued interest in the data/information;

(e) the availability of the data/information on the internet, which includes whether the access thereto is restricted or the data/information is freely accessible;

(f) search engines are required to comply with the relevant legislation, as well as any orders requesting that the data/information be de-indexed/de-linked/de-referenced from the data subject's name;

(g) specially, what impact will there be to the right to freedom of expression where there is an order to have the personal data/information de-indexed/de-linked/de-referenced. This will include a specific consideration to the impact that the right to be forgotten will have on freedom of the press; and,

(h) the courts have also looked into what would ultimately be the best solution, in terms of the available technological advancements, even if there is some costs involved. It may be that the information should be completely anonymised, or deleted, depending on the circumstances.

To emphasise, these are not the only criteria that were considered, others, discussed above in this Chapter, and in Chapter 3, were considered relevant to those specific facts before the court deciding on whether the right to be forgotten should be applied or not. These were the criteria that had universal application across the various cases discussed.

(e) The fourth question

This fourth question, which was discussed in this chapter, explores whether there are any other criteria that courts (or even the relevant data protection authority) may take into account where there is a right to be forgotten application. These criteria may assist, depending on the circumstances of the matter, in swaying the balance towards privacy and away from the rights of freedom of expression and information. The further criteria explored were, first, the de-commodification of personal data/information or combatting surveillance capitalism; second,

[1800] *Hurbain v Belgium* [2023] ECHR 948 para 205.

the eternal memory of the internet; and third, the protection of vulnerable family members or innocent bystanders through anonymisation.

The first two were mentioned in *Google Spain*. Regarding the decommodification of personal data/information, the CJEU detailed that search engines sell advertising space that is specific to the country (or domain) to companies. On the results page, adverts will appear among the search results. However, another issue was mentioned, this was specifically with regard to the insurance industry. The insurance industry lives off data/information, especially personal data/information. The insurance industry will either use the collected data/information to offer an insurance premium that is ridiculously high, and also exclude certain options to that plan or will merely refuse to offer the data subject any insurance cover. The French government implemented a type of right to be forgotten, specifically for cancer patients, so as to avoid the described situation. This is to prevent data subjects who have been cancer-free for a certain number of years from being excluded from obtaining compulsory household insurance cover when they purchase a house. This was detailed above.

Something similar could be implemented in South Africa, especially since when an immovable property and, in certain instances, also movable property is purchased, the data subject will need to obtain insurance, especially where the immovable or movable property is purchased in terms of a credit agreement. The reason is that if anything were to happen to the property before all the instalments are paid, then the insurance will often pay what the property was valued at, at the time of agreeing to the cover, etc. This would also be applicable where a data subject applies for life cover; if they have been cancer-free, especially for a number of years, then that diagnosis, especially where the data subject was diagnosed as a child, should not be burdened with a higher premium for less cover, or be refused cover.

The reason that this makes inroads into freedom of expression is because the data subject is under no obligation to share this data/information with the insurance company, which would want this data/information so as to provide a full assessment to ascertain a premium. However, where the data subject is under no legal obligation to disclose that personal data/information, then even if the insurance company obtains that data/information, they cannot use it against the data subject and require them to pay a higher premium. See the discussions above.

The second discussion was in light of the eternal memory of the internet. One solution

suggested was detailed in *GC & others.*[1801] Where the court does not order that the data/information be "forgotten" ie de-indexed/de-linked/de-referenced from the data subject's name, then the search engine must ensure that the information is displayed in chronological order on the results page, with the newest information being at the top of the first page. This is important where there have been criminal investigations that have led to a trial, and the data subject was acquitted of all charges, etc. The problem is that internet users tend to take matters out of context, and placing the information into the correct context is important for the data subject's dignity and reputation, and also for freedom of expression and information, because the data subject's relevant data/information is presented in the correct order. This, it is submitted, is a vital aspect of freedom of expression and information – the right to have all the data/information at one's disposal and not taken out of context.

The third discussion dealt with two aspects of anonymisation, first, the protection of vulnerable family members and, second, innocent bystanders through anonymisation of their data/information. The first aspect, provides for the protection of the identity of the data subject's vulnerable family members through anonymisation of the data/information The vulnerable family members include minor children, and elderly family members, such as their mother, father, uncle, aunt, grandparents, etc. This is important where an elderly family member lives in a village or close knitted community. It protects them from being ostracised by friends, and other members of the community, merely because of the data subject's behaviour. The example used was that of *ML v Slovakia*,[1802] although the ECtHR did not focus on this aspect. In *ML v Slovakia*[1803] the data subject, a priest, was charged and convicted of sexual assault. The complainant was the mother. The mother still lived in the village where she had brought up her son, and was still active within the community. Although this was not one of the reasons that the court used to justify that the search engine de-indexes/de-links/de-references the data/information, it is a possible criterion to consider, especially because the mother is not responsible for her adult son's/data subject's actions.

The second aspect discussed was the anonymisation of innocent bystanders. In the example given the innocent data subject's initials and identity are merged with that of the dishonest individual due to the similarity in their initials. The data subject is, via the press, implicated in having committed an action, etc. that they did not. The data subject, in protecting

[1801] *GC & others v CNIL* EU:C:2019:773.
[1802] *ML v Slovakia* [2021] ECHR 821.
[1803] *ML v Slovakia* [2021] ECHR 821.

their reputation, dignity, and privacy, may apply for the information to be deindexed/de-linked/de-referenced. Although there will be an impact on freedom of expression and information, in this instance, the information is partially false and, hence, the internet user's right to information will not be greatly impacted.

IX IN CLOSING

Depending on the circumstances of the matter before the court (or information officer/regulator) the rights of the relevant parties must be considered, including the rights of internet users to generally be able to access data/information. As stated before in light of the foregoing conclusions, the South African government could amend POPI to add a right to be forgotten – the GDPR provides a useful template in Article 17. SA would do well to follow the route taken by the EU. The strengthening of the right to privacy and data protection is vital, especially, as explained above, to protect data subjects' personal data/information from being exploited for commercial purposes, and providing an escape from the internet's eternal memory.

The right to be forgotten is certainly not a "one-size-fits-all" solution. It may not be the perfect solution in dealing with the overflow of information on the internet.[1804] However, the right to be forgotten certainly has its place as a tool to protect a data subject's privacy on the internet. There are instances where granting the right will not be enough to protect the data subject's privacy, or, it will be excessive. Put differently, there will be instances where it will be better to have the information anonymised or deleted. Alternatively, the information need not be "forgotten" because it does not affect the privacy of the data subject, and may only need to be placed in chronological order on the results page, depending on the circumstances.

The main aim of the right to be forgotten is to make the information more difficult to find, and not to delete or anonymise. This is especially important where the information is published in terms of a legal obligation, such as a court order, but due to the passage of time, the data/information has become outdated, inaccurate, etc. The fact that the data/information was published in terms of a legal obligation means that it cannot simply be removed. Hence, the CJEU created the right to be forgotten, which requires that the data/information be de-indexed/de-linked/de-referenced from the data subject's name so that the information is no longer available where a search is conducted using the data subject's name as the search term.

[1804] F Silva 'The right to be forgotten' *Law Society Journal* (1 December 2023). *https://lsj.com.au/articles/the-right-to-be-forgotten/#* (Accessed: 4 March 2025).

The data/information is still available, but is more difficult to find. Generally speaking, this affects only internet searches and not searches conducted in paper archives, which are more onerous and time-consuming.

The main aim of this thesis was to investigate whether South Africa has a right to be forgotten. Although, South Africa does not have an explicit right to be forgotten as provided in the GDPR, since POPI was based more on Directive 95/46. The drafters of POPI saw the development of the right to be forgotten during the drafting of the GDPR, but did not add a similar provision to POPI.

An important point to note is that the right to be forgotten is a part of the right to privacy, and not a separate right, however, it does have an impact on the right to freedom of expression and information. In light of freedom of expression, the right to be forgotten will mainly impact on journalists or the media, publishers, as well as content creators, such as those that write and host a blog, etc. In light of the right to information, this will affect internet users, who are interested in the information. What all the cases highlighted was that there must be a passage of time between the time of publication and the request or application for the data/information to be "forgotten". What will amount to a reasonable passage of time will vary, depending on the facts of the matter.

Furthermore, it is important to remember that where there is a request for personal data/information to be "forgotten", the right to privacy will be balanced with the right to freedom of expression and information. As stated above, there will be instances where the right to freedom of expression and information will be impacted where a right to be forgotten request is successful. If the request for the application of the right to be forgotten is not successful, as the data/information does not infringe the right to privacy, or the infringement is justified, it may mean that the data/information should merely be displayed in chronological order on the results page, but even this promotes freedom of expression and information because the information is available on all keywords, it is chronologically ordered, it provides a complete informative "picture" of the data subject, and it is not taken out of context. The importance of the right to be forgotten is that is allows for anonymisation or deletion, but also that information is not "forgotten", and is rather placed in chronological order. The fluidity of the right to be forgotten is certainly an important tool that will strengthen the protection of both the rights to privacy and freedom of expression and information.

In light of the above, it is important that data/information is protected and privacy is

preserved, especially in an age where technology develops in “leaps and bounds”. The EU is generally well known for preserving the privacy of its citizens. The reason for this can possibly be traced back to the world wars that have played out in Europe, or the mistrust of governments against their own citizens. Germany is a good example – first the Gestapo under Adolf Hitler, and later in East Germany, also referred to as the German Democratic Republic – where not only was there dedicated “police” or “secret service” that spied on the citizens, but also fellow citizens spied on each other. Many individual citizens were vigilant, not only when out in public, but also within their personal space, their homes, for fear that the neighbours may report them to the relevant authorities.

On the other end of the scale is the US who have entrenched freedom of speech and information as a part of their first amendment rights. Although there may not be a hierarchy of rights, a lot of emphasis, especially in daily interactions, is placed on the first amendment rights, in comparison to the others. Still privacy must find its place, even if it is only found in the fourth amendment. Privacy and freedom of expression are often viewed as polar opposites. In certain instances that may be true. Generally, privacy and freedom of expression, as well as all other rights, together form the basis of dignity. The ability to choose when to express and share and when to keep things private provides individuals with powerful tools in shaping their personality. This includes what they wish to share online.

Privacy is such an important right, especially because it provides an individual with an important space to grow and develop their personality and their sense of being. Privacy provides a space for individuals to “just be”, ie to have fun and dance to music, sing out of tune, study, find time and space for personal relationships, pursue hobbies, etc., in a space without the interference of others. Privacy is such a vital part of what is means to live in dignity. In an age where individuals “live online” instead of “living offline”, data protection and privacy come up short. There is a need, both ethically, morally and judicially, for some form of control to be placed on certain technological developments. Technology, as stated in the GDPR, should serve human beings, and not human beings serve technology. In between the commercialisation of data/information, the eternal memory of the internet and the rapid pace at which technology is developing, including AI, privacy must not be forgotten. Privacy, dignity and the ability to find a safe space in which individuals can remove themselves from the “outside world” and “let their guard down” are vital for relaxation, finding time to build personal relationships, protect what the world knows about them, are all important aspects for growth and development of an individual’s personality. These are only some of the reasons to why a right to be forgotten

would go a long way at preserving not only privacy, but also the right to expression and information, as they will be able to control what is known about them. There is no need to constantly “show and tell” all details and aspects of an individual’s life. Allowing individuals the ability to control what is known about them, allows for the preservation of their dignity and reputation, two very vital aspects that are protected under personality and privacy rights.

BIBLIOGRAPHY

BOOKS

Aagaard, A (ed) *Digital Business Models: Driving Transformation and Innovation*, Cham, Switzerland, Springer International Publishing AG (2019).

Burns, Y & Burger-Smit, A *A Commentary on the Protection of Personal Information Act*, Durban, LexisNexis (Pty) Ltd (2018).

Burns, Y & Burger-Smit, A *Protection of Personal Information: Law and Practice*, 2ed, Durban, South Africa, LexisNexis (Pty) Ltd (2023).

Cheadle, MH, Davis, DM & Haysom, NRL *South African Constitutional Law: The Bill of Rights*, Cape Town, South Africa, Juta and Company (Pty) Ltd (May 2020 – Service Issue 28).

Cronjé, F & Laubscher, E *PAIA: What You Need to Know*, Claremont, South Africa, Juta and Company (Pty) Ltd (2016).

Ctvrtník, M *Archives and Records: Privacy, Personality Rights, and Access*, Cham, Switzerland, Palgrave Macmillan (2023).

Currie, I & De Waal, J *The Bill of Rights Handbook*, 6ed, Cape Town, South Africa, Juta and Company (Pty) Ltd (2013).

De Stadler, E, Hattingh, IL, Esselaar, P & Boast, J *Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need*, Cape Town, South Africa, Juta and Company (Pty) Ltd (2021).

De Vos, P & Freedman, W (eds) *South African Constitutional Law in Context*, 2ed, Cape Town, South Africa, Oxford University Press Southern Africa (Pty) Ltd (2021).

Delport, P *Henochsberg on the Companies Act 71 of 2008*, Durban, South Africa, LexisNexis (Pty) Ltd (November 2021 – Service Issue 27).

Freedman, DW (assisted by Robinson, RM & Pugsley, GE – original text Devenish, GE) 'Constitutional Law: Bill of Rights' in WA Joubert (founding ed) *Lawsa* vol 5(4) 2ed, Durban, South Africa, LexisNexis (Pty) Ltd (2012).

Harms, D *Civil Procedure in the Superior Courts*, Durban, South Africa, LexisNexis (Pty) Ltd (August 2023 – Service Issue 77).

Hoeren, T, & Kolany-Raiser, B (eds) *Big Data in Context: Legal, Social and Technological Insights*, Cham, Switzerland, Springer International Publishing AG (2018).

Kruger, JM 'Protection of a Child's Right to Privacy in South African Law' in J Potgieter, J

Knobel & R Jansen (eds) *Essays in Honour of Johann Neethling* Durban, LexisNexis (Pty) Ltd (2015) 269 – 283.

Johnston, A & Unberath, H 'Law at, to or from the Centre? The European Court of Justice and the Harmonization of Private Law in the European Union' In Cafaggi, F (ed) *Collected Courses of the Academy of European Law*, Oxford, England, Oxford University Press (2006) 149 – 190

Law, J & Martin, EA (eds) *Oxford Dictionary of Law*, 7ed, Oxford, United Kingdom, Oxford University Press Inc. (2009).

Meredith, S & Nolan, D *The Oxford University Standard for Citation of Legal Authorities*, 4ed, Oxford, United Kingdom, Oxford University Press Inc. (2012).

Roos, A 'Data Protection Law in South Africa' In A Makulilo (ed) *African Data Privacy Laws* Cham, Switzerland, Spinger International Publishing AG (2016).

Smith, M & Miller, S *Biometric Identification, Law and Ethics*, Cham, Switzerland, Springer International Publishing AG (2021).

Waite, M (ed) *Paperback Oxford English Dictionary*, 7ed, Oxford, United Kingdom, Oxford University Press Inc. (2012).

ARTICLES AND BLOGS

Abiteboul, S & Stoyanovich, J 'Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation' (2019) 11(3) *Journal of Data and Information Quality* 15. DOI: *https://doi.org/10.1145/3310231*.

Albertus, L 'Has the balance been struck? The decision in *Johncom Media Investments Limited v M* 2009 4 SA 7 (CC)' (2011) 14(1) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 216 – 234.

Aldhouse, F 'Anonymisation of personal data – A missed opportunity for the European Commission' (2014) 30 *Computer Law & Security Review* 403 – 418.

Alexopoulou, S & Pavli, A '"Beneath this mask there is more than flesh, beneath this mask there is an idea": Anonymous as the (super)heroes of the internet?' (2021) 34 *International Journal for the Semiotics of Law* 237 – 264.

Allen, R & Masters, D 'Artificial intelligence: The right to protection from discrimination caused by algorithms, machine learning and automated decision-making' (2020) 20 *ERA Forum* 585 – 598.

Ambrose, ML & Ausloos, J 'The right to be forgotten across the pond' (2013) 3 *Journal of Information Policy* 1 – 23.

Andrew, J & Baker, M 'The General Data Protection Regulation in the age of surveillance capitalism' (2021) 168 *Journal of Business Ethics* 565 – 578.

Astfalck, L, Britton, N, MacRoberts, C & Van Der Vyver, E 'Cybercrimes Act: Cybercrimes are enforceable criminal offences in South Africa with effect from 1 December 2021' *Lexology*, 2 December 2021. *https://www.lexology.com/library/detail.aspx ?g=d1d7d561-0687-416c-b3a3-fb2f0bfe16cc* (Accessed: 4 March 2023).

Ausloos, J 'The "right to be forgotten" – Worth remembering?' (2012) 28 *Computer Law & Security Review* 143 – 152.

Ausloos, J & Veale, M 'Researching with data rights' (2020) *Technology and Regulation* 136 – 157.

Ayala, D 'Shore to shore: How Europe's new data privacy laws help global libraries and patrons' (2018) 50(3) *International Information & Library Review* 212 – 218.

Ballaschk, J 'In the unseen realm: Transnational intelligence sharing in the European Union - Challenges to fundamental rights and democratic legitimacy' (2015) 51 *Stanford Journal of International Law* 19 – 52.

Barfield, W 'Liability for autonomous and artificially intelligent robots' (2018) 9 *Paladyn, Journal of Behavioral Robotics* 193 – 203.

Barnard, J & Botha, MM 'Trade unions as suppliers of goods and services' (2018) 30(2) *South African Mercantile Law Journal* 216 – 250

Basdeo, V 'Criminal and procedural legal challenges of identity theft in the cyber and information age' (2017) 30 *South African Journal of Criminal Justice* 363 – 384.

Batchelor, B & Wazvaremhaka, T 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *South African Law Journal* 122 – 130.

Bayamlıoğlu, E 'The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"' (2022) 16 *Regulation & Governance* 1058 – 1078.

Bekink, M 'The constitutional protection afforded to child victims and child witnesses while testifying in criminal proceedings in South Africa' (2019) 22 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 50. DOI: *http://dx.doi.org/10.17159/17273781/2019/v22i0a5774*.

Belbin, R 'When Google becomes the norm: The case for privacy and the right to be forgotten' (2018) 26 *Dalhousie Journal of Legal Studies* 17 – 35.

Bell, P 'Algorithms: The intellectual capital of the internet' (2001) July/August *Ivey Business*

Journal 44 – 48.

Belogubets, K 'The protection of personal data in the context of law enforcement: Recent case law of the European Court of Human Rights' (2021) 22 *ERA Forum* 231 – 243.

Bentotahewa, V, Hewage C & Williams, J 'The normative power of the GDPR: A case study of data protection laws of South Asian countries' (2022) 3 *SN Computer Science* 183. DOI: *https://doi.org/10.1007/s42979-022-01079-z*.

Bernal, P 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1(2) *Journal of Cyber Policy* 243 – 264.

Bernal, P 'Facebook: Why Facebook makes the fake news problem inevitable' (2018) 69 *Northern Ireland Legal Quarterly* 513 – 530.

Bernal, PA 'A right to delete?' (2011) 2(2) *European Journal of Law and Technology* 1 – 18. *https://ejlt.org/index.php/ejlt/article/view/75* (Accessed 8 February 2024).

Berryman, J 'Equity in the age of the internet: *Google Inc. v. Equustek Solutions Inc*.' (2019) 31 *Intellectual Property Journal* 311 – 326.

Bertolini, A & Riccaboni, M 'Grounding the case for a European approach to the regulation of automated driving: The technology-selection effect of liability rules' (2021) 51 *European Journal of Law and Economics* 243 – 284.

Bessant, C 'The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online' (2015) 16(2) *European Journal of Law and Technology* 1 – 27. *https://ejlt.org/index.php/ejlt/article/view/390/571* (Accessed: 19 December 2022).

