Wits School of Law

Johannesburg, South Africa

DATA PROTECTION AND BORDERLESS BORDERS: THE EFFECT OF THE NAMIBIAN DATA PROTECTION BILL ON TRANSBORDER DATA FLOWS

by

Fenni P.N Negonga

Submitted in fulfilment of the requirements for the degree

Master of Laws (LLM)

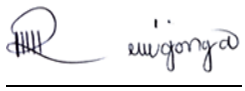
in the Faculty of Commerce, Law & Management

September 2022

Supervisor: Professor Jonathan Klaaren

DECLARATION

I, Fenni P. Negonga (Person number:742599) declare that this Dissertation is my own, unaided work. It is being submitted for the Degree of Master of Laws at the University of Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination at any other University.

Signature:  on the 30th day of September 2022 at Windhoek, Namibia

ACKNOWLEDGEMENTS

I am indebted to several people who helped shape this paper. First and foremost, I would like to thank my supervisor, Prof. Jonathan Klaaren, for his advice, his constructive comments, and, most importantly, his tolerance during the completion of this paper. I am indebted to him for his excellent suggestions and, most notably, his time and commitment to my paper. May you always be blessed.

To my mother, Sophia Negonga, oha ku ti anuwa, ‘uudhigu wondunda wupula eengudhi dhayo’. Only you know what it was like to raise a young girl as successfully as you did. You have performed admirably, mother, and I appreciate your support.

Thirdly, my gratitude goes to the one person, my friend and colleague Lorenzo Ipinge, who always appreciated my hard work and ensured that there was always hope. I appreciate your steadfast support. To my childhood friend Josephine Amushila, thank you once again for editing my second dissertation. Success is in the details; thank you for ensuring that I always paid close attention to every little detail. Lastly, I would want to express my heartfelt appreciation to my daughter Jerlina Ombili, my beloved sisters Selma and Sophia Negonga, Alice Nakale, Etutala Rebekka Shivute, Wilhelmina Kambala, Martha Ndeyapo, and Raina Nambinga for their unwavering support and belief in me.

TABLE OF CONTENTS

DECLARATION 1
ACKNOWLEDGEMENTS 2
LIST OF ABBREVIATIONS 6
ABSTRACT 9
CHAPTER 1 1
Overview of the Study 1
1.INTRODUCTION 1
2. BACKGROUND TO THE STUDY 4
3. ORIENTATION OF THE STUDY 9
3.1 Problem Statement 10
3.2 Research Objectives and Research Questions 12
3.3 Literature Review 13
3.3.1 Summary of the Literature Review 13
3.3.2 Review 14
3.4 Methodology 21
4. CONCLUSION 22
CHAPTER 2 27
Borderless Borders and Data Protection 27
1. DEFINING DATA PROTECTION AND TRANSBORDER DATA FLOWS 27
2. INTERNATIONAL AND REGIONAL REGULATORY FRAMEWORKS ON TRANSBORDER DATA FLOWS 29
2.1 International Instruments 30
2.1.1 The ICCPR and other UN Instruments 31
2.1.2 Organisation for Economic Cooperation and Development Guidelines, 1980 32
2.1.3 Council of Europe Convention 108 33
2.1.4 Council of Europe Convention 108 + ... 33
2.2 Regional Instruments 34
2.2.1 African Charter on Human and Peoples' Rights 34
2.2.2 Malabo Convention 35
2.2.3 SADC Uncitral Model on Data Protection 36
2.3 Conclusion 36
3.REGULATORY OBJECTIVES: A TYPOLOGY OF REGULATORY APROACHES USED BY THE WORLD'S LEADING ECONOMIES 37

3.1 The United States Market-Oriented Model 40
3.2 The Chinese National and Public Security Model 43
3.3 The European Union's Rights-Based Model 44
3.4 Recommendations for an EU Model: The Allure of the Middle Ground? 45
3.5 Final Remarks 49
4.CONCLUSION 51
CHAPTER 3 52
Data Protection in Namibia 52
1. INTRODUCTION 52
2. DATA PROTECTION: A HUMAN RIGHTS ISSUE 53
3. THE DEVELOPMENT OF THE RIGHT TO PRIVACY IN NAMIBIA 54
3.1 Common Law 56
3.2 The Namibian Constitution 57
4. CRITICAL ANALYSIS OF THE PROPOSED LEGISLATION: THE DATA PROTECTION BILL, 2013 58
5. CONCLUSION 64
CHAPTER 4 66
OECD Guidelines, 1980: A Comparative Study 66
1. INTRODUCTION 66
2. SUBSTANTIVE SCOPE OF THE OECD GUIDELINES ON TBDF 68
3. RISKS AND UNDERLYING POLICIES 70
4. REVISED OECD GUIDELINES, 2013 71
5. SHORTCOMINGS OF THE REVISED GUIDELINES 73
6. CONCLUSION 74
CHAPTER 5 77
Data Protection in the EU: A Comparative Study From the DPD to the GDPR 77
1. INTRODUCTION 77
2. A HUMAN RIGHT TO DATA PROTECTION 79
3. HISTORY OF THE EUROPEAN DATA PROTECTION LAW 81
4. EUROPEAN DATA PROTECTION DIRECTION, 1995 85
5. SHORT COMINGS OF THE DPD 89
6. SAFE HARBOUR AGREEMENT AND THE SNOWDEN REVELATIONS: A WAKE-UP CALL FOR THE GDPR 93
7. THE GENERAL DATA PROTECTION REGULATIONS 97
7.1 Long Arm of the GDPR: Redefining the Territorial Scope 98
7.2 The Conundrums of Extraterritorial Enforcement: Mission Impossible? 103
7.3 Ex ante Adequacy Requirements for TBDF 105