Bhaimia, S 'The General Data Protection Regulation: The next generation of EU data protection' (2018) 18 *Legal Information Management* 21 – 27.

Bilchitz, D 'Privacy, surveillance and the duties of corporations' (2016) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 45 – 67.

Bitiukova, N 'The GDPR's journalistic exemption and its side effects: GDPR anniversary – What does it mean for the media?' *VerfBlog*, 16 June 2023. DOI: *10.17176/20230616-111120-0*.

Blease, C 'Open AI meets open notes: Surveillance capitalism, patient privacy and online record access' (2024) 50 *Journal of Medical Ethics* 84 – 89.

Bobadilla, AM 'Digital rights in Europe after the entry into force of regulations for the protection of personal data: Before and after the right to be forgotten' (2023) 28(4) *Communication Law and Policy* 313 – 331.

Bobić, A 'Developments in the EU-German judicial love story: The *Right to be Forgotten II*'

(2020) 21 *German Law Journal* 31 – 39.

Boehm, F & De Hert, P 'Notification, an important safeguard against the improper use of surveillance - Finally recognized in case law and EU law' (2012) 3(3) *European Journal of Law and Technology*. *https://ejlt.org/index.php/ejlt/article/view/155* (Accessed: 27 December 2022).

Bohn, J, Coroamă, V, Langheinrich, M, Mattern, F & Rohs, M 'Living in a world of smart everyday objects — Social, economic, and ethical implications' (2004) 10(5) *Human and Ecological Risk Assessment* 763 – 785.

Bolognini, L & Bistolfi, C 'Pseudonymization and impacts of big (personal/anonymous) data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation' (2017) 33 *Computer Law & Security Review* 171 – 181.

Botes, M 'The use of geospatial surveillance data for public-health emergency and disaster management in South Africa: A review with legal recommendations' (2021) 3 *Tydskrif vir die Suid-Afrikaanse / Journal of South African Law Reg* 474 – 503.

Botes, M, Olckers, A & Labuschaigne, M 'Data commercialisation in the South African health care context' (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 36. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8577*.

Brittain, B 'Lawsuit says OpenAI violated US authors, copyrights to train AI chatbot' *Reuters*, 29 June 2023. *https://www.reuters.com/legal/lawsuit-says-openai-violated-us-authors-copyrights-train-ai-chatbot-2023-06-29/* (Accessed: 3 July 2023).

Bronstein, V 'Prioritising command-and-control over collaborative governance: The role of the Information Regulator under the Protection of Personal Information Act' (2022) 25 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 41. DOI: *http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11661*.

Brook, O & Eben, M 'Another missed opportunity? Case C-252/21 *Meta Platforms v Bundeskartellamt* and the relationship between EU competition law and national laws' (2023) *Journal of European Competition Law & Practice* lpad047. DOI: *https://doi.org/10.1093/jeclap/lpad047*.

Brown, AJ '"Should I stay or should I leave?": Exploring (dis)continued Facebook use after the Cambridge Analytica scandal' (2020) 6(1) *Social Media + Society* 1 – 8. DOI: *https://doi.org/10.1177/2056305120913884*.

Brugger, W 'The treatment of hate speech in German constitutional law (Part I)' (2003) 4 *German Law Journal* 1 – 22.

Brugger, W 'The treatment of hate speech in German constitutional law (Part II)' (2003) 4 *German Law Journal* 23 – 44.

Büchi, M, Fosch-Villaronga, E, Lutz, C, Tamò-Larrieux, A, Velidi, S & Viljoen, S 'The chilling effects of algorithmic profiling: Mapping the issues' (2020) 36 *Computer Law & Security Review* 105367. DOI: *https://doi.org/10.1016/j.clsr.2019.105367*.

Buiterlaar, JC 'Privacy: Back to the roots' (2012) 13 *German Law Journal* 171 – 202.

Bunn, A 'Children and the "right to be forgotten": What the right to erasure means for European children, and why Australian children should be afforded a similar right' (2019) 170(1) *Media International Australia* 37 – 46.

Buocz, T, Pfotenhauer, S & Eisenberger, I 'Regulatory sandboxes in the AI Act: Reconciling innovation and safety?' (2023) 15(2) *Law, Innovation and Technology* 357 – 389.

Bu-Pasha, S 'Cross-border issues under EU Data Protection Law with regards to personal data protection' (2017) 26(3) *Information & Communications Technology Law* 213 – 228.

Burchardt, D 'Backlash against the Court of Justice of the EU? The recent jurisprudence of the German Constitutional Court on EU fundamental rights as a standard of review' (2020) 21 *German Law Journal* 1 – 18.

Burdon, M, Lane, B & Von Nessen, P 'The mandatory notification of data breaches: Issues arising for Australian and EU legal developments' (2010) 26 *Computer Law & Security Review* 115 – 129.

Burrell, J 'How the machine "thinks": Understanding opacity in machine learning algorithms' (2016) 3(1) *Big Data & Society* 1-12. DOI: *10.1177/2053951715622512*.

Burri, M & Schär, R 'The reform of the EU Data Protection Framework: Outlining key changes and accessing their fitness for a data-driven economy' (2016) 6 *Journal of Information Policy* 479 – 511.

Busuioc, M 'Accountable artificial intelligence: Holding algorithms to account' (2021) 81 *Public Administration Review* 825 – 836.

Busuioc, M, Curtin, D & Almada, M 'Reclaiming transparency: Contesting the logics of secrecy within the AI Act' (2023) 2(1) *European Law Open* 79 – 105.

Butt, JS 'Analytical study of the world's first EU Artificial Intelligence (AI) Act, 2024' (2024) 5(3) *International Journal of Research Publication and Reviews* 7343 – 7364.

Buttarelli, G 'Guest editorial: The EU GDPR as a clarion call for a new global digital gold standard' (2016) 6(2) *International Data Privacy Law* 77 – 78.

Bygrave, LA 'Privacy and data protection in an international perspective' (2010) 56(8) *Scandinavian Studies in Law* 165 – 200.

Bygrave, LA 'The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects' (2021) 40 *Computer Law & Security Review* 105460. DOI: *https://doi.org/10.1016/j.clsr.2020.105460*.

Byleveld, R 'A brief overview of the Cybercrimes Act 19 of 2020' FluidRock Governance Group, 15 February 2022. *https://www.fluidrock.co.za/a-brief-overview-of-the-cybercrimes-act-19-of-2020/* (Accessed 4 March 2023).

Cabral, TS 'Forgetful AI: AI and the right to erasure under the GDPR' (2020) 6 *European Data Protection Law Review* 378 – 389.

Cachalia, F & Klaaren, J 'Digitalisation in the health sector: A South African public law perspective' (2022) 25 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 24. DOI: *http://dx.doi.org/10.17159/1727-3781/2022/v25i0a12979*.

Calderaro, A & Blumfelde, S 'Artificial Intelligence and EU security: The false promise of digital sovereignty' (2022) 31(3) *European Security* 415 – 434.

Calzati, S '"Data sovereignty" or "data colonialism"? Exploring the Chinese involvement in Africa's ICTs: A document review on Kenya' (2022) 40(2) *Journal of Contemporary African Studies* 270 – 285.

Çapar, G 'Global regulatory competition on digital rights and data protection: A novel and contractive form of Eurocentrism?' (2022) 11(3) *Global Constitutionalism* 465 – 493.

Carava, E 'Personal data kept in companies' registers: The denial of the right to be forgotten' (2017) 3 *European Data Protection Law Review* 287 – 292.

Carlson, CR & Terry, C 'The devil's in the details: How countries' defamation laws can (and can't) combat hate speech' (2023) *Journalism Practice*. DOI: *10.1080/17512786.2023.2251976*.

Carter, EL 'Argentina's right to be forgotten' (2013) 27 *Emory International Law Review* 23 – 39.

Cashmore, P 'Privacy is dead, and social media holds smoking gun' *CNN.com,* 28 October 2009. *https://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/* (Accessed: 3 December 2022).

Cassim, F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18(2) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 69 – 110.

Čerka, P, Grigienė, J & Sirbikytė, G 'Liability for damages caused by artificial intelligence' (2015) 31 *Computer Law & Security Review* 376 – 389.

Chalton, S 'The transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive)' (1997) 11(1) *International Review of Law, Computers & Technology* 25 – 32.

Chana, SH & Janjarasjitb, S 'Insight into hackers' reaction toward information security breach' (2019) 49 *International Journal of Information Management* 388 – 396.

Chandok, S & Manocha, L 'Right to be forgotten: A step forward in the implementation of Privacy Laws in India' (2018) 6 *Supremo Amicus* 445 – 457.

Chemlali, L 'Right to de-referencing in light of recent case law of the Court of Justice of the European Union (CJEU)' (2022) 25(S1) *Journal of Legal, Ethical and Regulatory Issues* 1 – 13.

Christensson, P 'Domain name definition' *TechTerms.com,* 14 September 2012, *https://techterms.com/definition/domain_name* (Accessed: 10 December 2022).

Chitimira, H & Ncube, P 'The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks' (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 34. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10742*.

Clifford, D & Ausloos, J 'Data protection and the role of fairness' (2018) 37(1) *Yearbook of European Law* 130 – 187.

Coetzee, F 'The press and POPI: Media law' (2014) 14(4) *Without Prejudice* 69 – 71.

Coetzee, J 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce' (2004) 15(3) *Stellenbosch Law Review* 501 – 521.

Coetzee, SA 'A legal perspective on social media use and employment: Lessons for South African educators' (2019) 22 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 37. DOI: *http://dx.doi.org/10.17159/1727-3781/2019/v22i0a5778*.

Cofone, I '*Google v. Spain*: A right to be forgotten?' (2015) 15(1) *Chicago-Kent Journal of International and Comparative Law* 1 – 11. *https://scholarship.kentlaw.iit.edu/ckjicl /vol15/iss1/1* (Accessed: 23 January 2023).

Cohen, D, Elalouf, A & Zeev, R 'Collaboration or separation maximizing the partnership between a "gray hat" hacker and an organization in a two-stage cybersecurity game' (2022) 2 *International Journal of Information Management Data Insights* 100073. DOI: *https://doi.org/10.1016/j.jjimei.2022.100073*.

Cohen, T 'Google and Facebook want your bank account. What could possibly go wrong?' *Business Maverick,* 25 November 2019. *https://www.dailymaverick.co.za*

/article/2019-11-25-google-and-facebook-want-your-bank-account-what-could-possibly-go-wrong/ (Accessed: 25 November 2019).

Connolly, J 'The right to erasure: Comparative perspectives on an emerging privacy right' (2021) 46(1) *Alternative Law Journal* 58 – 63.

Coors, C 'Headwind from Europe: The new position of the German courts on personality rights after the judgment of the European Court of Human Rights' (2010) 11 *German Law Journal* 527 – 537.

Copeland, BJ 'Artificial intelligence' *Encyclopedia Britannica,* 15 May 2024. *https://www.britannica.com/technology/artificial-intelligence* (Accessed: 16 May 2024).

Corcione, E 'The right to be forgotten, between web archives and search engines: Further steps at the European Court of Human Rights' (2019) 5 *European Data Protection Law Review* 262 – 265.

'Court upholds request for information identified by search terms' (2023) 429 *EU Focus* 9 – 11. (Westlaw, Accessed: 18 January 2024.)

Cox, N '*Delfi v. Estonia*: Privacy protection and chilling effect', *VerfBlog,* 19 June 2015. DOI: *10.17176/20170222-113330*.

Craig, R & Phillipson, G 'Privacy, reputation and anonymity until charge: ZXC goes to the Supreme Court' (2021) 13(2) *Journal of Media Law* 153 – 185.

Crockett, M 'The internet (never) forgets' (2017) 19 *SMU Science and Technology Law Review* 151 – 181.

Cunningham, M 'Privacy law that does not protect privacy, forgetting the right to be forgotten' (2017) 65(3) *Buffalo Law Review* 495 – 546.

Curran, D 'Are you ready? Here is all the data Facebook and Google have on you' *The Guardian,* 30 March 2018. *https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy* (Accessed: 29 January 2024).

Custers, B 'New digital rights: Imagining additional fundamental rights for the digital era' (2022) 44 *Computer Law & Security Review* 105636. DOI: *https://doi.org/10.1016/j.clsr.2021.105636*.

Custers, B & Malgieri, G 'Priceless data: Why the EU Fundamental right to data protection is at odds with trade in personal data' (2022) 45 *Computer Law & Security Review* 105683. DOI: *https://doi.org/10.1016/j.clsr.2022.105683*.

Dack, S 'Deep fakes, fake news, and what comes next' The Henry M. Jackson School of

International Studies, 20 March 2019. *https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/* (Accessed: 5 March 2024).

Dahiya, M 'A tool of conversation: Chatbot' (2017) 5(5) *International Journal of Computer Sciences and Engineering* 158 – 161.

Davies, G 'What does it all mean?' (2016) 17 *German Law Journal* 7 – 10.

De Andrade, NNG 'Oblivion: The right to be different … from oneself: Repurposing the right to be forgotten' (2012) 13 *IDP. Revista de Internet, Derecho y Política* 122 – 137.

De Conca, S '*GC et al v CNIL*: Balancing the right to be forgotten with the freedom of information, the duties of a search engine operator' (2019) 5 *European Data Protection Law Review* 561 – 567.

De Hert, P & Papakonstantinou, V 'The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130 – 142.

De Hert, P & Papakonstantinou, V '*Google Spain*: Addressing critiques and misunderstandings one year later' (2015) 22(4) *Maastricht Journal of European and Comparative Law* 624 – 638.

De Hert, P & Papakonstantinou, V 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179 – 194.

De Hert, P, Papakonstantinou, V, Malgieri, G, Beslay, L & Sanchez, I 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34(2) *Computer Law & Security Review* 193 – 203.

De Stadler, E & Van Zyl, L 'Plain language contracts: Challenges and opportunities' (2017) 1 *South African Mercantile Law Journal* 95 – 127.

De Veiga, A, Vorster, R, Li, F, Clarke, N & Furnell, SM 'Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements' (2020) 28(3) *Information & Computer Security* 399 – 422.

Dejan, L 'Personal rights and freedoms – The forms and trends of protection' (2023) 1 *Law Theory and Practice* 1 – 12.

Demetzou, K 'Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation' (2019) 35 *Computer Law & Security Review* 105342. DOI: *https://doi.org/10.1016/j.clsr.2019.105342*.

Denner, N, Heitzler, N & Koch, T 'Presentation of CEOs in the media: A framing analysis' (2018) 33(3) *European Journal of Communication* 271 – 289.

Dennis, MA 'Cybercrime' *Encyclopedia Britannica*, 25 August 2022. *https://www.britannica.com/topic/cybercrime* (Accessed: 7 December 2022).

DeSimone, C 'Pitting Karlsruhe against Luxembourg? German Data Protection and the contested implementation of the EU Data Retention Directive' (2010) 11(3) *German Law Journal* 291 – 317.

Diab, R 'Search engines and global takedown orders: *Google v Equustek* and the future of free speech online' (2020) 56(2) *Osgoode Hall Law Journal* 231 – 270, 2019 CanLIIDocs 4139.

Diggelmann, O & Cleis, MN 'How the right to privacy became a human right' (2014) 14 *Human Rights Law Review* 441 – 458.

Dlamini, S & Mbambo, C 'Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses' (2019) 5(1) *Cogent Social Sciences* 1675404. DOI: *10.1080/23311886.2019.1675404*.

Docksey, C 'Journalism on trial and the right to be forgotten', *VerfBlog*, 9 March 2022. DOI: *10.17176/20220309-121127-0*.

Docksey, C & Hijmans, H 'The Court of Justice as a key player in privacy and data protection: An overview of recent trends in case law at the start of a new era of data protection law' (2019) 5 *European Data Protection Law Review* 300 – 316.

Dollmann, M 'Streit um Nennung des Täters der Apollonia–Morde muss nochmal vor das OLG', 3 November 2020. *https://rsw.beck.de/aktuell/daily/meldung/detail/bgh-streit-um-nennung-des-taeters-der-apollonia-morde-muss-nochmal-vor-das-olg* (Accessed: 22 August 2022).

Donnelly, D 'First do no harm: Legal principles regulating the future of artificial intelligence in health care in South Africa' (2022) 25 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 44. DOI: *http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11118*.

Donnelley, DL '"Privacy by design" in the EU General Data Protection Regulation: A new privacy standard or the emperor's new clothes?' (2022) 139(3) *South African Law Journal* 541 – 575.

Douglas, DM 'Doxing: A conceptual analysis' (2016) 18 *Ethics and Information Technology* 199 – 210.

Douglas, M 'The exorbitant injunction in *X v Twitter* [2017] NSWSC 1300' (2017) 36(4) *Communications Law Bulletin* 11 – 12.

Duina, F 'Explaining legal implementation in the European Union' (1997) 25 *International*

Journal of the Sociology of Law 155 – 179.

Dumas, A, Allodji, R, Fresneau, B *et al* 'The right to be forgotten: A change in access to insurance and loans after childhood cancer?' (2017) 11 *Journal of Cancer Survivorship* 431 – 437.

Dumortier, J & Alonso Blas, DM 'Some legal issues related to the implementation of the European Data Protection Directive in Belgium' (1997) 11(2) *International Review of Law, Computers & Technology* 221 – 242.

Ebers, M, Hoch, VRS, Rosenkranz, F, Ruschemeier, H & Steinrötter, B 'The European Commission's proposal for an Artificial Intelligence Act—A critical assessment by members of the Robotics and AI Law Society (RAILS)' (2021) 4 *J – Multidisciplinary Scientific Journal* 589 – 603.

Editors of Encyclopaedia Britannica 'X' *Encyclopedia Britannica,* 25 June 2024. *https://www.britannica.com/money/Twitter* (Accessed 26 June 2024).

Edors, D 'European Union data protection law and media expression: Fundamentally off balance' (2016) 65 *International and Comparative Law Quarterly* 139 – 183.

Erdos, D 'Statutory regulation of professional journalism under European data protection: Down but not out?' (2016) 8(2) *Journal of Media Law* 229 – 265.

Edros, D 'Dead ringers? Legal persons and the deceased in European data protection law' (2021) 40 *Computer Law & Security Review* 105495. DOI: *https://doi.org/10.1016/j.clsr.2020.105495*.

Edros, D 'The "right to be forgotten" beyond the EU: An analysis of wider G20 regulatory action and potential next steps' (2021) 13(1) *Journal of Media Law* 1 – 35.

Eiselen, S 'Digitisation and consumer law in South Africa and Africa' (2021) 3 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 436 – 455.

Elgesem, D 'The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data' (1999) 1 *Ethics and Information Technology* 283 – 293.

Elliot, M, O'Hara, K, Raab, C, O'Keefe, CM, Mackey, E, Dibben, C, Gowans, H, Purdam, K & McCullagh, K 'Functional anonymisation: Personal data and the data environment' (2018) 34 *Computer Law &b Security Review* 204 – 221.

Enqvist, L '"Human oversight" in the EU Artificial Intelligence Act: What, when and by whom?' (2023) 15(2) *Law, Innovation and Technology* 508 – 535.

Erlank, W & Ramokanate, L 'Allocating the risk of software failures in automated message systems (autonomous electronic agents)' (2016) 28(2) *South African Mercantile Law*

Journal 201 – 237.

Esayas, SY 'The role of anonymisation and pseudonymisation under the EU data privacy rules: Beyond the "all or nothing" approach' (2015) 6(2) *European Journal of Law and Technology* (open access). *https://ejlt.org/index.php/ejlt/article/view/378/568* (Accessed 19 December 2022).

Espino, MM 'Sometimes I feel like somebody's watching me... read?: A comment on the need for heightened privacy rights for consumers of eBooks' (2013) 30(2) *UIC John Marshall Journal of Information Technology & Privacy Law* 281 – 306.

Esposito, E 'Algorithmic memory and the right to be forgotten on the web' (2017) 4(1) *Big Data & Society* 1 – 11. DOI: *10.1177/2053951717703996*.

Esselaar, P, Swales, L, Bellengère, D, Mhlongo, B & Thaldar, D 'Forcing a square into a circle: Why South Africa's draft revised material transfer agreement is not fit for purpose' (2024) 15 *Frontiers in Pharmacology* 1333672. DOI: *10.3389/fphar.2024.1333672*.

Estadella-Yuste, O 'Spain is on the road to implementing EU Directive 95/46' (1997) 11(1) *International Review of Law Computers & Technology* 33 – 46.

Esteve, A 'The business of personal data: Google, Facebook, and privacy issues in the EU and the USA' (2017) 7(1) *International Data Privacy Law* 36 – 47.

Euchner, J 'Almost human' (2023) 66(2) *Research-Technology Management* 10 – 11.

Faisal, K 'Balancing between right to be forgotten and right to freedom of expression in spent criminal convictions' (2021) 4 *Security and Privacy* e157. DOI: *10.1002/spy2.157*.

Farrand, B '"Is this a hate speech?" The difficulty in combating radicalisation in coded communications on social media platforms' (2023) 29 *European Journal on Criminal Policy and Research* 477 – 493.

Fazlioglu, M 'Forget me not: The clash of the right to be forgotten and freedom of expression on the Internet' (2013) 3(3) *International Data Privacy Law* 149 – 157.

Feichtner, I 'The German Constitutional Court's PSPP judgment: Impediment and impetus for the democratization of Europe' (2020) 21 *German Law Journal* 1090 – 1103.

Flett, E & Clover, J '*Google LLC v CNIL* – CJEU rules on the territorial scope of the "right to be forgotten"' (2020) 31(2) *Entertainment Law Review* 69 – 71.

Frantziou, E 'Further developments in the right to be forgotten: The European Court of Justice's judgment in case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*' (2014) 14 *Human Rights Law Review* 761 – 778.

Freedman, W & Schultz, H 'Plugins and POPI: A critical discussion into the legal implications of social plugins and the protection of personal information' (2023) 26 *Potchefstroomse*

Elektroniese Regsblad / Potchefstroom Electronic Law Journal 1 – 32. DOI: *http://dx.doi.org/10.17159/1727- 3781/2023/v26i0a15758*.

Friedewald, M & Pohoryles, RJ 'Technology and privacy' (2013) 26(1-2) *Innovation: The European Journal of Social Science Research* 1 – 6.

Fritz, C '"South African taxpayers" right to privacy in cross-border exchange of tax information' (2021) 11 *Constitutional Court Review* 411 – 432.

Fromholz, JM 'The European Union Data Privacy Directive' (2000) 15 *Berkeley Technology Law Journal* 461 – 484.

Frosio, GF 'The right to be forgotten: Much ado about nothing' (2017) 15 *Colorado Technology Law Journal* 307 – 336.

Gabriel, P 'The Protection of Personal Information Act 4 of 2013 and children's right to privacy in the context of social media' (2019) 82 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 605 – 620.

Gagrani, V 'The right to be forgotten: A need or a way to deviate misdeeds?' (2022) 30 *Supremo Amicus* 85.

Galli, F '*Digital Rights Ireland* as an opportunity to foster a desirable approximation of data retention provisions' (2016) 23(3) *Maastricht Journal of European and Comparative Law* 460 – 477.

Geradin, D & Katsifis, D 'An EU competition law analysis of online display advertising in the programmatic age' (2019) 15(1) *European Competition Journal* 55 – 96.

Geradin, D & Katsifis, D '"Trust me, I'm fair": Analysing Google's latest practices in ad tech from the perspective of EU competition law' (2020) 16(1) *European Competition Journal* 11 – 54.

Gerhold, M 'Rote Ampel für Geisterfahrer: Zur (hoffentlich letzten) EuGH-Entscheidung in Sachen Vorratsdatenspeicherung', *VerfBlog*, 21 September 2022. DOI: *10.17176/20220921-230542-0*.

Gilson, D 'Michael Jackson & Michel Foucault walk into a bar' (2015) 143 *The Threepenny Review* 22 – 25.

Giurgiu, A & Larsen, TA 'Roles and powers of national data protection authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and more "European" DPAs as guardians of consistency?' (2016) 2 *European Data Protection Law Review* 342 – 352.

Globocnik, J 'The right to be forgotten is taking shape: CJEU judgments in *GC and others* (C-136/17) and *Google v CNIL* (C-507/17)' (2020) 69(4) *GRUR International* 380 – 388.

Goddard, M 'The EU General Data Protection Regulation (GDPR): European regulation that

has a global impact' (2017) 59(6) *International Journal of Market Research* 703 – 705.

Goldman, M 'As darkness deepens: The right to be forgotten in the context of authoritarian constitutionalism' (2020) 21 *German Law Journal* 45 – 54.

Gollogly, F 'The blemish on the Clean Slate Act: Is there a right to be forgotten in New Zealand?' (2019) 25 *Auckland University Law Review* 129 – 154.

Gómez, S, Mejía, D & Tobón, S 'The deterrent effect of surveillance cameras on crime' (2021) 40 (2) *Journal of Policy Analysis and Management* 553 – 571.

González, EG & De Hert, P 'Understanding the legal provisions that allow processing and profiling of personal data—An analysis of GDPR provisions and principles' (2019) 19 *ERA Forum* 597 – 621.

Gooden, A & Thaldar, D 'The regulation of health-related direct-to-consumer genetic tests in South Africa by the Medicines and Related Substances Act' (2024) 141(1) *South African Law Journal* 112 – 142.

Goodman, S & Clayton, M 'When is an online publisher a publisher?' *Lexology,* 14 September 2022. *https://www.lexology.com/library/detail.aspx?g=3ca7b651-1da3-467c-9f72-0c5a18b71257* (Accessed: 21 September 2022).

Gordon, BJ 'Automated facial recognition in law enforcement: *The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police*' (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 30. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8923*.

Gordon, JS 'AI and law: Ethical, legal, and socio-political implications' (2021) 36 *AI & Society* 403 – 404.

Goswami, V 'Algorithms, expression and the Charter: A way forward for Canadian Courts' (2017) 7(1) *Western Journal of Legal Studies* Article 2, 2017 CanLIIDocs 331.

Graef, I '*Meta platforms*: How the CJEU leaves competition and data protection authorities with an assignment' (2023) 30(3) *Maastricht Journal of European and Comparative Law* 325 – 334.

Graef, I, Clifford, D, & Valcke, P 'Fairness and enforcement: Bridging competition, data protection, and consumer law' (2018) 8(3) *International Data Privacy Law* 200 – 223.

Gragl, P 'An olive branch from Strasbourg? Interpreting the European Court of Human Rights' resurrection of *Bosphorus* and reaction to *Opinion 2/13* in the *Avotiņš* Case: ECtHR 23 May 2016, Case No. 17502/07, *Avotiņš v Latvia*' (2017) 3(3) *European Constitutional Law Review* 551 – 567.

Graham, C 'NHS cyber attack: Everything you need to know about "biggest ransomware"

offensive in history', *The Telegraph*, 20 May 2017. *https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/* (Accessed: 14 June 2019).

Gregersen, E 'ChatGPT' *Encyclopedia Britannica*, 30 June 2023. *https://www.britannica.com/technology/ChatGPT* (Accessed: 12 July 2023).

Griffin, A 'NHS Hack: Cyber attack takes 16 hospitals offline as patients are turned away', *Independent*, 12 May 2017. *https://www.independent.co.uk* (Accessed: 14 June 2019).

Gstrein, OJ 'The judgment that will be forgotten: How the ECJ missed an opportunity in *Google vs CNIL* (C-507/17)', *VerfBlog*, 25 September 2019. DOI: *10.17176/20190925-232711-0*.

Gstrein, OJ 'Right to be forgotten: European data imperialism, national privilege, or universal human right?' (2020) 13(1) *Review of European Administrative Law* 125 – 152.

Gstrein, OJ 'The right to be forgotten in 2022: Luxembourg judges keep surfing the legislative void' *VerfBlog*, 20 December 2022. DOI: *10.17176/20221220-121718-0*.

Gstrein, OJ & Zwitter, AJ 'Extraterritorial application of the GDPR: Promoting European values or power?' (2021) 10(3) *Internet Policy Review* 1 – 30. DOI: *https://doi.org/10.14763/2021.3.1576*.

Hacker, P 'A legal framework for AI training data — From first principles to the Artificial Intelligence Act' (2021) 13(2) *Law, Innovation and Technology* 257 – 301.

Hadwick, D 'Peer reviewed articles: "Behind the one-way mirror: Reviewing the legality of EU Tax Algorithmic Governance"' (2022) 31(4) *EC Tax Review* 184 – 201.

Hallinan, D & Friedewald, M 'Open consent, biobanking and data protection law: Can open consent be "informed" under the forthcoming data protection regulation?' (2015) 11(1) *Life Sciences, Society and Policy* 1 – 36. DOI: *10.1186/s40504-014-0020-9*.

Hamann, B & Papadopoulos, S 'Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa' (2014) 47(1) *De Jure Law Journal* 42 – 62.

Hamilton, IA 'WhatsApp faces international pressure to hand over access to encrypted chats' *Business Insider South Africa* 31 July 2019, *https://www.businessinsider.co.za/encrypted-messaging-under-pressure-from-five-eyes-nations-2019-7* (Accessed: 5 August 2019).

Handley, P 'Snowden leaks: 10 years later, US intelligence still collects huge amounts of information' *Mail & Guardian*, 5 June 2023. *https://mg.co.za/world/2023-06-05-snowden-leaks-10-years-later-us-intelligence-still-collects-huge-amounts-of-*

information/ (Accessed: 29 January 2024).

Herlin-Karnell, E 'Recent developments in the area of European criminal law' (2007) 14(1) *Maastricht Journal of European and Comparative Law* 15 – 37.

Hertzog, L, Wittesaele, C, Titus, R, Chen, JJ, Kelly, J, Langwenya, N, Baerecke, L & Toska, E 'Seven essential instruments for POPIA compliance in research involving children and adolescents in South Africa' (2021) 117(9/10) *South African Journal of Science* Art. #12290. DOI: *https://doi.org/10.17159/sajs.2021/12290.*

Hickman, E & Petrin, M 'Trustworthy AI and corporate governance: The EU's ethics guidelines for trustworthy artificial intelligence from a company law perspective.' (2021) 22 *European Business Organisation Law Review* 593 – 625.

Hijmans, H 'Right to have links removed: Evidence of effective data protection' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 555 – 563.

Hintze, M & El Emam, K 'Comparing the benefits of pseudonymisation and anonymisation under the GDPR' (2018) 2(2) *Journal of Data Protection & Privacy* 145 – 158.

Hoffmann, LJ 'Commodification beyond data: Regulating the separation of information from noise' (2023) 2 *European Law Open* 424 – 433.

Hofmann, R, Heger, A & Gharibyan, T 'Die Wandlung des Grundrechtsschutzes durch das Bundesverfassungsgericht – *Recht auf Vergessen I* und *II* als "*Solange III*"?' (2019) 102(4) *KritV Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* 277 – 292.

Hoofnagle, C, Van der Sloot, B & Zuiderveen Borgesius, F 'The European Union general data protection regulation: What it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65 – 98.

Hosch, WL 'Malware' *Encyclopedia Britannica,* 30 September 2022. *https://www.britannica.com/technology/malware* (Accessed: 8 December 2022).

Hugo, C & Spruyt, W 'Money laundering, terrorist financing and financial sanctions: South Africa's response by means of the Financial Intelligence Centre Amendment Act 1 of 2017' (2018) 2 *Tydskrif vir die Suid-Afrikaanse / Journal of South African Law Reg* 277 – 255.

Huneberg, S & Berry, K 'Big data and the paradigmatic shift from passive insurer towards risk personalisation' (2022) 2 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 283 – 309.

Hurka, S & Steinebach, Y 'Legal instrument choice in the European Union' (2021) 59(2) *Journal of Common Market Studies* 278 – 296.

Hurter, AP & Van Buer, MG 'The newspaper production/distribution problem' (1996) 17(1) *Journal of Business Logistics* 85 – 107.

Hustinx, P 'EU data protection law: The review of Directive 95/46/EC and the proposed General Data Protection Regulation' EU: European Data Protection Supervisor *Statewatch: Monitoring the State and Civil Liberties in Europe,* 15 September 2014. *https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf* (Accessed: 5 July 2022).

Illia, L, Colleoni, E, & Zyglidopoulos, S 'Ethical implications of text generation in the age of artificial intelligence' (2023) 32(1) *Business Ethics, the Environment & Responsibility* 201 – 210.

Ilori, T 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solutions' *Association for Progressive Communications,* 15 June 2020. *https://africaninternetrights.org/en/updates/data-protection-africa-and-covid-19-pandemic-old-problems-new-challenges-and* (Accessed: 12 December 2023).

Isaak, J & Hanna, MJ 'User data privacy: Facebook, Cambridge Analytica, and privacy protection' (2018) 51(8) *Computer* 56 – 59.

Ismail, N 'Private closed-circuit television surveillance under the Protection of Personal Information Act 4 of 2013' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 20 – 37.

Iyer, D 'An analytical look into the concept of online defamation in South Africa' (2018) 32(2) *Speculum Juris* 124 – 134.

Janeček, V & Malgieri, G 'Commerce in data and the dynamically limited alienability rule' (2020) 21 *German Law Journal* 924 – 943.

Janiesch, C, Zschech, P & Heinrich, K 'Machine learning and deep learning' (2021) 31 *Electronic Markets* 685 – 695.

Jaume-Palasi, L '"*Google Spain* case": Court decision privatises the public sphere' Internet Policy Review 27 May 2014. *https://policyreview.info/articles/news/google-spain-case-court-decision-privatises-public-sphere/291* (Accessed: 22 February 2025).

Jelinić, Z & Radoja, KK 'Mutual recognition of judicial decisions and the right to a fair trial with special focus on the ECHR'S findings in the Case of *Avotiņš v Latvia*' (2018) *EU and Comparative Law Issues and Challenges Series* 571 – 585.

Jenkins, G 'An extended doctrine of implied consent – A digital mediator?' (2021) 52 *International Review of Intellectual Property and Competition Law* 706 – 733.

Jones, ML 'Forgetting made (too) easy' (2015) 58(6) *Communications of the ACM* 34 – 35.

Jones, ML 'The right to a human in the loop: Political constructions of computer automation and personhood' (2017) 47(2) *Social Studies of Science* 216 – 239.

Jones, ML & Kaminski, ME 'An American's guide to the GDPR' (2020) 98 *Denver Law Review* 93 – 128.

Jones, ML, Kaufman, E & Edenberg, E 'AI and the ethics of automating consent' (2018) 16(3) *IEEE Security & Privacy* 64 – 72.

Jooste, Y 'Surveillance capitalism as white world-making' (2021) 53 (1) *Acta Academica* 44 – 67.

Jooste, Y 'The right to deletion: Identity, memory, and surveillance capitalism' (2022) 33(3) *Stellenbosch Law Review* 460 – 483.

Jordan, T 'A genealogy of hacking' (2017) 23(5) *Convergence: The International Journal of Research into New Media Technologies* 528 – 544.

Jukam, K 'OpenAI sued over data collection practices' *Courthouse News Service,* 28 June 2023. *https://www.courthousenews.com/openai-sued-over-data-collection-practices/* (Accessed: 3 July 2023).

Kahvedžić, D 'Cybercrime investigations of mobile phone devices and the cloud in the light of EU safe harbour rulings' (2016) 17 *ERA Forum* 355 – 367.

Ka Mtuze, SS 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43(3) *Obiter* 536 – 569.

Ka Mtuze, SS & Morige, M 'Towards drafting artificial intelligence (AI) legislation in South Africa' (2024) 45(1) *Obiter* 161 – 179.

Karim, MS 'Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?' (2022) 143 *Marine Policy* 105138. DOI: *https://doi.org/10.1016/j.marpol.2022.105138*.

Katzav, G 'Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act' (2022) 139(2) *South African Law Journal* 432 – 470.

Kędzior, M 'GDPR and beyond — A year of changes in the data protection landscape of the European Union' (2019) 19 *ERA Forum* 505 – 509.

Keiter, M 'Criminal law principles in California: Balancing a right to be forgotten with a right to remember' (2018) 13 *California Legal History* 421 – 472.

Keller, KL & Richey, K 'The importance of corporate brand personality traits to a successful 21st century business' (2006) 14 *Journal of Brand Management* 74 – 81.

Kelly, MJ 'What is a web tracker?' *The Mozilla Blog*, 22 October 2019. *https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/* (Accessed: 16 November 2022).

Kelly, MJ & Satolam, D 'The right to be forgotten' (2017) 1 *University of Illinois Law Review* 1 – 64.

Kelsey, E '*Google Spain SL and Google Inc v AEPD and Mario Costeja Gonzalez*: Protection of personal data, freedom of information and the "right to be forgotten"' (2014) 4 *European Human Rights Law Review* 395 – 400.

Kendall, E 'Emoji' *Encyclopedia Britannica*, 24 August 2022. *https://www.britannica.com/topic/emoji* (Accessed: 4 December 2022).

Kerber, W 'Governance of data: Exclusive property vs. access' (2016) 47 *International Review of Intellectual Property and Competition Law* 759 – 762.

Kerber, W & Zolna, KK 'The German Facebook case: The law and economics of the relationship between competition and data protection law' (2022) 54 *European Journal of Law and Economics* 217 – 250.

Kerr, J 'What is a search engine? The simple question the Court of Justice of the European Union forgot to ask and what it means for the future of the right to be forgotten' (2016) 17(1) *Chicago Journal of International Law* 217 – 243.

Kierkegaard, S, Waters, N, Greenleaf, G, Bygrave, LA, Lloyd, I & Saxby, S '30 years on – The review of the Council of Europe Data Protection Convention 108' (2011) 27 *Computer Law & Security Review* 223 – 231.

Kietzmann, J, Lee, LW, McCarthy, IP & Kietzmann, TC 'Deepfakes: Trick or treat?' (2020) 63 *Business Horizons* 135 – 146.

King, MR 'A conversation on artificial intelligence, chatbots, and plagiarism in higher education' (2023) 16(1) *Cellular and Molecular Bioengineering* 1 – 2.

Kirby, N 'What SA law says about the right to be forgotten', 13 June 2014. *https://www.iol.co.za/business-report/opinion/what-sa-law-says-about-the-right-to-be-forgotten-1702860#.VdLApPmqqko* (Accessed: 27 September 2021).

Kirkwood, P '*NT1 & NT2 v Google LLC* – The secretive case giving the UK its first decision on the right to be forgotten' (2018) 4 *European Data Protection Law Review* 384 – 390.

Klaaren, J 'The judicial role in defining national security and access to information in South Africa' (2015) 11(3) *Democracy and Security* 275 – 297.

Klimas, T & Vaiciukaite, J 'The law of recitals in European Community legislation' (2008) 15 *ILSA Journal of International & Comparative Law* 61 – 94.

Kocharyan, H, Vardanyan, L, Hamuľák, O & Kerikmäe, T 'Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy?' (2021) 21(2) *International and Comparative Law Review* 96 – 115.

Kodde, C 'Germany's "Right to be forgotten" – Between the freedom of expression and the right to informational self-determination' (2016) 30 *International Review of Law, Computer & Technology* 17 – 31.