8. CONCLUSION 106
CHAPTER 6 109
Data Protection in South Africa: A Comparative Study 109
1. INTRODUCTION 109
2. THE RIGHT TO PRIVACY IN SOUTH AFRICA 110
3. THE POPI ACT 113
4. TERRITORIAL SCOPE 114
5. EX ANTE ADEQUACY REQUIREMENT 116
6. CONCLUSION 116
CHAPTER 7 118
Summary, Conclusions and Recommendations 118
1. INTRODUCTION 118
2. A COMPARATIVE STUDY OF THE SELECTED INTERNATIONAL INSTRUMENTS 120
3. THE NAMIBIAN DATA PROTECTION LAW: A BITTER PILL TO SWALLOW? 124
4. POSITIVE LESSONS FROM ABROAD: RECCOMENDATIONS 127
5. CONCLUSION 132
BIBLIOGRAPHY 136
LEGISLATION 146
TABLE OF CASES 147

LIST OF ABBREVIATIONS

ACHPR	African Charter on Human and Peoples' Rights
AI	Artificial Intelligence
AU	African Union
APEC	Asia-Pacific Economic Cooperation
BCR	Binding corporate rules
CC	Contractual clauses
CCL	Cabinet Committee on Legislation
CFR	Charter of Fundamental Rights (EU)
CJEU	Court of Justice of the European Union
DPAs	Data protection authorities
DPD	Data Protection Directive
EC	European Commission
ECHR	European Court of Human Rights
ECJ	European Court of Justice
EctHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor (EU)
EU	European Union
FISA	Foreign Intelligence Surveillance Act (America)
FTC	Federal Trade Commission (USA)
GDPR	General Data Protection Regulation
HIPSSA	Harmonisation of ICT Policies in Sub-Saharan Africa
ICCPR	International Covenant on Human and Political Rights
IOT	Internet of Things
ITU	International Telecommunication Union
MICT	Ministry of Information and Communication Technology
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OHCR	Office of the United Nations High Commissioner for Human Rights
POPI	Protection of Personal Information Act, 2013
RECs	Regional Economic Communities

SACU	Southern Africa Customs Union
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SCC	Standard contractual clauses
SSC	Social Security Council
TBDF	Transborder Data flows
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
US	United States
WEF	World Economic Forum
WPISP	Working Party on Information Security and Privacy (OECD)
4IR	Fourth Industrial Revolution

‘Data is the pollution problem of the information age, and protecting privacy is the environmental challenge’- Bruce Schneier

ABSTRACT

Data is the sine qua non of the modern economy. The proliferation of digital industries has led to concerns about the misuse of personal data. The resultant risks have sparked ethical and legal concerns across the globe, prompting the adoption of data protection laws. The Namibian constitution guarantees the right to privacy in Article 13, but the country lacks a comprehensive data protection legal framework. The Namibian government issued a Data Protection Bill in 2013.This dissertation critically analyses sections 2 and 48 of the Data Protection Bill dealing with transborder data flows, by employing a two-part theme. In the first instance, the dissertation advocates for a holistic approach that strikes a balance between the individual's right to privacy and the economic imperatives of transborder data flow. In the second instance, the dissertation investigates how to effectively govern transborder data flow with the continuous blurring of lines between physical and virtual worlds, where data transcends territorial borders with a simple click. The mainstream argument for regulating transborder data flow is that if there are no restrictions on the transfer of data to third-party countries, personal data may end up in jurisdictions with the laxest, or more likely, no data protection standards, just as money ends up in tax havens. To put the oft-quoted tax analogy into context, there may be nothing preventing international data processors from circumventing domestic data protection requirements by gravitating personal data to data havens. Through an elaborate comparative analysis, primarily referencing three instruments: the oecd Guidelines, the GDPR, and the POPI Act; the dissertation looked at how these issues are considered and whether the Namibian Data Protection Bill matches up to these standards. The analysed regulatory regimes varied; nonetheless, a corollary was drawn to adopt a broader EU-style territorial scope. This dissertation recommends that section 2 of the Bill should be amended to conform with Article 3(2) of the GDPR (targeting test/market principle). The chosen approach actively embraces the fourth industrial revolution by allowing data protection to 'travel' with personal data wherever it goes in a globalised world.

Keywords: *data protection law, transborder data flow, data havens, internet, disruptive technologies, territorial scope, borderless borders, human rights centric, economic growth, holistic approach.*

CHAPTER 1

Overview of the Study

'Aware of it or not, we are all heirs to potent enlightment ideas in matters relating to control. If knowledge is good, and informed action is preferable to the alternative, why shouldn't we expect institutions of all kinds to maximize their grip on the lives of those they deal with? If government and private organisations are pursuing what are recognized as legitimate ends, why shouldn't they do so as efficiently as possible?'- James B Rule[1]

1.INTRODUCTION

The world is currently embroiled in a tug of war over personal data access.[1] Private companies and governments, as the quote above suggests, have an insatiable appetite for data, believing in its ability to inform and streamline efficient decision-making.[2] Individuals are, however, losing this tug of war due to a lack of legal protection. Data protection law has been labelled a 'dead letter' as legislation and judicial findings allegedly have only a marginal effect on data processing practices.[3] The fluid nature of technological advancements continues to challenge the delicate balance that the classical data protection principles sought to maintain.[4] This has provoked renewed skepticism about the ability of these legal instruments to protect users from potential abuse. Consequently, lawmakers should prioritise maintaining this balance in the era of digital footprints.

Data in the 21st century is like oil in the 18th century; an immense and untapped asset.[4]Global Partners Digital has argued that, although, the analogy has become a cliché, it

[1] James B Rule *Privacy in the Peril: How We Are Sacrificing a Fundamental Right for Security and Convenience* (2007) at 192.

[2] Orla Lynskey *The Foundations of EU Data Protection Law* (2015) at 1.

[3] Bert-Jaap Koops 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 1-14 at 2.

[4] Global Digital Partner 'Travel Guide to the Digital World: Data Protection for Human Rights Defenders' (2018) last accessed from *https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf* on 12 July 2022.

alludes to contemporary practices that are real and grave.[5] There is a general consensus that the amount of data collected has grown at an exponential rate, and it looks like this trend will continue indefinitely.[6] This collection covers emerging technologies that are continuously influencing legal systems.[7] Cloud computing, Big Data, the Internet of Things ('IoT'), Artificial Intelligence ('AI'), cryptography, sensors, robotics, and algorithms are examples.[8]

The COVID-19 pandemic has accelerated the transition to a digital society.[9] People now rely almost entirely on digital tools to socialise, work, and access government services, creating digital footprints.[10] Similarly, almost every day we get phone calls, mail, and electronic communications from corporations throughout the world wanting to sell us their services or solicit our money.[11] How do they get access? How do they learn our patterns of behaviour? Who gathers, sells, and swaps our personal information? This is a direct consequence of the phenomena known as 'Transborder Data flows' ('TBDF').[12]

---

[5] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius 'The European Union general data protection regulation: What it Is and What it Means' (2019) 28 *Information & Communications Technology Law* 65–98 at 65. See also Global Digital Partner op cit note 4 at 5.

[6] Dário Moura Vicente & Sofia de Vasconcelos Casimiro 'Data Protection in the Internet: General Report' in Dário Moura Vicente & Sofia de Vasconcelos Casimiro (eds) *Data Protection in the Internet* (2020) 1-44 at 1. See Also L Swales 'The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock' (2022) 25 *PELJ* 2-32 at 2. Toriqul Islam Md. & Mohammad Ershadul Karim 'Extraterritorial Application of the EU General Data Protection Regulation: An International Law Perspective' (2020)28 *IIUM Law Journal* 531-565 at 532. Hoofnagle et al op cit note 5 at 65ff. See also M Kuneva 'Roundtable on Online Data Collection, Targeting and Profiling' (2009) last accessed from *http://europa.eu/rapid/press-release_SPEECH-09-156* on 07 June.

[7] Marcelo Corrales, Mark Fenwick & Nikolaus Forgó 'Disruptive Technologies Shaping the Law of the Future' in Marcelo Corrales, Mark Fenwick & Nikolaus Forgó (eds) *New Technology, Big Data, and the Law* (2017) at 2.

[8] Ibid.

[9] UNCTAD 'Cross-border Data Flows and Development: For whom the Data Flow' (2021) last accessed from *https://unctad.org/webflyer/digital-economy-report-2021* on 06 June 2022.

[10] Hoofnagle et al op cit note 5 at 66.

[11] Gregory Shaffer 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) 25 *The Yale Journal of International Law* 27–28 at 27.

[12] Ibid.

The epoch of globalisation has revealed the growing significance of data and data flows, including TBDF, in a contemporary economy.[13] Data moving across borders is critical for global commerce. Since personal data is so valuable, many businesses are prepared to forgo receiving payment in exchange for accessing it for their digital services.[14] Data is becoming an indispensable economic resource from which value can be extracted, and its potential effect on the future economic growth of countries is multi-dimensional.[15] According to a McKinsey report, 'in 2014 alone, data flows accounted for $2.8 trillion of global GDP and TBDF now generates more economic value than traditional flows of traded goods.'[16] Similarly, according to a UN research, between 4 and 15% of the global GDP is attributed to the digital economy.[17]

Beyond the economic impact of data, its effect on innovation is unequivocal. According to the World Economic Forum's ('WEF') Global Information Technology Report, new types of innovation, including changes to business models, are a significant part of innovation.[18] Conversely, it is the capacity to transfer data across borders that is enhancing corporate procedures and enabling companies to reconfigure their approach. [19] In

[13] Annegret Bendiek & Magnus Römer 'Externalizing Europe: the global effects of European data protection' (2019)21 *Digital Policy, Regulation and Governance* 32-43 at 32. See also Robert Pepper, John Garrity, Connie LaSalle & Cisco Systems 'Cross-Border Data Flows, Digital Innovation, and Economic Growth'(2016) last accessed from *https://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/* on 11 March 2022.