Kokott, J & Sobotta, C 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' (2013) 3(4) *International Data and Privacy Law* 222 – 228.

Koops, BJ 'Forgetting footprints shunning shadows: A critical analysis of the "right to be forgotten" in big data practice' (2011) 8(3) *SCRIPTed* 229 – 256.

Koops, BJ 'The trouble with European data protection law' (2014) 4(4) *International Data Privacy Law* 250 – 261.

Koops, BJ, Hoepman, JH, & Leenes, R 'Open-source intelligence and privacy by design' (2013) 28 *Computer Law & Security Review* 676 – 688.

Koops, BJ & Leenes, R 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data protection law' (2014) 28(2) *International Review of Law, Computers & Technology* 159 – 171.

Koritnik, B 'Discretion of the EU member state when implementing the Data Protection Directive 95/46/EC' (2005) 12(1/2) *Murdoch University Electronic Journal of Law*. *http://classic.austlii.edu.au/au/journals/MurdochUeJlLaw/ 2005/4.html* (Accessed: 18 December 2022).

Kornblith, AB, Herndon II, JE, Weiss, RB *et al* 'Long-term adjustment of survivors of early-stage breast carcinoma, 20 years after adjuvant chemotherapy' (2003) 98(4) *Cancer: Interdisciplinary International Journal of the American Cancer Society* 679 – 689.

Kosta, E 'Algorithmic state surveillance: Challenging the notion of agency in human rights' (2022) 16 *Regulation & Governance* 212 – 224.

Kraus, S, Kanbach, DK, Krysta, PM, Steinhoff, MM & Tomini, N 'Facebook and the creation of the metaverse: Radical business model innovation or incremental transformation?' (2022) 28(9) *International Journal of Entrepreneurial Behavior & Research* 52 – 77.

Krönke, C 'Attention is all you need: ChatGPT und die DSGVO' *VerfBlog*, 14 April 2023. DOI: *10.17176/20230414-190229-0.*

Kruger, H 'The protection of children's right to self-determination in South African law with specific reference to medical treatment and operations' (2018) 21 *Potchefstroomse*

Elektroniese Regsblad / Potchefstroom Electronic Law Journal 1 – 34. DOI: *http://dx.doi.org/10.17159/17273781/2018/v21i0a4609*.

Kuczerawy, A & Ausloos, J 'From notice-and-takedown to notice-and-delist: Implementing *Google Spain*' (2015) 14(2) *Colorado Technology Law Journal* 219 – 257.

Kugler, L 'The war over the value of personal data' (2018) 61(2*) Communications of the Association for Computing Machinery (ACM)* 17 – 19.

Kulk, S & Zuiderveen Borgesius, F '*Google Spain v. González*: Did the court forget about freedom of expression?' (2014) 5 *European Journal of Risk Regulation* 389 – 398.

Kulk, S & Zuiderveen Borgesius, F 'Freedom of expression and right to be forgotten cases in the Netherlands after Google Spain' (2015) 1 *European Data Protection Law Review* 113 – 124.

Kulkarni, A 'Data of 500 million WhatsApp users leaked, up for sale online: Report' *NDTV*, 28 November 2022. *https://www.ndtv.com/world-news/whatsapp-data-leaked-data-phone-numbers-of-500-million-whatsapp-users-leaked-up-for-sale-online-report-3558403* (Accessed: 30 November 2022).

Kuner, C '*Google Spain* in the EU and international context' (2015) 22(1) *Maastricht Journal of Comparative and European Law* 158 – 164.

Kuner, C '*Schrems II* re-examined' *VerfBlog*, 25 August 2020. DOI: *10.17176/20200825-183419-0*.

Kuner, C 'The path to recognition of data protection in India: The role of the GDPR and international standards' (2021) 33 *National Law School of India Review* 69 – 91.

Labuschagne, H 'Apple vs Google vs Facebook — This is who tracks the most personal data types' *My Broadband*, 26 August 2022. *https://mybroadband.co.za/news/internet/458095-apple-vs-google-vs-facebook-this-is-who-tracks-the-most-personal-data-types.html* (29 January 2024).

Lam, C 'Unsafe harbor: The European Union's demand for heightened data privacy standards in *Schrems v. Irish Data Protection Commissioner*' (2017) 40(3) *Boston College International and Comparative Law Review Electronic Supplementary* 1 – 13.

Lane, L 'Clarifying human rights standards through artificial intelligence initiatives' (2022) 71(4) *International & Comparative Law Quarterly* 915 – 944.

Larson, E 'Tracking criminals with internet protocol addresses: Is law enforcement correctly identifying perpetrators?' (2017) 18 *North Carolina Journal of Law & Technology* 316 – 358.

Laurer, M & Seidl, T 'Regulating the European data-driven economy: A case study on the

general data protection regulation' (2021) 13(2) *Policy & Internet* 257 – 277.

Laursen, F 'The founding treaties of the European Union and their reform' (31 August 2016) *Oxford Research Encyclopedia of Politics* 151. *https://oxfordre.com/politics /view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-151* (Accessed: 10 February 2024).

Lawack, V, Mupangavanhu, BM & Olivier, E 'The protection of consumers of retail central bank digital currency – Some considerations' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 285 – 306.

Lazzarelli, F 'The mobile borders between the right to be forgotten and freedom of information' (2023) 8(2) *Italian Law Journal* 925 – 938.

Le Blond, J 'German politicians' personal data leaked online' *The Guardian*, 4 January 2019. *https://www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online* (Accessed: 22 January 2019).

Lee, DH & Schleyer, T 'Social tagging is no substitute for controlled indexing: A comparison of medical subject headings and CiteULike tags assigned to 231,388 papers' (2012) 63(9) *Journal of the American Society for Information Science and Technology* 1747 – 1757.

Leets, L 'Responses to internet hate sites: Is speech too free in cyberspace?' (2001) 6(2) *Communication Law & Policy* 287 – 317.

Lim, W 'Assessing the implications of digital contact tracing for COVID-19 for human rights and the rule of law in South Africa' (2020) 20(2) *African Human Rights Law Journal* 540 – 557.

Lindroos-Hovinheimo, S 'Who controls our data? The legal reasoning of the European Court of Justice in *Wirtschaftsakademie Schleswig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*' (2019) 28(2) *Information & Communications Technology Law* 225 – 238.

Lock, T 'The future of EU Human Rights Law: Is accession to the ECHR still desirable? (2020) 7(2) *Journal of International and Comparative Law* 427 – 447.

Lynskey, O 'Control over personal data in a digital age: G*oogle Spain v AEPD and Mano Costeja Gonzalez*' (2015) 78 (3) *The Modern Law Review* 522 – 534.

Maat, EP '*Google v. CNIL*: A commentary on the territorial scope of the right to be forgotten' (2022) 30(2) *European Review of Private Law* 241 – 261.

MacDonnell, P 'The European Union's proposed equality and data protection rules: An existential problem for insurers?' (2015) 35(2) *Economic Affairs* 225 – 239.

Magrath, P 'The Genie and the Lamp: How can artificial intelligence help us find new case law?' (2022) 22 *Legal Information Management* 114 – 118.

Maimela, C 'The reasonable accommodation of employees with cancer and their right to privacy in the workplace' (2018) 21 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1- 31. DOI: *http://dx.doi.org/10.17159/1727-3781/2018/v21i0a1703*.

Malahleka, M 'The right to data portability: A ghost in the protection of personal information' (2023) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 1 – 19.

Malahleka, M 'The problem of trans-border information flows in the protection of personal information' (2024) 27 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 41. DOI: *http://dx.doi.org/10.17159/1727-3781/2024/v27i0a14296*.

Malgieri, G & Custers, B 'Pricing privacy – The right to know the value of your personal data' (2018) 34 *Computer Law & Security Review* 289 – 303.

Mantelero, A 'Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution' (2012) 3(2) *European Journal for Law and Technology* 1 – 6. *https://ejlt.org/index.php/ejlt/article/view/96* (Accessed: 28 November 2022).

Mantelero, A 'The future of data protection: Gold standard vs. global standard' (2021) 40 *Computer Law & Security Review* 105500. DOI: *https://doi.org/10.1016/j.clsr.2020.105500*.

Marais, ME 'Hate speech in the Equality Act following the Constitutional Court judgment in *Qwelane v SAHRC*' (2023) 26 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 33. DOI: *http://dx.doi.org/10.17159/1727-3781/2023/v26i0a15438*.

Marelli, M 'The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders' (2023) 50 *Computer Law & Security Review* 105849. DOI: *https://doi.org/10.1016/j.clsr.2023.105849*.

Marosi, J 'Who controls a Facebook page?' *VerfBlog,* 6 June 2018. DOI: *10.17176/20180607-094351-0*.

Mashinini, N 'The impact of deepfakes on the right to identity: A South African perspective' (2020) 32(5) *SA Mercantile Law Journal* 407 – 436.

Mashinini, N 'The processing of personal information using remotely piloted aircraft systems

in South Africa' (2020) 51(1) *De Jure Law Journal* 140 – 158.

Mathews, J 'Some kind of right' (2020) 21 *German Law Journal* 40 – 44.

Mauz, G 'Was man nach alter Tradition Meuterei nennt' (1983) 1 *Der Spiegel* 58 – 59. *https://www.spiegel.de/politik/was-man-nach-alter-tradition-meuterei-nennt-a-c4c213f9-0002-0001-0000-000014018172* (Accessed: 22 August 2022).

Mayer-Schönberger, V 'The internet is rotting – Let's embrace it' *The Conversation: Academic rigour, journalistic flair*, 25 July 2019. *https://theconversation.com/the-internet-is-rotting-lets-embrace-it-116239* (Accessed: 1 March 2025).

Mayer-Schönberger, V & Padova, Y 'Regime change? Enabling big data through Europe's new Data Protection Regulation' (2016) XVII *The Columbia Scientific & Technology Law Review* 315 – 335.

Mazurek, G & Małagocka, K 'Perception of privacy and data protection in the context of the development of artificial intelligence' (2019) 6(4) *Journal of Management Analytics* 344 – 364.

McAuliffe, K 'Hybrid texts and uniform law? The multilingual case law of the Court of Justice of the European Union' (2011) 24 *International Journal for the Semiotics of Law* 97 – 115.

McDermott, Y 'Conceptualising the right to data protection in an era of big data' (2017) 4(1) *Big Data & Society* 1 – 7. DOI: *10.1177/2053951716686994*.

McGoldrick, D 'Developments in the right to be forgotten' (2013) 13 *Human Rights Law Review* 761 – 776.

Mellet, K & Beauvisage, T 'Cookie monsters. Anatomy of a digital market infrastructure' (2020) 23(2) *Consumption Markets & Culture* 110 – 129.

Merriam-Webster 'Paywall' *Merriam-Webster.com Dictionary*. *https://www.merriam-webster.com/dictionary/paywall* (Accessed: 25 November 2023).

Merriam-Webster 'Web crawler' *Merriam-Webster.com Dictionary*. *https://www.merriam-webster.com/dictionary/web%20crawler* (Accessed 5 March 2024).

Mesnil, M 'What do we mean by the right to be forgotten? An analysis of the French case study from a lawyer's perspective' (2018) 15(B) *Journal of Cancer Policy*' 122 – 127.

Miadzvetskaya, Y & Van Calster G 'Google at the Kirchberg Dock. On delisting requests, and on the territorial reach of the EU's GDPR.' (2020) 6(1) *European Data Protection Law Review* 143 – 151.

Mik, E 'Contracts governing the use of websites' (2016) *Singapore Journal of Legal Studies* 70 – 94.

Milkaite, I & Lievens, E 'Children's rights to privacy and data protection around the world: Challenges in the digital realm' (2019) 10(1) *European Journal of Law and Technology* 1 – 24. *https://biblio.ugent.be/publication/8618586* (Accessed 19 February 2025).

Milker, J 'Karlsruhe im Luxemburger Gewand, aberdennoch eigenständig: Der Umgang mit Online-Archiven im Lichte der Beschlüsse des BVerfG vom 6.11.2019 (1 BvR 16/13 und 1 BvR 276/17)' *VerfBlog*, 29 November 2019. DOI: *10.17176/20191129-180939-0*.

Millard, D & Bascerano, EG 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Review* 1 – 38. DOI: *http://dx.doi.org/10.17159/1727-3781/2016/v19i0a555*.

Milossi, M, Alexandropoulou-Egyptiadou, E & Psannis, KE 'AI ethics: Algorithmic determinism or self-determination? The GPDR approach' (2021) 9 IEEE Access 58455 – 58466.

Mswela, MM 'Tagging and tracking of persons with albinism: A reflection of some critical human rights and ethical issues arising from the use of the Global Positioning System (GPS) as part of a solution to cracking down on violent crimes against persons with albinism' (2019) 22 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Review* 1 – 28. DOI: *http://dx.doi.org/10.17159/1727-3781/2019/v22i0a5206.*

Mujuzi, JD 'Spent convictions in Mauritius: Analysing the Police and Criminal Evidence Bill, 2013' (2015) 3 *South African Journal of Criminal Justice* 284 – 302.

Murphy, MH 'Assessing the implications of *Schrems II* for EU–US Data Flow' (2021) 71 *International and Comparative Law Quarterly* 245–262.

MyWayLife 'Can I get life insurance if I have cancer?' MyWayLife Blog, 17 June 2018. *https://www.miwaylife.co.za/blog/can-i-get-life-insurance-if-i-have-cancer/* (Accessed: 13 April 2024).

Nagumotu, K 'Deepfakes are taking over social media: Can the law keep up?' (2022) 62 *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property* 102 – 146.

Naude, A & Papadopoulos, S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 51 – 68.

Naude, A & Papadopoulos, S 'Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)' (2016) 79 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 213 – 230.

Nebbia, P 'The *Schrems* judgments: A silent revolution for the Member States' procedural autonomy?' (2021) 22 *ERA Forum* 327 – 336.

Neethling, J 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18 – 28.

Nettesheim, M 'Digital autonomy in contractual relationships: On the relationship between contractual autonomy and control over data' *VerfBlog*, 18 October 2022. DOI: *10.17176/20221018-130331-0*.

Neuwirth, RJ 'Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA)' (2023) 48 *Computer Law & Security Review* 105798. DOI: *https://doi.org/10.1016/j.clsr.2023.105798*.

Newman, J 'How "Somebody's Watching Me" singer Rockwell created a paranoid pop classic' *Rolling Stone*, 7 December 2016. *https://www.rollingstone.com/ music/music-features/how-somebodys-watching-me-singer-rockwell-created-a-paranoid-pop-classic-125907/amp/* (Accessed: 15 December 2022).

Njotini, MN 'Preserving the integrity of medical-related information – How "informed" is consent?' 2018 (21) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 20. DOI: *http://dx.doi.org/10.17159/1727-3781/2018/v21i0a3400*.

Njotini, M 'Securing shareholder information in the digital age — An analysis of the proposed amendments to section 26 of the Companies Act' (2020) 32(3) *South African Mercantile Law Journal* 334 – 359.

Nunziato, DC 'The fourth year of forgetting: The troubling expansion of the right to be forgotten' (2018) 39(4) *University of Pennsylvania Journal of International Law* 1011 – 1064.

O'Hara, K 'The right to be forgotten: The Good, the Bad, and the Ugly' (2015) July/August *The Digital Citizen* 73 – 79.

O'Leary, S 'A tale of two cities: Fundamental rights protection in Strasbourg and Luxembourg' (2018) 20 *Cambridge Yearbook of European Legal Studies* 3 – 31.

O'Neill, A 'BREXIT, democracy and the rule of law' (2020) *European Law Journal* 1 – 46.

Ojanen, T 'Making the essence of fundamental rights real: The Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter' (2016) 12 *European Constitutional Law Review* 318 – 329.

Ong, B & Toh, DJ 'Digital dominance and social media platforms: Are competition authorities up to the task?' (2023) 54 *International Review of Intellectual Property and*

Competition Law 527 – 572.

Orgad, L 'The preamble in constitutional interpretation' (2010) 8(4) *International Journal of Constitutional Law* 714 – 738

Ovčak Kos, M 'The right to be forgotten and the media' (2019) 11(2) *LeXonomica* 195 – 212.

Pang, XZ 'Civil law protection of personal information in the era of big data' (2021) 8 *Open Access Library Journal* e8016. DOI: *https://doi.org/10.4236/oalib.1108016*.

Papadopoulos, NA 'Revisiting the preamble of the European Social Charter: Paper tiger or blessing in disguise?' (2022) 22 *Human Rights Law Review* 1 – 21.

Papadopoulos, S 'The long road to mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator*' (2022) 85 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 397 – 408.

Papastefanou, S 'Smart grids and machine learning in Chinese and Western Intellectual Property Law' (2021) 52 *International Review of Intellectual Property and Competition Law* 989 – 1019.

Parker, ES, Cahill, L & McGaugh, JL 'A case of unusual autobiographical remembering' (2006) 12 *Neurocase* 35 – 49.

Peguera, M 'In the aftermath of *Google Spain*: How the right to be forgotten is being shaped in Spain by courts and the Data Protection Authority' (2015) 23 *International Journal of Law and Information Technology* 325 – 347.

Penfold, G & Milo, D 'Media freedom and the law of privacy: *NM & Others v Smith & Others (Freedom of Expression Institute as amicus curiae)* 2007 (5) SA 250 (CC): case comments' (2008) 1(1) *Constitutional Court Review* 311 – 334.

Perper, R 'Chinese citizens will soon need to scan their face before they can access internet services or get a new phone number' *Business Insider South Africa,* 10 October 2019. *https://www.businessinsider.co.za/china-to-require-facial-id-for-internet-and-mobile-services-2019-10* (Accessed: 11 October 2019).

Petkova, B 'Privacy as Europe's First Amendment' (2019) 25 *European Law Journal* 140 – 154.

Peuker, E 'The EU General Data Protection Regulation: Powerful tool for data subjects?' *VerfBlog,* 22 June 2016. DOI: *10.17176/20160622-161620*.

Pfeiffer, G & Timmerbeil, S 'US-American company law – An overview' (2008) 6 *Zeitschrift für das Juristische Studium* 597 – 599.

Phillips, J '*South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku*: The rejection of the International Holocaust Remembrance

Alliance definition' (2023) *South African Journal on Human Rights* 1 – 11. DOI: *10.1080/02587203.2023.2275311*.

Phillips, M 'International data-sharing norms: From the OECD to the General Data Protection Regulation (GDPR)' (2018) 137 *Human Genetics* 575 – 582.

Piza, EL, Welsh, BC, Farrington, DP & Thomas, AL 'CCTV surveillance for crime prevention' (2019) 18 *Criminology & Public Policy* 135 – 159.

Politou, E, Alepis, E & Patsakis, C 'Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions' (2018) 4(1) *Journal of Cybersecurity* tyy001. DOI: *https://doi.org/10.1093/cybsec/tyy001*.

Popenici, SAD & Kerr, S 'Exploring the impact of artificial intelligence on teaching and learning in higher education' (2017) 12(22) *Research and Practice in Technology Enhanced Learning* 1 – 13. DOI: *10.1186/s41039-017-0062-8*.

Poullet, Y 'EU data protection policy: The Directive 95/46/EC: Ten years after' (2006) 22 *Computer Law & Security Report* 206 – 217.

Poullet, Y 'Is the general data protection regulation the solution?' (2018) 34 *Computer Law & Security Review* 773 – 778.

Powles, J 'The case that won't be forgotten' (2015) 47 *Loyola University Chicago Law Journal* 583 – 615.

Princen, S, Schimmelfennig, F, Sczepanski, R, Smekal, H & Zbiral, R 'Different yet the same? Differentiated integration and flexibility in implementation in the European Union' (2022) *West European Politics*. DOI: *10.1080/01402382.2022.2150944*.