[14] Costa-Cabral, Francisco & Lynskey Orla 'Family ties: the intersection between data protection and competition in EU Law' (2017) 54 *Common Market Law Review* 11-50 at 12.

[15] UNCTAD op cit note 9 at 3.

[16] Last accessed from *https://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/* on 11 March 2022.

[17] Sasa Jovanovic 'Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation' (2020) last accessed from *https://digitalcommons.bowdoin.edu/honorsprojects/175* last accessed on 11 July 2022. See also UNCTAD 'Digital Economy Report 2019: Value Creation and Capture Implications for Developing Countries' (2019) last accessed from *https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.* on 11 July 2022.

[18] Last accessed from *https://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf* last accessed on 30 July 2022.

[19] Ibid.

acknowledging the significance of data and cross-border data flows, the G20 Trade Ministers reached the following resolution in June 2019:[20]

> '[T]ransborder flow of data, information, ideas, and expertise increases productivity, innovation, and sustainable development. Nonetheless, we acknowledge that the free flow of data presents significant obstacles. By continuing to resolve concerns relating to privacy, data protection, intellectual property rights, and security, we may further facilitate data free flow and bolster consumer and corporate confidence. The digital economy will benefit from the open flow of data that is supported by trust. We will work together to promote the interoperability of many frameworks, and we recognise the importance of data for development.'[21]

Notwithstanding the undeniable benefits of ICT, with the increasing collection, processing, and transmission of personal data across national boundaries, individuals' data is vulnerable to misuse, theft, and loss. The evolving threats in the cyber landscape and the prevalence of crimes related to personal data, such as, identity theft and fraud, have prompted jurisdictions across the world to adopt data protection laws. These laws are meant to mitigate evolving threats. The following section provides a brief background to this research.

2. BACKGROUND TO THE STUDY

Data and its transborder movement are vital. It is noted in the preceding section that data flows can help achieve sustainable development goals. This study will assess Namibia's legislative framework on TBDF in a digital environment. Fishman argues that, as the third world struggles to join the modern world and enjoy its benefits, these countries now recognise that information resources should be developed in parallel to industrialisation as key economic goals. In addition, governments must have some control over the use of national resources.[22]

[20] G20 Digital Economy Task Force 'Mapping Approaches to Data and Data Flows' last accessed from *https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf* on 17 March 2022.

[21] Ibid.

[22] William Fishman 'Introduction to Transborder Data Flows' (1980) 16 *Stanford Journal of International Law* 1-26 at 1.

The Vision 2030 manifesto of the Namibian government, outlines that ICT must be the most important sector in the economic development of the country by 2030.[23] From the perspective of a developing country, ICT is both a prerequisite for economic progress and a major potential contributor to economic growth.[24] According to Pria Chetty, the demand-driven need to develop Namibia into a knowledge-based economy where data and personal data are shared in compliance with laws and principles of treatment is vital to achieving this goal.[25] Regrettably, despite multiple high-profile data security breaches, Namibia does not have a complete legal framework for data protection. There exists only a brief section on data subject rights and protection in the Credit Bureau Regulations General Notice No. 5518 of 2014. A detailed account of the Namibian Data Protection Framework will be given in chapter 3.

A notable and equally concerning data breach incident in Namibia was the 2018 Namibian Social Security Commission ('SSC') leak.[26] Personal information about thousands of people registered with the SSC was leaked on the institution's website.[27] The leaked data included private client information such as salaries, home addresses, and copies of national documents, including identity cards and passports.[28] No accountability nor an official remedy followed the data breach of this magnitude. Given Namibia's lack of a data protection law, it is critical that the government take the necessary steps to protect its citizens' personal data. Namibia recognises the right to privacy as a fundamental human right in Article 13 of the Namibian Constitution, which states inter alia that:

> 'No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety of the economic well-being of the country, for

[23] Namibian Vision 2030 manifesto last accessed from *https://www.npc.gov.na/wp-content/uploads/2021/11/vision_2030.pdf* on 30 August 2022.

[24] William L Fishman et al op cit note 22 at 23.

[25] Presentation of the Draft Data Protection Policy for Namibia by Pria Chetty, ITU International Legal Expert on Data Protection last accessed from *https://www.itu.int/en/ITU-D/Projects/ITU-EC CP/HIPSSA/Documents/Incountry%20support%20documents/Namibia_Data_Protection_Draft_Policy_Chetty_Version1.pdf* on 02 June 2022.

[26] Shinovene Immanuel & Okeri Ngutjinazo 'SSC leak exposes personal info online' *The Namibian Newspaper* 11 June 2018 at 1.

[27] Ibid.

[28] Ibid.

the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.'

It is trite that there is a correlation between the right to privacy and data protection.[29] Indeed, it is impossible wholly and/or decisively to detach the right to privacy from the data protection rights. This is mainly because the underlying data protection principles do, in fact, guard the privacy of data subjects. Wacks argues that the exploitation and misuse of personal data lie at the heart of privacy concerns.[30] According to Maria Tzanou, most national data protection texts, or their travaux préparatoires, often refer to privacy as one of the main aims of data protection legislation.[31] The interconnectedness of privacy and data protection has prompted some academics to argue that data protection functions as a transparency tool that enables certain processing, but privacy functions as an opacity tool against which admissible constraints should be evaluated.[32] As a corollary, the author contends that the two cannot be considered in isolation as they are interlinked.

The right to privacy is protected under various instruments in terms of international human rights law. At a regional level, the African Charter on Human and Peoples' Rights ('ACHPR') does not expressly provide for the right to privacy. At an international level, Namibia has ratified the International Covenant on Civil and Political Rights (ICCPR), which under Article 17 of the ICCPR reinforces Article 12 of the Universal Declaration of Human Rights ('UDHR'). The latter guarantees a fundamental human right to privacy.[33]Notably, the General Comment No. 16 on Article 17 ICCPR refers expressly to the right of protection of personal data.[34]

---

[29] William L Fishman op cit note 22 at 1.

[30] Raymond Wacks *Privacy and Press Freedom* (1995) at 23.

[31] Maria Tzanou *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance* (2017) at 24.

[32] Ibid at 247.

[33] Namibia has ratified the ICCPR on 28 November 1994.

[34] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies last accessed from *https://www.refworld.org/docid/453883f922.html* on 27 June 2021.

Article 144 of the Namibian Constitution states: *'Except as otherwise specified by this Constitution or an Act of Parliament, the general norms of public international law and international agreements that bind Namibia according to this Constitution must be incorporated into Namibian law.'* The Human Rights Committee has highlighted that states parties to the ICCPR have a positive duty to implement legislation and other measures to give effect to the prohibition against privacy intrusion and harassment as well as to preserve this right to privacy.[35]

Although the right to privacy is a key concept in human rights law, the fundamental right to privacy enshrined in the Namibian constitution is not adequate to deal with issues arising from information and technology ('ICT'). Consequently, the Namibian government has drafted a Data Protection Bill, 2013 ('the Data Protection Bill') to protect citizens against abuse of their personal data and to regulate transborder data transfers. Namibia's government seems to be in the final stages of refining a draft Data Protection Bill. At the time of writing this dissertation, the bill was at the Cabinet Committee on Legislation ('CCL').[36] The Bill has been criticised for being worryingly thin on personal data protection and for lacking coherence and consistency with global trends and standards for data protection. [37]

While relying on international jurisprudence does not substitute Namibia for adopting its own comprehensive data protection law, the international jurisprudence on data protection laws and challenges faced over the years with the advent of the internet, provide significant lessons. It is beneficial to consider these lessons at an early stage of legislative drafting and incorporate them into the Data Protection Bill de lege ferenda. As the adage goes, 'a stitch in time saves nine'. The analogy is to mend a small rip versus sewing an entirely new seam.[38]

---

[35] Last accessed from at *https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx* on 27June 2021.

[36] Information received from an official at the Ministry of ICT in Namibia.

[37] Links, F 'Tackling Cybersecurity/Crime in Namibia: Calling for a Human Rights Respecting Framework' (2018) Last accessed from *https://ippr.org.na/publication/tackling-cybersecurity-crime-namibia* on 23 June 2020.

[38] See also Guidelines on the Territorial Scope of the GDPR (Article 3)- Version for Public Consultation Adopted 16 November 2018.Last accessed from *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf* on 31 July 2022.

Moreover, today's increasingly connected planet and mass TBDF warrant that there is an alignment of the various national laws on Data Protection with international standards.[39]

This study will critically analyse the proposed Namibian Data Protection Bill (with specific reference to provisions dealing with TBDF), considering international data protection standards. Whilst recognising the existence of numerous exemplary international data privacy instruments, this study focuses on three influential instruments that are based on the fundamental rights and values of individuals, namely: The Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ('OECD Guidelines'), the General Data Protection Regulation (EU) 2016/679 ('GDPR') and the South African Protection of Personal Information Act, 2013 (Act No. 4 of 2013) ('POPI Act').

Historically, the OECD Guidelines were the first mechanisms established to approximate regulations in this field. The GDPR, on the other hand, is regarded as the gold standard for data protection. Lastly, the POPI Act has been chosen because of the link between Namibia and South Africa. Both countries are developing member nations of the Southern African Development Community ('SADC') and the Southern African Customs Union ('SACU'), showing a degree of integration based on comparable economic and social systems. To this end, the discussion will be incomplete without an exposition of the law in South Africa.