Prinsen, L & Muller, EC 'The leading causes behind medico-legal claims and the use of mediation as a possible solution' (2023) 34(4) *Stellenbosch Law Review* 387 – 405.

Purtova, N 'Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table . . . and back on again?' (2014) 30 *Computer Law & Security Review* 6 – 24.

Purtova, N 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) *Law, Innovation and Technology* 40 – 81.

Pushka, J 'The applicability of the Personal Information Protection and Electronic Documents Act to de-indexing internet search engine results' (2019) 19 *Asper Review of International Business and Trade Law* 175 – 194.

Rascão, JP 'Freedom of expression, privacy, and ethical and social responsibility in democracy in the digital age' (2020) 1(3) *International Journal of Business Strategy and Automation* 1 – 23. DOI: *10.4018/IJBSA.2020070101*.

Reddy, E 'Policing the Onion Router (Tor) crypto-markets on the dark web: An analysis of South African investigatory powers' (2023) 36(3) *South African Journal of Criminal Justice* 406 – 433.

Rodriguez-Izquierdo Serrano, M 'The Spanish Constitutional Court and fundamental rights adjudication after the first preliminary reference' (2015) 16(6) *German Law Journal* 1509 – 1528.

Rolph, D 'Liability for the publication of third party comments: *Fairfax Media Publications Pty Ltd v Voller*' (2021) 43(2) *Sydney Law Review* 225 – 240.

Roos, A 'Core principles of data protection law' (2006) 39(1) *Comparative and International Law Journal of Southern Africa* 102 – 130.

Roos, A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *South African Law Journal* 400 – 433.

Roos, A 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Review* 62 – 109.

Roos, A 'Privacy in the Facebook era: A South African legal perspective' (2012) 129(2) *South African Law Journal* 375 – 402.

Roos, A 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected "content principles"' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* #7985. DOI: *https://doi.org/10.25159/2522-3062/7985*.

Roos, A 'Data protection principles under the GDPR and the POPI Act: A comparison' (2023) 86 *Tydskrif vir Hedendagse Romeins-Hollandse Reg* 1 – 26.

Roos, A & Slabbert, M 'Defamation on Facebook: *Isparta v Richter* 2013 6 SA 529 (GP)' (2014) 7(6) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Review* 2845 – 2868.

Rosen, J 'The web means the end of forgetting' *New York Times Magazine,* 21 July 2010. *https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html* (Available: 28 November 2022).

Rosen, J 'Free speech, privacy, and the web that never forgets' (2011) 9 *Journal on Telecommunications & High Technology Law* 345 – 356.

Rosen, J 'Symposium issue: The right to be forgotten' (2012) 64 *Stanford Law Review Online* 88 – 92.

Rosenberg, W 'The mother's right to privacy in infant abandonment cases' (2022) 1 *Tydskrif*

vir die Suid-Afrikaanse Reg / Journal of South African Law 92 – 105.

Rotenberg, M '*Schrems II,* from Snowden to China: Toward a new alignment on transatlantic data protection' (2020) 26 *European Law Journal* 141 – 152.

Ryngaert, C & Taylor, M 'The GDPR as global data protection regulation?' (2020) 114 *AJIL Unbound* 5 – 9.

Saltzman, I 'The status of national implementation of Directive 95/46/EC on the processing and free movement of personal data' (1996) 18(12) *European Intellectual Property Review* 680 – 683.

Sánchez de Diego, M 'Right to one's own image in Spain: What it is and what it is not' (2018) 8 *Journal of Information Policy* 401 – 416.

Sartor, G 'Search Engines as controllers: Inconvenient implications of a questionable classification' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 564 – 573.

Sartor, G 'The right to be forgotten: Balancing interests in the flux of time' (2016) 24 *International Journal of Law and Information Technology* 72 – 98.

Saville, G 'Surveillance and crime prevention' (2004) 3 *Criminology & Public Policy* 493 – 496.

Schreurs, S, Van der Kammen, N & Oosterhuis, S 'A Dutch perspective on the "right to be forgotten": An analysis of Dutch Lower Court judgments in light of the *Hoge Raad* Judgment of 24 February 2017 and the *Costeja* Judgment' (2022) 30(2) *European Review of Private Law* 315 – 348.

Schwartz, PM 'Free speech vs. information privacy: Eugene Volokh's First Amendment Jurisprudence' (1999 – 2000) 52 *Stanford Law Review* 1559 – 1572.

Schweda, S 'Right to be forgotten also applies to online news archive, Supreme Court Rules' (2015) 1 *European Data Protection Law Review* 301 – 304.

Senft, TM 'Emoticon' *Encyclopedia Britannica,* 27 February 2022. *https://www.britannica.com/topic/emoticon* (Accessed: 4 December 2022).

Seyfert, R 'Algorithms as regulatory objects' (2022) 25(11) *Information, Communication & Society* 1542 – 1558.

Shaik-Peremanov, N 'Basel II - The right to privacy: A South African perspective' (2009) 21 *South African Mercantile Law Journal* 546 – 554.

Shanapinda, S 'Asymmetry in South Africa's regulation of customer data protection: Unequal treatment between mobile network operators (MNOs) and over-the-top (OTT) service providers' (2019) 23 *The African Journal of Information and Communication (AJIC)* 1

– 20

Shapiro, S ‘Places and spaces: The historical interaction of technology, home, and privacy’ (1998) 14(4) *The Information Society: An International Journal* 275 – 284.

Shatz, S & Chylik, SE ‘The California Consumer Privacy Act of 2018: A sea change in the protection of California consumers’ personal information’ (2019) 75 *The Business Lawyer* 1917 – 1924.

Shay, RM & Moleya, NI ‘Discovering the value of liberty in intellectual property adjudication: A methodological critique of the reasoning in *Discovery Ltd v Liberty Group Ltd* 2020 4 SA 160 (GJ)’ (2021) 4 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 33. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10703*.

Silva, F ‘The right to be forgotten’ *Law Society Journal* (1 December 2023). *https://lsj.com.au/articles/the-right-to-be-forgotten/#* (Accessed: 4 March 2025).

Singh, P ‘Can an emoji be considered as defamation? A legal analysis of *Burrows v Houda* [2020] NSWDC 485’ (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 26. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a8918*.

Singleton, S ‘Balancing a right to be forgotten with a right to freedom of expression in the wake of *Google Spain v. AEPD*’ (2015) 44 *Georgia Journal of International and Comparative Law* 165 – 194.

Sive, D & Price, A ‘Regulating expression on social media’ (2019) 136(1) *South African Law Journal* 51 – 83.

Slane, A ‘Search engines and the right to be forgotten: Squaring the remedy with Canadian Values on personal information flow’ (2018) 55 *Osgoode Hall Law Journal* 349 – 397.

Sookman, B ‘US Court thumbs its nose at Supreme Court of Canada: *Google v. Equustek*’ (2018) 30(3) *Intellectual Property Journal* 375 – 405.

Spillane, J ‘Google’s “right to be forgotten” – A dream come true for job seekers?’ *Business 2 Community*, 17 July 2014. *https://www.business2community.com/human-resources/googles-right-forgotten-dream-come-true-job-seekers-0946918* (Accessed: 26 November 2022).

Stancescu-Cojocaru, R ‘Overview of the recent case-law of the European Court of Human Rights on the balance between the right to private life and the right to freedom of expression’ (2023) 24 *ERA Forum* 261 – 274.

Staunton, C & De Stadler, E ‘Protection of Personal Information Act No. 4 of 2013:

Implications for biobanks' (2019) 109(4) *South African Medical Journal* 232 – 234.

Steinbeis, M 'Was hilft mir das Recht auf Vergessen, wenn ich nicht für mich sein kann?' *VerfBlog*, 31 May 2014. *https://verfassungsblog.de/hilft-mir-das-recht-auf-vergessen-wenn-ich-nicht-fuer-mich-sein-kann/* (Accessed 14 January 2023).

Stevanovic, D, An, A & Vlajic, N 'Feature evaluation for web crawler detection with data mining techniques' (2012) 39 *Expert Systems with Applications* 8707 – 8717.

Stiakakis, E, Georgiadis, CK & Andronoudi, A 'Users' perceptions about mobile security breaches' (2016) 14 *Information Systems and e-Business Management* 857 – 882.

Stoop, PN & Chürr, C 'Unpacking the right to plain and understandable language in the Consumer Protection Act 68 of 2008' (2013) 16(5) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 515 – 555.

Stuurman, K & Lachaud, E 'Regulating AI. A label to complete the proposed act on artificial intelligence' (2022) 44 *Computer Law & Security Review* 105657. DOI: *https://doi.org/10.1016/j.clsr.2022.105657*.

Swales, L 'Protection of Personal Information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)" (2016) 28 *South African Mercantile Law Journal* 49 – 84.

Swales, L 'The Protection of Personal Information Act and data de-identification' (2021) 117(7/8) *South African Journal of Science* Art #10808. DOI: *https://doi.org/10.17159/sajs.2021/10808*.

Swales, L, Thaldar, D & Donnelly, D-L 'Why research institutions should indemnify researchers against POPIA civil liability' (2022) 118(3/4) *South African Journal of Science* 22 – 24.

Sychenko, E & Chernyaeva, D 'The impact of the ECHR on employee's privacy protection' (2019) 12(2) *Italian Labour Law e-Journal* 171 – 188.

Tanczer, LM '50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers' (2020) 41(1) *Contemporary Security Policy* 108 – 128.

Taylor, H 'Can I get life insurance after a cancer diagnosis?' *FA News*, 18 October 2016. *https://www.fanews.co.za/article/life-insurance/9/general/1202/can-i-get-life-insurance-after-a-cancer-diagnosis/21225* (Accessed: 13 April 2024)

Thaldar, D 'Does data protection law in South Africa apply to pseudonymised data?' (2023) 14 *Frontiers in Pharmacology* 1238749. DOI: *10.3389/fphar.2023.1238749*.

Thalder, D & Shozi, B 'Is open-identity gamete donation lawful in South Africa?' (2022) 112(6) *South African Medical Journal* 409 – 412 at 411 – 412

Thalder, DW & Steytler, M 'Time for Cinderella to go to the ball: Reflections on the right to freedom of scientific research' (2021) 138(2) *South African Law Journal* 258 – 286.

Thaldar, DW & Townsend, BA 'Exempting health research from the consent provisions of POPIA' (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 31. DOI: *http://dx.doi.org/10.17159/1727-781/2021/v24i0a10420*.

Thomson, R, Torenvlied, R & Arregui, J 'The paradox of compliance: Infringements and delays in transposing European Union Directives' (2007) 37 *British Journal of Political Science* 685 – 709.

Thorbecke, C 'OpenAI, maker of ChatGPT, hit with proposed class action lawsuit alleging it stole people's data' *CNN Business*, 28 June 2023. *https://edition.cnn.com/2023/06/28/tech/openai-chatgpt-microsoft-data-sued/index.html* (Accessed: 29 June 2023).

Thylstrup, NB 'The World's Digital Memory Is at Risk' *New York Times (Online)*, 21 June 2023. Proquest One Academic. *https://www.proquest.com/?accountid=158225* (Accessed: 26 February 2025).

Tikkinen-Piri, C, Rohunen, A & Markkula, J 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 – 153.

Tomlinson, H '*Hurbain v Belgium*: The Grand Chamber of the European Court of Human Rights upholds decision that order anonymising newspaper archive did not violate article 10' (2024) 35(1) *Entertainment Law Review* 30 – 35.

Toth R, & Trifonova, T 'Somebody's Watching Me: Smartphone use tracking and reactivity' (2021) 4 *Computers in Human Behavior Reports* 100142. DOI: *https://doi.org/10.1016/j.chbr.2021.100142*.

Trottier, D 'Denunciation and doxing: Towards a conceptual model of digital vigilantism' (2020) 21(3-4) *Global Crime* 196 – 212.

Ucar, M & Yalcintas, A 'GDPR and digital protectionism in the EU: The cases of Android and iOS' (2023) 57(4) *Journal of Economic Issues* 1079 – 1094.

Ugland, E & Lambe, JL 'Newspaper theft, self-preservation and the dimensions of censorship' (2010) 15(4) *Communication Law and Policy* 365 – 403.

Ulbricht, L & Yeung, K 'Algorithmic regulation: A maturing concept for investigating regulation of and through algorithms' (2022) 16 *Regulation & Governance* 3 – 22.

Van Alsenoy, B 'Allocating responsibility among controllers, processors, and "everything in between": The definition of actors and roles in Directive 95/46/EC' (2012) 28

Computer Law & Security Review 25 – 43.

Van Alsenoy, B & Koekkoek, M 'Internet and jurisdiction after *Google Spain*: The extraterritorial reach of the "right to be delisted"' (2015) 5(2) *International Data Privacy Law* 105 – 120.

Van der Merwe, D 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17(1) *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Review* 296 – 328.

Van der Sloot, B & Wagensveld, Y 'Deepfakes: Regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review* 105716. DOI: *https://doi.org/10.1016/j.clsr.2022.105716*.

Van Deventer, S 'Problems relating to the formation of online contracts: A South African perspective' (2021) 138(2) *South Africa Law Journal* 219 – 257.

Van Deventer, S 'Regulating substantively unfair terms in online contracts' (2021) 32(2) *Stellenbosch Law Review* 518 – 542.

Van Eck, M 'Error 404 or an error of judgment? An ethical framework for the use of ChatGPT in the legal profession' (2024) 4 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 469 – 490.

Van Oyen, JS, Lange, M & Kreinsen, S 'The right to be forgotten in Germany' (2022) 30(2) *European Review of Private Law* 291 – 314.

Van Schagen, E 'More consistency and legal certainty in the private law *acquis*: A plea for better justification for the harmonization of private law' (2012) 19(1) *Maastricht Journal of European and Comparative Law* 37 – 62.

Van Staden, M 'A comparative analysis of common-law presumptions of statutory interpretation' (2015) 26(3) *Stellenbosch Law Review* 550 – 582.

Vavra, AN 'The right to be forgotten: An archival perspective' (2018) 81(1) *The American Archivist* 100 – 111.

Veale, M, Binns, R & Ausloos, J 'When data protection by design and data subject rights clash' (2018) 8(2) *International Data Privacy Law* 105 – 123.

Veale, M & Zuiderveen Borgesius, F 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach' (2021) 22(4) *Computer Law Review International* 97 – 112.

Venter, R 'The role of freedom of expression in a democratic system (part 1)' (2018) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 52 – 87.

Venter, R 'The role of freedom of expression in a democratic system (part 2)' (2018) 1 *Tydskrif vir die Suid-Afrikaanse Reg / Journal of South African Law* 308 – 343.

Villaronga, EF, Kiesberg, P & Li, T 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law & Security Review* 304.

Walden, I 'The application of Directive 95/46/EC' (1996) 3 *EDI Law Review* 85 – 98.

Warikandwa, TV 'Personal data security in South Africa's financial services market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation compared' (2021) 24 *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law Journal* 1 – 32. DOI: *http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727*.

Warren, SD & Brandeis, LD 'Right to Privacy' (1890-1891) 4 *Harvard Law Review* 193 – 220.

Weideman, K 'A matter of choice: The German Federal Supreme Court's interim decision in the abuse-of-dominance proceedings *Bundeskartellamt v. Facebook* (Case KVR 69/19)' (2020) 51 *International Review of Intellectual Property and Competition Law* 1168 – 1181.

Weideman, K 'Profiling and (automated) decision-making under the GDPR: A two-step approach' (2022) 45 *Computer Law & Security Review* 105662. DOI: *https://doi.org/10.1016/j.clsr.2022.105662*.

Weitzenboeck, EM, Lison, P, Cyndecka, M & Langford, M 'The GDPR and unstructured data: Is anonymization possible' (2022) 12(3) *International Data Privacy Law* 184 – 206.

Welsh, S 'Forgetting as a function: When the internet wants to remember, how can we learn to forget?' (2020) 24(2) *Kairos: A Journal of Rhetoric, Technology, and Pedagogy*. *https://kairos.technorhetoric.net/24.2/disputatio/welsh/index.html* (Accessed: 1 March 2025).

White, M 'Is the incompatibility of UK data retention law with EU law really a victory?' (2021) 41(1) *Legal Studies* 130 – 155.

Whittaker, L, Kietzmann, TC, Kietzmann, J & Dabirian, A '"All around me are synthetic faces": The mad world of AI-Generated media' (2020) 22(5) *IT Professional* 90 – 99.

Willers, PA 'Betriebsrat – einfach erklärt!' W.A.F. Betreibts Wissen. *https://www.betriebsrat.com/wissen/betriebsrat* (Accessed: 28 September 2021).

Wiśniewski, A 'The European Court of Human Rights and internet-related cases' (2021) 26(3) *Białostockie Studia Prawnicze* 109 – 133.

Wolf, C 'Impact of the CJEU's right to be forgotten: Decision on search engines and other

service providers in Europe' (2014) 21(3) *Maastricht Journal of Comparative and European Law* 547 – 554.

Wolters, PTJ 'The security of personal data under the GDPR: A harmonized duty or a shared responsibility?' (2017) 7(3) *International Data Privacy Law* 165 – 178.

Wong, R 'Data protection: The future of privacy' (2011) 27 *Computer Law & Security* 53 – 57.

Wong, R 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229 – 244.

Woods, DW & Böhme, R 'The commodification of consent' (2022) 115 *Computers & Security* 102605. DOI: *https://doi.org/10.1016/j.cose.2022.102605*.

Woods, FA & Ruscher, JB 'Viral sticks, virtual stones: Addressing anonymous hate speech online' (2021) 55(3) *Patterns of Prejudice* 265 – 289.

Wulf, AJ & Seizov, O '"Please understand we cannot provide further information": Evaluating content and transparency of GDPR-mandated AI disclosures' (2024) 39 *AI & Society* 235 – 256.

Wulff, CM 'The right to be forgotten in post-*Google Spain* case law: An example of legal interpretivism in action?' (2020) 26 *Comparative Law Review* 255 – 279.

Xiao, G 'Bad bots: Regulating the scraping of public personal information' (2020) 34(2) *Harvard Journal of Law & Technology* 701 – 732.

Zalnieriute, M '*Google LLC v. Commission Nationale de l'informatique et des Libertés* (*CNIL*)' (2020) 114(2) *The American Journal of International Law*' 261 – 267.

Zalnieriute, M '*Big Brother Watch and Others v the United Kingdom*' (2022) 116(3) *American Journal of International Law* 585 – 592.

Zalnieriute, M & Churches, G 'When a "like is not a "like": A new fragmented approach to data controllership' (2020) 83(4) *Modern Law Review* 861 – 876.

Zech, H 'Information as property' (2015) 6 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 192 – 197.

Zufall, F 'Challenging the EU's right to be forgotten: Society's right to know in Japan' (2019) 5 *European Data Protection Law Review* 17 – 25.

Zunger, Y 'Computer science faces an ethics crisis: The Cambridge Analytica scandal proves it.' *The Boston Globe*, 22 March 2018. *https://www.delaat.net/ecis/Computer-science-faces-an-ethics-crisis-The-Boston-Globe.pdf* (Accessed: 22 January 2019).

CONFERENCE PAPERS AND CONFERENCE PROCEEDINGS

Al-Fedaghi, S 'How sensitive is your personal information? In *Proceedings of the 2007 ACM symposium on Applied computing (SAC '07)* (11 – 15 March 2007, Seoul, Korea) 165 – 169.

Baldassarre, MT, Caivano, D, Fernandez Nieto, B, Gigante, D & Ragone, A 'The social impact of generative AI: An analysis on ChatGPT' In *Proceedings of the 2023 ACM Conference on Information Technology for Social Good (GoodIT '23)* (6 – 8 September 2023, Lisbon, Portugal) 363 – 373.