To put the above in context, the dissertation examines sections 2 and 48 of the Data Protection Bill. Section 48 lays down an ex-ante data protection regime that will be explained later in this research. Section 2(2) on the other hand states, inter alia, that:

> *'This Act is applicable:*
>
> *(a) to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established in Namibia or Namibian High Commission or Representative Office abroad;*

[39] OECD Guidelines on the Protection of Privacy and Transborder Data Flows (1980) last accessed from *https://www.oecd.org* on 05 May 2021.

(b) to the processing of personal data by a controller who is not permanently established in Namibia, if the means used, which can be automatic or other means is located in Namibia, and is not merely for the purposes of transit of personal data through Namibia.'

Section 2(2)*(b)* of the Bill has proven controversial and problematic to say the least. No aspect of the Namibian Data Protection Bill's architecture has provoked more controversy than its jurisdictional limitations. In terms of the above section, the Bill only applies when processing of data is carried out by 'means' located in Namibia (jurisdiction tied to territorial borders). This research will demonstrate that the Data Protection Bill fails to measure up to comparable standards in the GDPR. Article 3(2) of the GDPR provides for an extraterritorial application. Article 3(2) is one of the new salient elements introduced by GDPR to address regulatory conundrums caused by the borderless nature of the internet and disruptive technologies. Consequently, this research will argue that the direction of the Data Protection Bill is essentially antiquated. It is worth noting that section 2(2)*(b)* of the Namibian Data Protection Bill is similar, albeit to a lesser extent, to the former global benchmark for data protection, the European Data Protection Directive, 1995, which has been superseded by the GDPR.[40] Evidently, Namibia has jumped onto a data protection bandwagon riddled with obsolete regulations.

This chapter will provide the conceptual and contextual background as well as the rationale for the study. The chapter will comprise the problem statement, the research objectives, and the methodology employed in the study. It will provide an overarching review of the literature that supports the study's research questions and stated concerns. This will be achieved by presenting an overview of worldwide debates on data protection and the governance of TBDF. Reference to relevant research and literature, as well as the analysis of findings and conclusions in the latter, will be used to examine historical and contemporary discussions on the regulation of TBDF.[41]

3. ORIENTATION OF THE STUDY

[40] Section 2 of the Namibian Data Protection Bill.

[41] Clever Mapaure '*Water Wars: Legal Pluralism and Hydropolitics in Namibian Water Law*'(unpublished LLM thesis, University of Namibia, 2009) last accessed from *https://repository.unam.edu.na/bitstream/handle/11070/499/mapaure2009.pdf?sequence=1&isAllowed* last accessed on 20 July 2021.

3.1 Problem Statement

> *'[T]he fantastic advancements in the sphere for digitalisation pose a greater danger to the individual's right to privacy.'*[42]

This study's problem is guided by one key issue: the extraterritorial effect of the Namibian Data Protection Bill on TBDF. At its conception, the internet was a virtual space and a boundless medium of communication.[43] However, the maturing of the internet, spurred by recent improvements in ICT, has generated and aggravated several privacy issues. Regardless, the internet and any actions performed on it should be subject to the same legal scrutiny as any other human action.[44] As Goldsmith has argued, in the cyberspace, individuals engage in activities that would be governed by the state, national, or international law if they occurred in person.[45] They defame, invade privacy, harass, and commit business delict.[46] Given the borderless nature of the internet, how can it be effectively regulated in a world where data crosses borders with the press of a button?[47]

The first step is always to determine if a certain legislation or regulatory framework applies.[48] In determining whether a legal entity is subject to the provisions of a given piece of legislation or regulatory instrument, one must first determine whether the provisions of that piece of legislation or regulatory instrument are relevant to the activities of that corporate entity.[49] There are two common factors that determine the applicability of the law: one has to do with the sector or line of activity in which the entity operates, and the other is solely geographical.[50]

---

[42] Earl Warren, 14th Chief Justice of the United States. See Ana Gascon Marcen 'The Extraterritorial Application of the European Union Data Protection Law' (2019) 23 *SYBIL* 413-425 at 413.

[43] Ibid at 414.

[44] Ibid.

[45] Jack L. Goldsmith 'Against Cyberanarchy' (1998) 65 *The University of Chicago Law Review* 1199-1249 at 1202.

[46] Ibid.

[47] Ana Gascon Marcen op cit note 42 at 413.

[48] Noriswadi Ismail & Edwin Lee Yong Cieh *Beyond Data Protection: Strategic Case Studies and Practical Guidance* (2013) at 136.

[49] Ibid.

[50] Ibid.

Traditionally, territorial borders delineate areas within which different sets of legal rules apply. As more human activities, industrial processes, and research become inextricably connected to the internet, its effectiveness is questioned. In an ideal world, the borderless internet needs a different set of rules than those that govern physically defined territories.[51] Cyberspace defies the law's conventional reliance on geographical boundaries; it's a realm characterised by computers and usernames rather than geographical markers.[52] Global computer-based communications bypass territorial boundaries, spawning a new sphere of human conduct and weakening the viability and validity of laws based on physical boundaries.[53]

This research identifies deficiencies in the Data Protection Bill pertaining to the regulation of TBDF in a borderless environment. Currently, only processors with 'means' in Namibia are subject to the Bill. Regrettably, this does not offer comprehensive regulation for TBDF. Moreover, it does not offer comprehensive protection of personal data in a borderless environment. In the early days of the internet, the data controller, the data subject, and the data processing means were often located in the same territory.[54] Today, data processing is a global phenomenon.[55] Technological advancement has enabled remote data processing. Therefore, the Namibian Data Protection Bill, in its current form, can easily be circumvented when personal data is handled remotely.