Bertram, T, Bursztein, E, Caro S *et al* 'Five years of the right to be forgotten' In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*) (11 – 15 November 2019, London, United Kingdom) 959 – 972.

Botha, J, Grobler, MM, Hahn, J, & Eloff, MM 'A high-level comparison between the South African Protection of Personal Information Act and international data protection laws.' In *Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS)* (2 – 3 March 2017, Dayton, Ohio, USA). *https://www.researchgate.net/publication/311495321_A_High-Level_Comparison_between_the_South_African_Protection_of_Personal_Information_Act_and_International_Data_Protection_Laws* (Accessed: 23 May 2024).

Canadian Journalism Foundation 'Striking the Balance: Privacy and Freedom of Expression in a Digital Age: A half day symposium' (The Globe and Mail Centre, Toronto, Canada, 4 April 2018).

Canh, TT 'The right to be forgotten according to European Union law in the face of challenges of artificial intelligence to human's private life' In *Proceedings of the 3rd International Conference On Science, Technology and Society Studies (STS 2022)* (22 July 2022, Ho Chi Minh City, Vietnam) 315 – 320.

Franzen, D, Nuñez von Voigt, S, Sörries, P, Tschorsch, F & Müller-Birn, C 'Am I private and if so, how many? Communicating privacy guarantees of differential privacy with risk communication' In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '22*) (7 – 11 November 2022, Los Angeles, California, United States of America) 1125 – 1139.

Govender, I 'Mapping "Security Safeguard" Requirements in a data privacy legislation to an international privacy framework: A compliance methodology' In *2015 Information Security for South Africa* (*ISSA*) (12 – 13 August 2015, Johannesburg, South Africa) 1 – 8.

Gumzej, N 'Technical solutions supporting the online RTBF in the CJEU and ECHR jurisprudence' In *Proceedings of the 2023 46th MIPRO ICT and Electronics Convention (MIPRO)* (22 – 26 May 2023, Opatija, Croatia) 1467 – 1473.

Hacker, P, Engel, A & Mauer, M 'Regulating ChatGPT and other large generative AI models' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago Illinois, United Stated of America) 1112 – 1123.

Karan, A, Balepur, N & Sundaram, H 'Your browsing history may cost you: A framework for discovering differential pricing in non-transparent markets' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 717 – 735.

Metcalf, J, Singh, R, Moss, E, Tafesse, E & Watkins, EA 'Taking algorithms to courts: A relational approach to algorithmic accountability' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 1450 – 1462.

Mzila, P 'Protection of personal information in South Africa: A framework for biometric data collection security' In *Proceedings of INTERNET 2016: The Eighth International Conference on Evolving Internet* (13 – 17 November 2016, Barcelona, Spain) 1 – 6.

Pelteret, M & Ophoff, J 'Organizational information privacy strategy and the impact of the PoPI Act' In *2017 Information Security for South Africa (ISSA)* (16 - 17 August 2017, Johannesburg, South Africa) 56 – 65.

Swartz, P & Da Veiga, A 'PoPI Act - opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment' In *2016 Information Security for South Africa* (*ISSA*) (17 – 18 August 2016, Johannesburg, South Africa) 9 – 17.

Zilka, M, Fogliato, R, Hron, J, Butcher, B, Ashurst, C & Weller, A 'The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments' In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)* (12 – 15 June 2023, Chicago, Illinois, United States of America) 1553 – 1569.

DISSERTATIONS/THESES

Ausloos, J *The Right to Erasure: Safeguard for Informational Self-determination in a Digital Society?* (unpublished LLD thesis), University in Leuven, Belgium, September 2018.

https://kuleuven.limo.libis.be/discovery/search?query=any,contains,LIRIAS2123546&tab=LIRIAS&search_scope=lirias_profile&vid=32KUL_KUL:Lirias&offset=0 (Accessed: 2 February 2025).

Basson, AS *The Right to be Forgotten: A South African Perspective* (unpublished LLM thesis (partial-fulfilment), University of Pretoria, October 2015). *https://repository.up.ac.za/bitstream/handle/2263/53162/Basson_Right_2016.pdf?sequence =1&isAllowed=y* (Accessed: 4 March 2019).

Donnelly, DL *Privacy by (re)Design: A Comparative Study of the Protection of Personal Information in the Mobile Applications Ecosystem under United States, European Union and South African Law* (unpublished LLD thesis, University of KwaZulu-Natal, 2020). *https://researchspace.ukzn.ac.za/handle/10413/19431* (Accessed: 30 August 2022).

Naude, A *Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments* (unpublished LLM thesis (partial-fulfilment), University of Pretoria, December 2014). https://repository.up.ac.za/bitstream/handle/2263/46094/Naude_Data_2015.pdf?sequence=1&isAllowed=y (Accessed: 1 February 2022).

Wasser, M *You're Forgiven but not Forgotten: The Coherence of the Right "to be forgotten" in Germany and the EU* (unpublished bachelor thesis (partial-fulfilment), University of Twente, the Netherlands, 2 July 2020). *http://essay.utwente.nl/82360/* (Accessed: 20 August 2022).

OPINIONS

Bobek (Advocate General) Opinion in *Puppinck & others v European Commission* (Case C-418/18P) EU:C:2019:640, delivered on 29 July 2019.

Campos Sánchez-Bordona M (Advocate General) Opinion in *UI v Österreichische Post AG* (C-300/21) EU:C:2022:756, delivered on 6 October 2022.

Jääskinen, N (Advocate General) Opinion in *Google Spain SL, Google Inc. and Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) EU:C:2013:424, delivered on 25 June 2013.

Kokott, J (Advocate General) Opinion in *Opinion procedure 2/13 initiated following a request made by the European Commission* EU:C:2014:2475, delivered on 13 June 2014.

Rantos, A (Advocate General) Opinion in *Meta Platforms Ireland Inc., formerly Facebook Inc., & others v Bundeskartellamt* (Case C-252/21) EU:C:2022:704, delivered on 20

September 2022.

Szpunar, M (Advocate General) Opinion in *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (C-507/17) EU:C:2019:15, delivered 10 January 2019.

Szpunar, M (Advocate General) Opinion in *Planet 49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* EU:C:2019:246, delivered 21 March 2019.

ONLINE SOURCES

Article 19 'Digital Rights'. *https://www.article19.org/issue/digital-rights/* (Accessed: 15 April 2019).

BizPortal – Brought to you by the CIPC 'BizProfile: Google'. *https://bizportal.gov.za/bizprofile.aspx* (Accessed: 21 April 2022).

Constitutional Court of South Africa '*Herman Botha v Bool Smuts and another*'. *https://collections.concourt.org.za/handle/20.500.12144/38290* (Accessed: 23 October 2023).

Council of Europe 'Chart of signatures and ratifications of Treaty 108'. *https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108* (Accessed: 24 July 2023).

Der SPIEGEL. *https://www.spiegel.de/* (Accessed: 29 December 2022).

Freedom of Expression Institute 'What is Freedom of Expression'. *https://www.freedomforuminstitute.org/about/faq/what-is-freedom-of-expression/* (Accessed: 7 February 2019).

Genius Lyrics 'Rockwell – Somebody's Watching Me Lyrics'. *https://genius.com/Rockwell-somebodys-watching-me-lyrics* (Accessed: 15 December 2022).

'Hinweise für Autoren' in *Neue Juristische Wochenschrift*, no. 12/2019. *https://www.beck.de/rsw/upload/NJW/Autorenhinweise_2019.pdf* (Accessed: 21 April 2021).

Journal of International Law and Politics Guide to Foreign and International Legal Citations 2006 (New York University). *https://www.law.nyu.edu/sites/default/files/upload_documents/Final_GFILC_pdf.pdf* (Accessed: 17 November 2020).

Library of Congress 'Guide to Law Online: Germany'. *https://www.loc.gov/law/help/constitutional-court-cases/germany.php* (Accessed: 21 April 2021).

Norddeutscher Rundfunk – a broadcasting service in the Federal Republic of Germany, with a focus on the northern German states or Bundesländer. *https://www.ndr.de/* (Accessed: 23 August 2022).

'Privacy Commissioners'. *https://lop.parl.ca/sites/ParlInfo/default/en_CA/People/Officers Parliament/privacyCommissioner* (Accessed: 27 April 2024).

Safe City Msunduzi NPC. *http://safecity.co.za/* (Accessed: 17 December 2022).

'South Africa and the OECD'. *https://www.oecd.org/southafrica/south-africa-and-oecd.htm* (Accessed: 27 January 2024).

Verdi 'Der Betriebsrat: Was Beschäftigte und Betriebsräte wissen müssen', 23 September 2021. *https://www.verdi.de/themen/arbeit/der-betriebsrat* (Accessed: 28 September 2021).

REPORTS/PAPERS

Access Now *Human Rights in the Age of Artificial Intelligence* (November 2018).

Access Now *Human Rights Impact Assessments for AI: Analysis and Recommendations* (October 2022).

Article 19 *Policy Brief 2016: The "Right to be Forgotten": Remembering Freedom of Expression*, London, United Kingdom (2015).

Article 19 *Draft Background Paper: Friend or Foe? Protecting Freedom of Expression and Privacy in the Digital Age* (May 2016).

Article 29 Data Protection Working Party *Opinion 4/2007 on the concept of personal data*, adopted 20 June 2007.

Article 29 Data Protection Working Party *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, adopted on 16 February 2010.

Article 29 Data Protection Working Party *Opinion 8/2010 on Applicable Law*, adopted on 16 December 2010.

Article 29 Data Protection Working Party *Opinion 15/2011 on the definition of consent*, adopted 13 July 2011.

Article 29 Data Protection Working Party *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González" C-131/12*, adopted 26 November 2014.

Article 29 Data Protection Working Party *Update of Opinion 8/2010 on Applicable Law in Light of the CJEU Judgment in Google Spain*, adopted 16 December 2015.

Article 29 Data Protection Working Party *Guidelines on consent under Regulation 2016/679*, revised and adopted 10 April 2018.

European Data Protection Board *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* ver. 2.1 adopted 12 November 2019.

European Data Protection Board *Guidelines 05/2020 on Consent under Regulation 2016/679* adopted 4 May 2020.

European Data Protection Board *Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1)* adopted 7 July 2020.

European Data Protection Board *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* adopted 2 September 2020.

European Data Protection Board *Internal EDPB Document 02/2021 on SAs duties in relation to alleged GDPR infringements* adopted 2 February 2021.

Information Regulator (South Africa) 'Guidance Note on Application for Prior Authorisation' (March 2021). *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf* (Accessed: 8 February 2022).

Information Regulator (South Africa) 'Guidance Note on Exemptions from the Conditions for Lawful Processing of Personal Information in terms of Section 37 and 38 of the Protection of Personal Information Act 4 of 2013' (June 2021). *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPILawful Processing-202106.pdf* (Accessed: 8 February 2022).

OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Revised: 2013). *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf* (Accessed: 11 November 2021).

OECD *Recommendation of the Council on Artificial Intelligence* (2024). *https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#:~:text=The%20Recommendation%20aims%20to%20foster,Principles%2C%20drawn%20from%20the%20Recommendation* (Accessed: 4 July 2024).

Privacy International and Article 19 *Privacy and Freedom of Expression in the Age of Artificial Intelligence* (April 2018). *https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf* (Accessed: 21 January 2019).

The Press Code of Ethics and Conduct for South African Print and Online Media. https://presscouncil.org.za/ContentPage?code=PRESSCODE (Accessed: 3 February 2022).

South African Law Reform Commission *Privacy and Data Protection*. Pretoria: South African Law Reform Commission, (Discussion Paper 109, Project 124, October 2005).

South African Law Reform Commission. *Report on Privacy and Data Protection*. Pretoria: South African Law Reform Commission, (Project 124, 2009).

UNESCO *Recommendation on Artificial Intelligence*, (adopted 23 November 2021), Paris. *https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence* (Accessed: 14 July 2023).

UNHCR (Sub-commission) F La Rue 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet' (16 May 2011) UN Doc. A/HRC/17/27.

UNHCR (Sub-commission), F La Rue 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: The implications of States' surveillance of communications for the exercise of the human rights to privacy and to freedom of opinion and expression' (17 April 2013) UN Doc A/HRC/23/40.

UNHCR (Sub-commission), D Kaye 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: A framework for the moderation of user-generated online content that puts human rights at the very centre' (6 April 2018) UN Doc. A/HRC/38/35.

Van Alsenoy B, Kuczerawy, A & Ausloos, J 'Search engines after *Google Spain*: Internet@Liberty or Privacy@Peril?' (6 September 2013). ICRI Working Paper Series: ICRI Research Paper 15. DOI: *http://dx.doi.org/10.2139/ssrn.2321494*.

TABLE OF CASES

AUSTRALIA

Andrew Koh Nominees Pty Ltd v Pacific Corporation Ltd [No 2] [2009] WASC 207

Australian Competition and Consumer Commission v Allphones Retail Pty Limited (No 3) [2009] FCA 1075

British American Tobacco Australia Services Ltd v Cowell (No 2) (2003) 8 VR 571

Burrows v Houda [2020] NSWDC 485

Esso Australia Resources Ltd v Plowman [1995] 183 CLR 10

Fairfax Media Publications Pty Ltd v Voller; Nationwide News Pty Limited v Voller; Australian News Channel Pty Ltd v Voller [2021] HCA 27

Google Inc v Duffy [2017] SASCFC 130

Google LLC v Defteros [2022] HCA 27

X v Twitter Inc [2017] NSWSC 1300

X v Y & Z [2017] NSWSC 1214

CANADA

Attorney General (Nova Scotia) v MacIntyre [1982] 1 SCR 175

Autorité des marchés financiers v. PlexCorps 2017 QCTMF 88

Douez v Facebook Inc. 2017 SCC 33

Google Inc. v Equustek Solutions Inc. 2017 SCC 34, [2017] 1 S.C.R. 824

Google LLC v The Privacy Commissioner of Canada, The Attorney General of Canada & The Complainant 2023 FCA 200

Hogan v Hinch [2011] 243 CLR 506

Hunter et al. v. Southam Inc. 1984 CanLII 33 (SCC), [1984] 2 SCR 145

Juman v Doucette 2008 SCC 8

R v Keegstra; Attorney-General Canada & other intervening parties [1990] 3 S.C.R. 697, [1991] 3 CRR (2d) 193

R v McKinlay Transport Ltd. 1990 CanLII 137 (SCC), [1990] 1 SCR 627

Taylor and Western Guard Party v Canadian Human Rights Commission; Attorney General of Canada & other intervening parties [1991] 3 CRR (2d) 116

EUROPE AND THE EUROPEAN UNION

A v B & others (C-112/13) EU:C:2014:2195

Åklagaren v Åkerberg Fransson (C-617/10) EU:C:2013:105, [2013] EUECJ C-617/10

Antović and Mirković v Montenegro (European Court of Human Rights – Second Section) application no. 70838/13 (28 November 2017), [2017] ECHR 1068

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado (C-468/10 & C-469/10) EU:C:2011:777, [2011] EUECJ C-468/10, [2011] EUECJ C-469/10

Avotiņš v Latvia (European Court of Human Rights – Grand Chamber) application no. 17502/07 (23 May 2016), [2016] ECHR 440

Axel Springer AG v Germany (European Court of Human Rights – Grand Chamber) application no. 9954/08 (7 February 2012), [2012] ECHR 227

Axel Springer SE and RTL Television GmbH v Germany (European Court of Human Rights – Fifth Section) application no. 51405/12 (21 September 2017), [2017] ECHR 793

B v Latvijas Republikas Saeima (C-439/19) EU:C:2021:504, [2021] EUECJ C-439/19

Bara & others v Președintele Casei Naționale de Asigurări de Sănătate & others (C-201/14) EU:C:2015:638, [2015] EUECJ C-201/14

BE v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-132/21) EU:C:2023:2, [2023] EUECJ C-132/21

Bernard Connolly v European Commission (C-274/99) EU:C:2001:127, [2001] EUECJ C-274/99

Biancardi v Italy (European Court of Human Rights – First Section) application no. 77419/16 (25 November 2021), [2021] ECHR 972

Big Brother Watch & others v The United Kingdom (European Court of Human Rights – Grand Chamber) application nos. 58170/13, 62322/14 and 24960/15 (25 May 2021), [2021] ECHR 439

Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v Ireland (European Court of Human Rights – Grand Chamber) application no 45036/98 (30 June 2005), [2005] ECHR 440

Breyer v Bundesrepublik Deutschland (C-582/14) EU:C:2016:779, [2016] EUECJ C-582/14

Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-46/23) EU:C:2024:239, [2024] EUECJ C-46/23

Bundesrepublik Deutschland v SpaceNet AG & Telekom Deutschland GmbH (C-793/19 & C-794/19) EU:C:2022:702, [2022] EUECJ C-793/19

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale

Bundesverband e.V. v Planet49 GmbH (C-673/17) EU:C:2019:801, [2019] EUECJ C-673/17

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni (C-398/15) EU:C:2017:197, [2017] EUECJ C-398/15

ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA) (C-615/13 P) EU:C:2015:489

CN v European Parliament (T-343/13) EU:T:2015:926

College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer (C-553/07) EU:C:2009:293, [2009] EUECJ C-553/07

Data Protection Commission v Facebook Ireland & Schrems (C-311/18) EU:C:2020:559, [2020] EUECJ C-311/18 (*Schrems II*)

Delfi AS v Estonia (European Court of Human Rights – Grand Chamber) application no. 64569/09 (16 June 2015), [2015] ECHR 586

Denisov v Ukraine (European Court of Human Rights – Grand Chamber) application no. 76639/11 (25 September 2018), [2018] ECHR 1061

Deutsche Post AG v Hauptzollamt Köln (C-496/17) EU:C:2019:26, [2019] EUECJ C-496/17

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & others, and Kärntner Landesregierung & others (C-293/12 & C-594/12) EU:C:2014:238, [2014] EUECJ C-293/12

eDate Advertising GmbH v X, Martinez & another v MGN Limited (C-509/09 and C-161/10) EU:C:2011:685, [2011] EUECJ C-509/09, [2011] EUECJ C-161/10

Editorial Board of PravoyeDelo and Shtekel v Ukraine (European Court of Human Rights – Fifth Section) application no. 33014/05 (5 May 2011), [2011] ECHR 748

Falzon v Malta (European Court of Human Rights – Fourth Section) application no. 45791/13 (20 March 2018)

Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V. (C-40/17) EU:C:2019:629

Fayed v The United Kingdom Series A No 294B, Application No 17101/90, (1994) 18 EHRR 393

FF v Österreichische Datenschutzbehörde (CRIF GmbH, intervening party) (C-487/21) EU:C:2023:369, [2023] EUECJ C-487/21

Flinkkila & others v Finland (European Court of Human Rights – Fourth Section) application no. 25576/04 (6 April 2010), [2010] ECHR 446

Florindo de Almeida Vasconcelos Gramaxo v Portugal (European Court of Human Rights – Fourth Section) application no. 26968/16 (13 December 2022) – legal summary dated

December 2022

FT v DW (C-307/22) EU:C:2023:811, [2023] EUECJ C-307/22

Fuchsmann v Germany (European Court of Human Rights – Fifth Section) application no 71233/13 (19 October 2017), [2017] ECHR 925

Fürst-Pfeifer v Austria (European Court of Human Rights – Fourth Section) application nos. 33677/10 and 52340/10 (17 May 2016), [2016] ECHR 431

GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL) (Premier minister and Google LLC, intervening parties) (C-136/17) EU:C:2019:773, [2019] EUECJ C-136/17

GD v Commissioner of An Garda Síochána & others (C-140/20) EU:C:2022:258, [2022] EUECJ C-140/20