According to the UNCTAD, in the borderless digital economy, data protection and TBDF are intimately associated with the trade in goods and services.[56] For some, the problem is ensuring that when data is moved beyond a particular country, it continues to get the same

[51] Ibid.

[52] Brian H. Holland 'The Failure of the Rule of Law in the Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty' (2005) 24 *J. Marshall J. Computer & Info. L.* 1 1-34 at 1f. See also Jack L. Goldsmith op cit note 44 at 1202f.

[53] Ibid.

[54] Adèle Azzi 'The Challenges Faced by the Extraterritorial Scope of General Data Protection Regulation' (2021) Last accessed from available *https://www.jipitec.eu* on 01 April 2021.

[55] Ibid at paragraph 5.

[56] UNCTAD 'Data protection regulations and international data flows: Implications for trade and develop-ment' (2016) Last accessed from *https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf* on 13 April 2021.

level of protection as it had inside that jurisdiction. Limited protection may diminish consumer trust, while excessive protection may unduly restrict businesses, leading to unfavourable economic repercussions.[57] Since TBDFs are becoming more and more reliant on the internet, it is very important that regulations take on a global character and encourage harmonisation with other frameworks.[58]

Ultimately, as this research will show, the goal of a broader territorial scope is that the protection offered by data protection legislative frameworks must 'travel' with personal data wherever it goes in a globalised society where data crosses borders with a simple click. Furthermore, as noted earlier in this paper, the common occurrence of data breaches has accentuated the need for robust legislative interventions to hold accountable those responsible for processing personal data.

3.2 Research Objectives and Research Questions

The purpose of this research is to critically analyse legislative proposals, culminating in the Data Protection Bill, which is set to be tabled in parliament. In particular, the analysis focuses on the provisions dealing with the regulation of TBDF. Additionally, the research intends to evaluate the extent to which the Namibian Data Protection Bill conforms with international standards on data protection and whether there is a need to bring it on par with recent developments in data protection.

This will be achieved through an elaborate examination and comparative analysis of the Data Protection Bill with the legislative approaches adopted by the General Data Protection Regulation (EU) 2016/679, the South African Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and the Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (OECD Guidelines).

The comparative research method employed herein is believed to provide much broader solutions than a study devoted to the law of a single nation.[59] By analysing

[57] Ibid at xi.

[58] Ibid.

[59] Konrad Zweigert & Hein Kötz *An Introduction to Comparative Law* (1998) at 15.

international patterns, borrowing, modifying, and adapting, a country may construct a legal fabric that is sui generis and more diverse than if left to its own domestic inclinations.[60] The research synthesises the issues in debate regarding the extraterritorial reach of data protection law and offers perspectives on how and why it should also be adopted in the Namibian context. In a nutshell, research seeks to answer one main question:

- Whether the Data Protection Bill offers comprehensive protection to data subjects in terms of TBDF in accordance with internationally recognised standards.

3.3 Literature Review

3.3.1 Summary of the Literature Review

The primary purpose of a literature review is to establish a scholarly significance of the research problem and research questions, as outlined above. This literature discusses the breadth of existing publications, assesses their implications, and identifies the lacunas. It offers a general organisational structure and a conceptual unification of international data protection legal principles applicable to TBDF.[61] In particular, the literature review will survey intellectual progress in the fields of data protection and TBDF, including theoretical viewpoints, notable theoretical debates, and earlier research insights.

From the bulk of the literature reviewed, there is a consensus that the rapid increase in TBDF has generated several complex legal problems. By its nature, the law tends to be related to a particular territory. TBDF, on the other hand, is a global phenomenon that mocks legal jurisdiction, defies its efficacy, and tests the law's ability to keep up with growing ICT developments.[62] The examined mainstream literature focuses on two key issues: first, can the law regulate ICT in the realm of data protection? Second, how best can the law's concept of jurisdiction be effectively tailored in the context of data protection in a borderless world?

In summary, the existing corpus of literature dating back to the 1970s recognises the necessity for governments to enact robust data protection laws that include provisions for

[60] Ibid.

[61] Clever Mapaure op cit note 41 at 37f.

[62] Michael Kirby 'Legal Aspects of Transborder Data Flows' (1991) 11 *Computer Law Journal* 233-246 at 233.

controlling TBDF in the cyberspace. Furthermore, there is a growing trend amongst law makers to draft data protection legislation in such a way that the protection provided by the data protection legal framework 'travels' with personal data wherever it goes in a globalised society. The EU GDPR (the so-called 'target test') has greatly progressed in this area and follows this position. This research offers perspectives on how and why this approach should be adopted in the Namibian context. Even though the OECD Guidelines and the South African POPI Act take a different approach than the GDPR, both have important lessons to offer.