G.I.E.M. S.R.L. & others v Italy (European Court of Human Rights – Grand Chamber) application nos. 1828/06, 34163/07 and 19029/11 (28 June 2018), [2018] ECHR 564

Google France SARL & Google Inc. v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA & Luteciel SARL; Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin & Tiger SARL (C-236/08, C-237/08 & C-238/08) EU:C:2010:159, [2010] EUECJ C-236/08

Google LLC v Commission nationale de l'informatique et des libertés (CNIL) (C-507/17) EU:C:2019:772, [2019] EUECJ C-507/17

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12) EU:C:2014:317, [2014] EUECJ C-131/12

Harman v UK (1985) 7 EHRR 146 (EComm)

Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums (C-34/21) EU:C:2023:270, [2023] EUECJ C-34/21

Huber v Bundesrepublik Deutschland (C-524/06) EU:C:2008:724, [2008] EUECJ C-524/06

Hurbain v Belgium (European Court of Human Rights – Third Section) application no 57292/16 (22 June 2021)

Hurbain v Belgium (European Court of Human Rights – Grand Chamber) application no 57292/16 (4 July 2023), [2023] ECHR 948

HYA & others (Spetsializirana prokuratura a further party to the proceedings) (C-349/21) EU:C:2023:102, [2023] EUECJ C-349/21

Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert & others (C-473/12) EU:C:2013:715, [2013] EUECJ C-473/12

IVT v Romania (European Court of Human Rights – Fourth Section) application no. 35582/15

(1 March 2022), [2022] ECHR 189

Jankauskas v Lithuania (No. 2) (European Court of Human Rights – Fourth Section) application no. 50446/09 (17 June 2017), [2017] ECHR 593

Jeunesse v The Netherlands (European Court of Human Rights – Grand Chamber) application no. 12738/10 (3 October 2014), [2014] ECHR 1036

JM (Apulaistietosuojavaltuutettu and Pankki S, intervening parties) (C-579/21) EU:C:2023:501, [2023] EUECJ C-579/21

Köpke v Germany (European Court of Human Rights – Fifth Section) application no. 420/07 (5 October 2010), [2010] ECHR 1725

L'Oréal SA and others v eBay International AG and others (C-324/09) EU:C:2011:474

La Quadrature du Net & others v Premier minister & others; *Ordre des barreaux francophones et germanophone & others v Conseil des ministers* (C-511/18, C-512/18 & C-520/18) EU:C:2020:791

Land Nordrhein-Westfalen v Renckhoff (C-161/17) EU:C:2018:634

LB v Hungary (European Court of Human Rights – Fourth Section) application no. 36345/16 (12 January 2021), [2021] ECHR 2

LB v Hungary (European Court of Human Rights – Grand Chamber) application no. 36345/16 (9 March 2023), [2023] ECHR 239

Liberty & others v United Kingdom (European Court of Human Rights – Fourth Section) application no. 58243/0 (1 July 2008), [2008] ECHR 568

Ligue des droits humains v Conseil des ministres (C-817/19) EU:C:2022:491

Lindqvist (C-101/01) EU:C:2003:596, [2003] EUECJ C-101/01

López Ribalda & others v Spain (European Court of Human Rights – Grand Chamber) application nos. 1874/13 and 8567/13 (17 October 2019), [2019] ECHR 752

Mediengruppe Österreich GmbH v Austria (European Court of Human Rights – Fourth Section) application no. 37713/18 (26 April 2022), [2022] ECHR 316

McFadden v Sony Music Entertainment Germany GmbH (C-484/14) EU:C:2016:689

Melloni v Ministerio Fiscal (C-399/11) EU:C:2013:107:60, [2012] EUECJ C-399/11

Menci v Procura della Repubblica (C-524/15) EU:C:2018:197, [2018] EUECJ C-524/15

Meta Platforms Inc. & others v Bundeskartellamt (Verbraucherzentrale Bundesverband eV, intervening party) (C-252/21) EU:C:2023:537, [2023] EUECJ C-252/21

Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – VerbraucherzentraleBundesverband e.V. (C-319/20) EU:C:2022:322, [2022] EUECJ C-319/20

Meta Platforms Ireland Ltd v European Commission (Federal Republic of Germany, intervening party) (T-451/20) EU:T:2023:276, [2023] EUECJ T-451/20

Meta Platforms Ireland Ltd v European Commission (Federal Republic of Germany, intervening party) (T-452/20) EU:T:2023:277, [2023] EUECJ T-452/

ML v Slovakia (European Court of Human Rights – First Section) application no. 34159/17 (14 October 2021), [2021] ECHR 821

ML & WW v Germany (European Court of Human Rights – Fifth Section) application nos. 60798/10 & 65599/10 (28 June 2018)

Mosley v The United Kingdom (European Court of Human Rights – Fourth Section) application no. 48009/08 (10 May 2011), [2011] ECHR 774

Nowak v Data Protection Commissioner (C- 434/16) EU:C:2017:994, [2017] EUECJ C-434/16

Opinion 2/13 of the Court of Justice of the European Union EU:C:2014:2454

Österreichischer Rundfunk v Austria (European Court of Human Rights – First Section) application no. 35841/02 (7 December 2006), [2006] ECHR 1043

OT v Vyriausioji tarnybinės etikos komisija (C-184/20) EU:C:2022:601, [2022] EUECJ C-184/20

Perincek v Switzerland (European Court of Human Rights – Grand Chamber) application no. 27510/08 (25 October 2015), [2015] ECHR 907

Pihl v Sweden (European Court of Human Rights – First Section) application no. 74742/14 (7 February 2017)

Promusicae v Telefónica de España SAU (C-275/06) EU:C:2008:54, [2008] EUECJ C-275/06

Proximus NV v Gegevensbeschermingsautoriteit (C-129/21) EU:C:2022:833

Puppinck & others v European Commission (C-418/18P) EU:C:2019:1113

Puškár v Finančné riaditeľstvo Slovenskej republiky & another (C-73/16) EU:C:2017:725, [2017] EUECJ C-73/16,

Rechnungshof v Österreichischer Rundfunk & others and Christa Neukomm & Joseph Lauermann v Österreichischer Rundfunk (C-465/00, C-138/01 & C-139/01) EU:C:2003:294

RW v Österreichische Post AG (C-154/21) EU:C:2023:3, [2023] EUECJ C-154/21

Ryneš v Úřad pro ochranu osobních údajů (C-212/13) EU:C:2014:2428, [2014] EUECJ C-212/13

Saaristo & others v Finland (European Court of Human Rights – Fourth Section) application no. 184/06 (12 October 2010), [2010] ECHR 1497

Samoylova v Russia (European Court of Human Rights – Third Section) application no.

49108/11 (14 December 2021), [2021] ECHR 1067

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland (European Court of Human Rights – Grand Section) application no. 931/13 (27 June 2017), [2017] ECHR 607

Schrems v Data Protection Commissioner (C-362/14) EU:C:2015:650, EUECJ C-362/14 (*Schrems I*)

Schwarz v Stadt Bochum (C-291/12) EU:C:2013:670, [2013] EUECJ C-291/12

Single Resolution Board (SRB) v European Data Protection Supervisor (EDPS) (T-557/20) EU:T:2023:219, [2023] EUECJ T-557/20

Spiegel Online GmbH v Volcker Beck (C-516/17) EU:C:2019:625, [2019] EUECJ C-516/17

'SS' SIA v Valsts ieņēmumu dienests (C-175/20) EU:C:2022:124

Standard Verlagsgesellschaft mbH v Austria (No. 3) (European Court of Human Rights – Fourth Section) application no. 39378/15 (7 December 2021), [2021] ECHR 1029

Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson & others (C-203/15 & C-698/15) EU:C:2016:970, [2016] EUECJ C-203/15

Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH (C-314/12) EU:C:2014:192, [2014] EUECJ C-314/12

Tietosuojavaltuutettu (Jehovan todistajat — uskonnollinen yhdyskunta as intervening party) (C-25/17) EU:C:2018:551, [2018] EUECJ C-25/17

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (C-73/07) EU:C:2008:727

Times Newspapers Ltd v The United Kingdom (Nos. 1 & 2) (European Court of Human Rights Fourth Section) application nos. 3002/03 and 23676/03 (10 March 2009), [2009] ECHR 451

TU, RE v Google Spain LLC (C-460/20) EU:C:2022:962, [2022] EUECJ C-460/20

UI v Österreichische Post AG (C-300/21) EU:C:2023:370, [2023] EUECJ C-300/21

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16) EU:C:2018:388, [2018] EUECJ C-210/16

UZ v Bundesrepublik Deutschland (C-60/22) EU:C:2023:373, [2023] EUECJ C-60/22

Uzun v Germany (European Court of Human Rights – Fifth Section) application no. 35623/05 (02 September 2010), [2010] ECHR 2263

VD & SR (C-339/20 & C-397/20) EU:C:2022:703, [2022] EUECJ C-339/20

Veen v Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) (T-436/21) EU:T:2022:261

Volker und Markus Schecke GbR & Eifert v Land Hessen (Bundesanstalt für Landwirtschaft

und Ernährung, joined party) (C-92/09 & C-93/09) EU:C:2010:662, [2010] EUECJ C-92/09, [2010] EUECJ C-93/09

Von Hannover v Germany (no. 2) (European Court of Human Rights – Grand Chamber) application nos. 40660/08 and 60641/08 (7 February 2012), [2012] ECHR 228

VS (Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost, third party) (C-205/21) EU:C:2023:49, [2023] EUECJ C-205/21

VS v Inspektor v Inspektorata kam Visshia sadeben savet (C-180/21) EU:C:2022:967, [2022] EUECJ C-180/21

Węgrzynowski and Smolczewski v Poland (European Court of Human Rights – Fourth Section) application no. 33846/07 (16 July 2013), [2013] ECHR 690

WM & Sovim SA v Luxembourg Business Registers (C-37/20 & C-601/20) EU:C:2022:912

Worten — Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho (ACT) (C-342/12) EU:C:2013:355, [2013] EUECJ C-342/12

X, Z v Autoriteit Persoonsgegevens (C-245/20) EU:C:2022:216, [2022] EUECJ C-245/20

X-FAB Dresden GmbH & Co. KG v FC (C-543/21) EU:C:2023:79, [2023] EUECJ C-453/21

YS v Minister voor Immigratie, Integratie en Asiel & Minister voor Immigratie, Integratie en Asiel v M & S (C-141/12 & C-372/12) EU:C:2014:2081, [2014] EUECJ C-141/12

ZS v Zweckverband "Kommunale Informationsverarbeitung Sachsen" KISA, Körperschaft des öffentlichen Rechts (C-560/21) EU:C:2023:81

GERMANY

34 *BVerfGE* 238 – *Tonband*

BGH, Urteil vom 23. Juni 2020 – KVR 69/19, DE:BGH:2020:230620BKVR69.19.0 – *Bundeskartellamt v Facebook*

BGH, Urteil vom 22. September 2020 – VI ZR 476/19, DE:BGH:2020:220920UVIZR476.19.0

BGH, Urteil vom 26. Januar 2021 – VI ZR 437/19, DE:BGH:2021:260121UVIZR437.19.0

BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 16/13, DE:BVerfG:2019:rs20191106.1bvr001613 – *Recht auf Vergessen I*

BVerfG, Beschluss des Ersten Senats vom 6. November 2019 – 1 BvR 276/17, DE:BVerfG:2019:rs20191106.1bvr027617 – *Recht auf Vergessen II*

BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, DE:BVerfG:1983:rs19831215.1bvr020983 – *Volkszählungsurteil*

BVerfG, Urteil des Zweiten Senats vom 5. Mai 2020 – 2 BvR 859/15, 2 BvR 980/16, 2 BvR

2006/15, 2 BvR 1651/15, DE:BVerfG:2020:rs20200505.2bvr085915

OLG Stuttgart, Urt. vom 8. Oktober 2015 - 2 U 25/15

THE NETHERLANDS

Google Netherlands B.V, Google Inc. (Hoge Raad) unreported case no 15/03380 (24 February 2017), NL:HR:2017:316

NORTHERN IRELAND

CG v Facebook Ireland Ltd & another [2016] NICA 54

SOUTH AFRICA

Afriforum v Economic Freedom Fighters & others [2022] ZAEQC 2, 2022 (6) SA 357 (GJ)

Afriforum NPC v Nelson Mandela Foundation Trust and others [2023] ZASCA 58, 2023 (4) SA 1 (SCA), [2023] 3 All SA 1 (SCA)

Amabhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others [2019] ZAGPPHC 384, 2020 (1) SA 90 (GP), [2019] 4 All SA 343 (GP)

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice [2021] ZACC 3, 2021 (3) SA 246 (CC), 2021 (4) BCLR 349 (CC)

Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others [2021] ZAGPPHC 779, 2022 (2) SA 485 (GP)

Arena Holdings (Pty) Ltd t/a Financial Mail & others v South African Revenue Services & others [2023] ZACC 13, 2023 (5) SA 319 (CC), 2023 (8) BCLR 905 (CC)

Bato Star Fishing (Pty) Ltd v Minister of Environmental Affairs & others [2004] ZACC 15, 2004 (4) SA 490 (CC), 2004 (7) BCLR 687 (CC)

Bernstein & others v Bester NNO & others [1996] ZACC 2, 1996 (2) SA 751 (CC), 1996 (4) BCLR 449 (CC)

Blind SA v Minister of Trade, Industry and Competition & others [2022] ZACC 33, 2023 (2) BCLR 117 (CC)

Bobroff & another v National Director of Public Prosecutions [2021] ZASCA 56; 2021 (2) SACR 53 (SCA); [2021] 3 All SA 1 (SCA)

Bosasa Operations (Pty) Ltd v Basson & another [2012] ZAGPJHC 71, 2013 (2) SA 570 (GSJ)

Botha v Smuts and another [2024] ZACC 22, 2025 (1) SA 581 (CC), 2024 (12) BCLR 1477 (CC)

British American Tobacco South Africa (Pty) Ltd v Minister of Health (National Council against Smoking as amicus curiae) [2012] ZASCA 107, [2012] 3 All SA 593 (SCA)

Carmichele v Minister of Safety and Security & another [2001] ZACC 22, 2001 (4) SA 938 (CC), 2001 (10) BCLR 995 (CC)

Case v Minister of Safety and Security; Curtis v Minister of Safety and Security [1996] ZACC 7, 1996 (3) SA 617 (CC), 1996 (5) BCLR 608 (CC).

Caxton and CTP Publishers and Printers Ltd v Novus Holdings Ltd [2022] ZASCA 24, [2022] 2 All SA 299 (SCA)

Centre for Child Law v Director of Public Prosecutions, Johannesburg & others [2022] ZACC 35, 2022 (2) SACR 629 (CC), 2022 (12) BCLR 1440 (CC)

Centre for Child Law & others v Media 24 Ltd [2019] ZACC 46, 2020 (4) SA 319 (CC), 2020 (3) BCLR 245 (CC)

Certification of the Constitution of the Republic of South Africa, 1996 [1996] ZACC 26, 1996 (4) SA 744 (CC), 1996 (10) BCLR 1253 (CC)

Chinese Association v Henning & others (Gauteng Division of the High Court sitting as the Equality Court) unreported case no EQ2/2017 (28 July 2022), [2022] ZAGPJHC 590

Chinese Association, Gauteng v SABC 2 (Broadcasting Complaints Commission) unreported case no 02/2020 (6 March 2020)

City of Cape Town v South African National Roads Authority Limited & others [2015] ZASCA 58, 2015 (3) SA 386 (SCA), [2015] 2 All SA 517 (SCA)

Cochrane Steel Products (Pty) Ltd v M-Systems Group (Pty) Ltd & another [2016] ZASCA 74, 2016 (6) SA 1 (SCA), [2016] 3 All SA 345 (SCA)

Commissioner, South African Police Service & others v Maimela & another 2003 (5) SA 480 (T)

Competition Commission v Bank of America Merrill Lynch International Ltd & others [2020] ZACAC 1; 2020 (4) SA 105 (CAC)

Crown Cork & Seal Co Inc & another v Rheem South Africa (Pty) Ltd & others 1980 (3) SA 1093 (W)

De Lange v Methodist Church & another [2015] ZACC 35, 2016 (2) SA 1 (CC), 2016 (1) BCLR 1 (CC)

De Lille v Speaker of the National Assembly 1998 (3) SA 430 (C), 1998 (7) BCLR 916 (C)

Democratic Alliance v African National Congress & another [2015] ZACC 1, 2015 (2) SA 232 (CC), 2015 (3) BCLR 298 (CC)

De Reuck v Director of Public Prosecutions, Witwatersrand Local Division & others [2003] ZACC 19, 2004 (1) SA 406 (CC), 2003 (12) BCLR 1333 (CC)

Dikoko v Mokhatla [2006] ZACC 10, 2006 (6) SA 235 (CC), 2007 (1) BCLR 1 (CC)

Director of Public Prosecutions, Eastern Cape, Makhanda v Coko [2024] ZASCA 59

Director of Public Prosecutions, Kwazulu-Natal Pietermaritzburg v Ndlovu [2024] ZASCA 23; [2024] 2 All SA 315 (SCA)

Director of Public Prosecutions, Western Cape v Kouwenhoven [2020] ZAWCHC 185; 2021 (1) SACR 579 (WCC); [2021] 1 All SA 843 (WCC)

Discovery Ltd & others v Liberty Group Ltd [2020] ZAGPJHC 67, 2020 (4) SA 160 (GJ), [2020] 2 All SA 819 (GJ)

Divine Inspiration Trading 205 (Pty) Ltd & another v Gordon & others [2021] ZAWCHC 38, 2021 (4) SA 206 (WCC)

Du Toit v The Magistrate & others [2016] ZASCA 15, 2016 (2) SACR 112 (SCA), [2016] 2 All SA 328 (SCA)

Economic Freedom Fighters & another v Minister of Justice and Constitutional Development & another; Economic Freedom Fighters & another v Minister of Justice and Constitutional Development & another [2019] ZAGPPHC 253, 2019 (2) SACR 297 (GP), [2019] 3 All SA 723 (GP)

Economic Freedom Fighters & another v Minister of Justice and Correctional Services & another [2020] ZACC 25, 2021 (2) SA 1 (CC), 2021 (2) BCLR 118 (CC)

Economic Freedom Fighters & others v Manuel [2020] ZASCA 172, 2021 (3) SA 425 (SCA), [2021] 1 All SA 623 (SCA)

Financial Mail (Pty) Ltd & others v Sage Holdings Ltd & another [1993] ZASCA 3, 1993 (2) SA 451 (A), [1993] 2 All SA 109 (A)

Gaertner & others v Minister of Finance & others [2013] ZACC 38, 2014 (1) SA 442 (CC), 2014 (1) BCLR 38 (CC)

Gavric v Refugee Status Determination Officer & others [2018] ZACC 38, 2019 (1) SA 21 (CC), 2019 (1) BCLR 1 (CC)

Gigaba v Minister of Police & others [2021] ZAGPPHC 55, [2021] 3 All SA 495 (GP)

Goosen-Joubert v Women4Women NPC [2022] ZAWCHC 82

Growthpoint Properties Ltd v South Africa Commercial Catering and Allied Workers Union (SACCAWU) & others [2010] ZAKZDHC 38, [2011] 1 All SA 537 (KZD)

Heroldt v Wills [2013] ZAGPJHC 1, 2013 (2) SA 530 (GSJ), [2013] 2 All SA 218 (GSJ)

Holomisa v Argus Newspapers Ltd 1996 (2) SA 588 (W), [1996] 1 All SA 478 (W)

Hotz & others v University of Cape Town [2016] ZASCA 159, 2017 (2) SA 485 (SCA), [2016] 4 All SA 723 (SCA)

Ibex RSA Holdco Ltd & another v Tiso Blackstar Group (Pty) Ltd & others [2024] ZASCA 166

Independent Newspapers Holdings Ltd & others v Suliman [2004] ZASCA 57, [2004] 3 All SA 137 (SCA)

Indigenous Film Distribution (Pty) Ltd & another v Film and Publication Appeal Tribunal & others [2018] ZAGPPHC 438, [2018] 3 All SA 783 (GP)

Investigating Directorate: Serious Economic Offences & others v Hyundai Motor Distributors (Pty) Ltd & others: In re Hyundai Motor Distributors (Pty) Ltd & others v Smit NO & others [2000] ZACC 12, 2001 (1) SA 545 (CC), 2000 (10) BCLR 1079

Islamic Unity Convention v Independent Broadcasting Authority & others [2002] ZACC 3, 2002 (4) SA 294 (CC), 2002 (5) BCLR 433 (CC)

Isparta v Richter & another [2013] ZAGPPHC 243, 2013 (6) SA 529 (GNP)

Jansen van Vuuren & another NNO v Kruger 1993 (4) SA 842 (A)

Johncom Media Investments Limited v M & others (Media Monitoring Group as Amicus Curiae) [2009] ZACC 5, 2009 (4) SA 7 (CC), 2009 (8) BCLR 751 (CC)

Kemp & another v Republican Press (Pty) Ltd 1994 (4) SA 261 (E)

Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association [2014] 1 All SA 566 (GSJ), 2014 (2) SA 569 (GSJ)

Khumalo & others v Holomisa [2002] ZACC 12, 2002 (5) SA 401 (CC), 2002 (8) BCLR 771 (CC)

Koyabe v Minister for Home Affairs (Lawyers for Human Rights as amicus curiae) [2009] ZACC 23, 2010 (4) SA 327 (CC), 2009 (12) BCLR 1192 (CC)

Laugh It Off Promotions CC v SAB International (Finance) BV t/a Sabmark International [2005] ZACC 7, 2006 (1) SA 144 (CC), 2005 (8) BCLR 743 (CC)

M & another v M & another [2022] ZAGPJHC 1025

Magajane v Chairperson, North West Gambling Board & others [2006] ZACC 8, 2006 (5) SA 250 (CC), 2006 (10) BCLR 1133 (CC)

Mail & Guardian Media Ltd & others v Chipu NO [2013] ZACC 32, 2013 (6) SA 367 (CC)

Masuku & another v South African Human Rights Commission obo South African Jewish Board of Deputies [2018] ZASCA 180, 2019 (2) SA 194 (SCA)

Mathias International Ltd & another v Baillache & others [2010] ZAWCHC 68, 2015 (2) SA 357 (WCC)

Midi Television (Pty) Limited t/a E-TV v Director of Public Prosecutions (Western Cape) [2007] ZASCA 56, 2007 (5) SA 540 (SCA)

Minister of Health & another NO v New Clicks South Africa (Pty) Ltd & others (Treatment Action Campaign & another as amici curiae) [2005] ZACC 14, 2006 (2) SA 311 (CC), 2006 (1) BCLR 1 (CC)

Minister of Justice and Constitutional Development & others v Prince; National Director of Public Prosecutions & others v Rubin; National Director of Public Prosecutions & others v Acton & others [2018] ZACC 30, 2018 (6) SA 393 (CC) (*Prince III*)

Mistry v Interim Medical and Dental Council of South Africa & others [1998] ZACC 10, 1998 (4) SA 1127 (CC), 1998 (7) BCLR 880 (CC)

Modiri v Minister of Safety and Security & others [2011] ZASCA 153, 2011 (6) SA 370 (SCA), [2012] 1 All SA 154 (SCA)

Mthembi-Mahanyele v Mail & Guardian Ltd & another [2004] ZASCA 67, [2004] 3 All SA 511 (SCA)

Munetsi v Madhuyu & another [2024] ZAWCHC 209

My Vote Counts NPC v Speaker of the National Assembly & others [2015] ZACC 31; 2016 (1) SA 132 (CC); 2015 (12) BCLR 1407 (CC)

Natal Joint Municipal Pension Fund v Endumeni Municipality [2012] ZASCA 13, 2012 (4) SA 593 (SCA), [2012] 2 All SA 262 (SCA)

National Coalition for Gay and Lesbian Equality & another v Minister of Justice & others [1998] ZACC 15, 1998 (12) BCLR 1517 (CC)

National Media Ltd & others v Bogoshi [1998] ZASCA 94, 1998 (4) SA 1196 (SCA), [1998] 4 All SA 347 (A)

Nelson Mandela Foundation Trust & another v Afriforum NPC & others [2019] ZAEQC 2, [2019] 4 All SA 237 (EqC)

Netshipise v Munnick & others [2018] ZAGPJHC 547

Nimble Investments (Pty) Ltd v Malan & others [2021] ZASCA 129, 2022 (4) SA 554 (SCA), [2021] 4 All SA 672 (SCA)

NM & others v Smith & others (Freedom of Expression Institute as amicus curiae) [2007] ZACC 6; 2007 (5) SA 250 (CC), 2007 (7) BCLR 751 (CC)

NUMSA obo Nhlabathi & 1 other v PFG Building Glass (Pty) Ltd [2022] ZALCJHB 292

Parker v Forsyth NO and others (Regional Court, Johannesburg, Gauteng) unreported case no 1585/20 (29 June 2023)

Premier of the Western Cape Province v Public Protector & another [2022] ZASCA 16, 2022

(3) SA 121 (SCA), [2022] 2 All SA 95 (SCA)

President of the Republic of South Africa & others v South African Rugby Football Union & others [1999] ZACC 11, 1999 (10) BCLR 1059 (CC)

Primedia Broadcasting (a division of Primedia (Pty) Ltd) & others v Speaker of the National Assembly & others [2016] ZASCA 142, 2017 (1) SA 572 (SCA), [2016] 4 All SA 793 (SCA)

Prince v President, Cape Law Society, & others [2002] ZACC 1, 2002 (2) SA 794 (CC) (*Prince II*)

Print Media South Africa & another v Minister of Home Affairs & another [2012] ZACC 22, 2012 (6) SA 443 (CC)

Publications Control Board v William Heinemann Ltd & others 1965 (4) SA 137 (A)

Qwelane v South African Human Rights Commission & another [2021] ZACC 22, 2021 (6) SA 579 (CC), 2021 (4) BCLR 349 (CC)

Replication Technology Group & others v Gallo Africa Ltd [2009] ZAGPJHC 8, 2009 (5) SA 531 (GSJ)

Residents of: Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others [2020] ZAGPJHC 146, 2021 (2) SA 220 (GJ), [2020] 3 All SA 902 (GJ)

Residents of Industry House, 5 Davies Street, New Doornfontein, Johannesburg & others v Minister of Police & others [2021] ZACC 37, 2022 (1) BCLR 46 (CC)

Rustenburg Platinum Mine v SAEWA obo Bester & others [2018] ZACC 13, 2018 (5) SA 78 (CC), 2018 (8) BCLR 951 (CC)

S v Chapman [1997] ZASCA 45, 1997 (2) SACR 3 (SCA)

S v Dube 2000 (2) SA 583 (N)

S v Jordan & others (Sex Workers Education and Advocacy Task Force & others as amici curiae) [2002] ZACC 22, 2002 (6) SA 642 (CC), 2002 (11) BCLR 1117 (CC)

S v Mamabolo (E-TV, Business Day & the Freedom of Expression Institute intervening) [2001] ZACC 17, 2001 (3) SA 409 (CC), 2001 (5) BCLR 449 (CC)

S v Manamela & another (Director-General of Justice intervening) [2000] ZACC 5, 2000 (3) SA 1 (CC), 2000 (5) BCLR 491 (CC)

S v Miller & others [2015] ZAWCHC 118, 2016 (1) SACR 251 (WCC), [2015] All SA 503 (WCC)

S v Motloutsi 1996 (1) SA 584 (C)

S v Naudé 1975 (1) SA 681 (A)

S v Okah [2018] ZACC 3; 2018 (1) SACR 492 (CC); 2018 (4) BCLR 456 (CC)

S v Tshabalala; S v Ntuli [2019] ZACC 48, 2020 (5) SA 1 (CC), 2020 (3) BCLR 307 (CC)

S v Zinn 1969 (2) SA 537 (A)

Shange & others v The State [2016] ZAKZPHC 115, [2017] 3 All SA 289 (KZP)

Sheburi v Railway Safety Regulator (Commission for Conciliation, Mediation and Arbitration) unreported ruling, case no GATW 15200-21 (2 March 2022)

Smuts & another v Botha [2022] ZASCA 3, 2022 (2) SA 425 (SCA)

Smuts NO & others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & others [2022] ZAECMKHC 42

Solidarity & another v Black First Land First & others [2022] ZAEQC 1, [2022] 2 All SA 549 (GJ)

South African Airways SOC v BDFM Publishers (Pty) Ltd & others [2015] ZAGPJHC 293, 2016 (2) SA 561 (GJ), [2016] 1 All SA 860 (GJ)

South African Broadcasting Corporation v Avusa Limited & another (Freedom of Expression Institute as amicus curiae) [2009] ZAGPJHC 80, 2010 (1) SA 280 (GSJ)

South African Broadcasting Corporation Limited v National Director of Public Prosecutions [2006] ZACC 15, 2007 (1) SA 523 (CC), 2007 (2) BCLR 167 (CC)

South African History Archive Trust v South African Reserve Bank and another [2020] ZASCA 56, 2020 (6) SA 127 (SCA), [2020] 3 All SA 380 (SCA)

South African Human Rights Commission v Masuku & another [2017] ZAEQC 1, 2018 (3) SA 291 (GJ)

South African Human Rights Commission obo South African Jewish Board of Deputies v Masuku & another [2022] ZACC 5, 2022 (4) SA 1 (CC), 2022 (7) BCLR 850 (CC)

South African National Defence Union v Minister of Defence & another [1999] ZACC 7, 1999 (4) SA 469 (CC), 1999 (6) BCLR 615 (CC)

South African Legal Practice Council v Chalom [2020] ZAGPPHC 663

Speaker of the National Assembly v De Lille & another [1999] ZASCA 50, 1999 (4) SA 863 (SCA)

Tap Wine Trading CC & another v Cape Classic Wines (Western Cape) CC & another 1999 (4) SA 194 (C)

The Citizen 1978 (Pty) Ltd & others v McBride [2011] ZACC 11, 2011 (4) SA 191 (CC), 2011 (8) BCLR 816 (CC)

Trust Sentrum (Kaapstad) (Edms) Bpk & another v Zevenberg & another 1989 (1) SA 145 (C)

Tshabalala-Msimang & another v Makhanya & others [2007] ZAGPHC 161, 2008 (6) SA 102 (W), 2008 (3) BCLR 338 (W)

Unitas Hospital v Van Wyk & another [2006] ZASCA 34, 2006 (4) SA 436 (SCA), [2006] 4 All SA 231 (SCA)

University of KwaZulu-Natal v Independent Newspapers (Pty) Ltd & others [2018] JOL 40414 (KZD)

Van Breda v Media 24 Ltd & others [2017] ZASCA 97, 2017 (5) SA 533 (SCA)

Van Wyk v Pretorius [2019] ZAGPPHC 474

Waldis & another v Von Ulmenstein [2016] ZAWCHC 201, 2017 (4) SA 503 (WCC)

Welch v Commissioner for the South African Revenue Service [2004] ZASCA 40, 2005 (4) SA 173 (SCA), [2004] 2 All SA 586 (SCA)

Yuppichef Holdings (Pty) Ltd v Yuppie Gadgets Holdings (Pty) Ltd [2016] ZASCA 118

UNITED KINGDOM

Alterskye v Scott [1948] 1 All ER 469

Attorney General for Gibraltar v May and others [1999] 1 WLR 998

British Steel Corporation v Granada Television Ltd [1981] 1 All ER 417

Ex parte Simms [1999] 3 All ER 400, [2000] 2 AC 115

Guardian News & Media Ltd & others Re: HM Treasury v Ahmed & others [2010] UKSC 1

Hearne v Street [2008] HCA 36

Home Office v Harman [1982] 1 All ER 532 (HL)

Interflora Inc & another v Marks and Spencer Plc (Rev 1) [2014] EWCA Civ 1403

Lord McAlpine of West Green v Bercow [2013] EWHC 1342 (QB)

NT1 & another v Google LLC & another [2018] EWHC 799 (QB), [2018] 3 All ER 581

OBG Ltd and another v Allan and others; *Douglas and another v Hello! Ltd and others (No 3)*; *Mainstream Properties Ltd v Young and others* [2007] UKHL 21, [2007] 4 All ER 545

R (Guardian News and Media Ltd) v Westminster Magistrate's Court [2013] QB 618

R v Legal Aid Board, Ex parte Kaim Todner (a firm) [1999] QB 966

R (on the application of British Broadcasting Corporation & another) v Secretary of State for Justice [2012] EWHC 13 (Admin), [2012] 2 All ER 1089

R v Secretary of State for the Home Department, ex parte Simms [1999] 3 All ER 400, [2000] 2 AC 115

Rank Film Distributors Ltd v Video Information Centre [1982] AC 380 (HL)

The Queen (on application of Bridges) v Chief Constable of South Wales Police & others

[2019] EWHC 2341 (Admin)

The Queen on the application of The National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department & another [2018] EWHC 975 (Admin)

UNITED STATES

Abrams v United States, 10 November 1919, 250 U.S. 616 (1919)

Carpenter v United States, 22 June 2018, 138 S. Ct. 2206 (2018)

Cohen v California, 7 June 1971, 403 U.S. 15 (1971)

Detroit Free Press v John Ashcroft, 26 August 2002, 303 F.3d 681 (6th Cir. 2002)

Mata v Avianca Inc., 22 June 2023, Case no 22-cv-1461 (PKC) (S.D.N.Y.)

Olmstead v United States, 4 June 1928, 277 U.S. 438 (1928)

PM & others v OpenAI LP & others Case no 3:23-cv-03199, United States District Court, Northern District of California (filed on 28 June 2023)

Ravin v State of Alaska, 27 May 1975, 537 P.2d 494 (1975)

Richmond Newspapers v Virginia, 2 July 1980, 448 U.S. 555 (1980)

Retail, Wholesale and Department Store Union (RWDSU) & others v Dolphin Delivery Ltd., 18 December 1986, [1986] 2 S.C.R. 573

Stanley v Georgia, 7 April 1969, 394 U.S. 557 (1969)

Silverman & others v OpenAI Inc. & others Case no 3:23-cv-03416, United States District Court, Northern District of California, San Francisco Division (filed on 7 July 2023)

Tremblay & Awad v OpenAI Inc. & others Case no 4:23-cv-03223-KAW, United States District Court, Northern District of California, San Francisco Division (filed on 28 June 2023)

TABLE OF STATUTES

CANADA

Canadian Bill of Rights S.C. 1960, c. 44.

Canadian Charter of Rights and Freedoms

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5

Quebec Act Respecting the Protection of Personal Information in the Private Sector, 1993

EUROPE AND THE EUROPEAN UNION

Statutes/Regulations

Commission Decision 2000/520/EC of 26 July 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000, L 215/7, 25.8.200. Known as the 'Safe Harbour Privacy Principles'.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016, L 207/1, 1.8.2016. Known as the 'EU-US Privacy Shield'.

Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code, OJ 2015, L 343, 29.12.2015.

First Council Directive of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community (68/151/EEC), OJ 1968, No L 65/8, 14.3.68 (repealed).

Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (recast), OJ 2013, L 269, 10.10.2013.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ 2016, L 119/1, 4.5.2016 (the General Data Protection Regulation or GDPR).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018

OJ 2018, L 295/39, 21.11.2018.

Directives

Council Directive of 10 February 1975 on the approximation of the laws of the Member States relating to the application of the principle of equal pay for men and women (75/117/ EEC) OJ 1975, No L 45/ 19, 19.2.1975 (Equal Pay Directive)

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, No L 281 /31, 23. 11. 95 (Directive 95/46).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) OJ 2000, L 178, 17.7.2000 (also referred to as eCommerce Directive 2000/31).

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002, L 201/37, 31.7.2002.

Directive 2009/101/EC of the European Parliament and of the Council of 16 September2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent, OJ 2009, L 258/11, 1.10.2009.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L 119, 4.5.2016 (Law Enforcement Directive).

Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, OJ 2017, L 169/46, 30.6.2017.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ 2019, L 130/92, 17.5.2019.

Treaties/Conventions

Charter of Fundamental Rights of the European Union (2012/C 326/02) OJ 2012, C 326/391, 26.10.2012.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No 108, 1981, Strasbourg, France (Convention 108)

European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950, as amended by Protocols Nos. 11, 14 and 15, and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16.

Modernised Convention for Protection of Individuals to the Processing of Personal Data, adopted on 18 May 2018, Elsinore (Helsingør), Denmark (Convention 108+)

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (2007/C 306/01), signed at Lisbon, on 13 December 2007, OJ 2007, C 306/01, 17.12.2007. (Treaty of Lisbon)

Treaty on European Union (Consolidated), OJ 2016, C 202/1, 7.6.2016 (originally signed at Maastricht, on 7 February 1992, Treaty of Maastricht).

Treaty on the Functioning of the European Union (Consolidated), OJ 2016, C 202/1, 7.6.2016., formerly the Treaty Establishing the Economic Community, signed at Rome, on 25 March 1957 (Treaty of Rome).

GERMANY

Basic Law for the Federal Republic of Germany / Grundgesetz für die Bundesrepublik Deutschland (GG)

German Civil Code / Bürgerliches Gesetzbuch (BGB)

SOUTH AFRICA

(Listed below is the legislation referred or discussed from the Republic of South Africa. Where possible, the subordinate legislation used, is listed under its empowering statute.)

Child Justice Act 75 of 2008

Companies Act 71 of 2008

Constitution of the Republic of South Africa, 1996 (Constitution)

Constitution of the Republic of South Africa Act 200 of 1993 (Interim Constitution)

Consumer Protection Act 68 of 2008

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007

Criminal Procedure Act 51 of 1977

Expungement of Criminal Records GN 513 in *Government Gazette* 32205 of 6 May 2009

Criminal Procedure Amendment Act 16 of 2021

Cybercrimes Act 19 of 2020

Proclamation R42 in *Government Gazette* 45562 of 30 November 2021

Divorce Act 70 of 1979

Drugs and Drug Trafficking Act 140 of 1992

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

Immorality Act 23 of 1957 (renamed the Sexual Offences Act; repealed)

Income Tax Act 58 of 1962

Indecent or Obscene Photographic Matter Act 37 of 1967 (repealed)

Medicines and Related Substances Control Act 101 of 1965

National Health Act 61 of 2003

Health Professions Act 56 of 1974

Ethical Rules of Conduct for Professionals

Occupational Health and Safety Act 85 of 1993

Promotion of Access to Information Act 2 of 2000 (PAIA)

Promotion of Administrative Justice Act 3 of 2000 (PAJA)

Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

Protection of Personal Information Act 4 of 2013 (POPI)

Guidelines to Develop Codes of Conduct GN 75 in *Government Gazette* 44191 of 26 February 2021

Proclamation R21 in *Government Gazette* 43461 of 22 June 2020

Regulations relating to the Protection of Personal Information Act, GN R 1383 in *Government Gazette* 42110 of 14 December 2018

Publications Act 62 of 1974

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)

Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill B28- 2023, *Government Gazette* 49189 of 25 August 2023

Uniform Rules of the High Court

UNITED KINGDOM

Data Protection Act 2018

Human Rights Act 1998

Rehabilitation of Offenders Act 1974 (1974 Act)

UNITED STATES

Bill of Rights to the United States Constitution