The issue of a broader territorial scope for transborder data transfers, on the other hand, is not without controversy. On the contrary, many privacy and data protection scholars have criticised the concept of personal data for becoming overly broad. On the other hand, proponents of the unavoidable extraterritoriality of data protection law, owing to the borderless nature of the internet, argue that there are both direct and indirect enforcement alternatives. This study takes the latter view.

3.3.2 Review

The current epoch of globalisation, advances in communication and technology have resulted in companies, agencies, and organisations storing vast amounts of identifying information electronically. The internet has revolutionised commerce by making it simpler for people to do business across a multitude of jurisdictions.[63] Unfortunately, it has also resulted in hazards and threats. Additionally, it is also susceptible to cyberattacks.[64] Since the 1970s, governments throughout the globe have enacted data protection laws in response to ICT-related issues.[65]

The emergence of new telecommunications technology, which connects computers to networks (primarily the Internet) and enables the movement of data across computer systems, necessitates the harmonisation of rules governing transborder data flows. For instance, Cunha, contends that, in addition to safeguarding their people, nations must have a keen interest in

[63] Robert,L & Stevenson, B 'Plugging the "Phishing Hole: Legislation Versus Technology' (2005) 5 *Duke Law & Technology Review* 1-14 at 1.

[64] The term 'cyberspace' refers to a unique medium or space that has no specific geographical location, but it can be available to anyone anywhere in the world who has access to the Internet (as defined *in Renor v ACLU US 844, 851 (1997*)).

[65] Logan Kugler 'Online privacy: regional differences' (2015) 58 *Communications of the ACM* 18-20 at 18.

making their data protection rules interoperable and even more interchangeable to make transactions involving the transfer of personal data as 'noise-free' as possible.[66]

The regulation of TBDF has always been a component of data protection law. Unfortunately, the evolution of technology poses a threat to the continuing effectiveness of existing regulatory approaches.[67] According to Kirby, in order to regulate TBDF in cyberspace effectively, national laws must include the adoption of 'long-arm statutes' with purported extraterritorial application of one state's law in another territory.[68] In addition, according to UNCTAD, as the global economy transitions toward a networked digital landscape, the necessity for data protection and the need to regulate privacy will increase.[69] To enable international trade and e-commerce, it is essential to comprehend the various strategies and prospective avenues for constructing more suitable legal frameworks at the national, regional, and worldwide levels.[70]

The first attempt to approximate the emerging laws in this field was by the Organisation for Economic Co-operation and Development ('OECD'), which issued guidelines in September 1980.[71] The guidelines set out the following objectives:

> '(i) to achieve the acceptance of certain minimum standards of protection of personal data privacy; (ii) to reduce the differences between relevant domestic rules and practices of states; (iii) to avoid undue interference with flows of personal data between countries; and (iv) to eliminate, to the extent possible, reasons which might induce states to restrict transborder data flows.'[72]

In relation to transborder data flows, the OECD Guideline 17 provide that:

---

[66] Mario Viola de Azevedo Cunha *Market Integration through Data Protection: An Analysis of the Insurance and Financial Industries in the EU* (2013) at 3.

[67] Alison White 'Control of Transborder Data Flow: Reactions to the European Data Protection *Directive' (2014) 5 International Journal of Law and Technology* 230-247 at 230.

[68] Kirby op cit note 62 at 233.

[69] UNCTAD op cit note 55 at iii.

[70] Ibid.

[71] Orla Lynskey op cit note 2 at 2.

[72] Ibid.

> 'A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.'

In the European Union, data privacy is protected as a fundamental right under Article 8 (1) of the Charter of Fundamental Rights and Article 16 (1) of the Treaty on the Functioning of the European Union ('TFEU'). The study examines the legal developments in relation to Article 4 of the European Data Protection Directive[73] ('DPD'), as well as the most recent version of its counterpart, Article 3 of the GDPR. The territorial scope is provided for in Article 4 of the DPD which states, inter alia, that it applies when:

> '[T]he controller is not established on community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said member state, unless such equipment is used only for purposes of transit through the territory of the Community.'

When the DPD was adopted, the internet was still in its infancy.[74] Today, we now live in a world where the internet has outgrown this stage, necessitating the need for more robust protections that provide positive effects in practice.[75] The threats posed by new technologies and globalisation need a creative approach to regulation in order to provide comprehensive protection.[76] Discussions of the expanding scope of personal data have been brewing for some time in the data protection community.[77] As noted above, many privacy and data protection scholars have been critical of the concept of personal data growing too broad.[78] The mainstream literature reviewed in the EU was centered on one central theme, namely the extraterritoriality of data protection regulations.

---

[73] Directive 95/46/EC of the European Parliament and of the Council (1995) Last accessed from *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN* on 11 August 2022.

[74] Ibid.

[75] Anneliese Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South Africa Data Privacy Law: An Evaluation of Selected 'Content Principles'' (2020)53 *Comparative and International Law Journal of Southern Africa* 1-37 at 3.

[76] Ibid.

[77] Dan Svantesson 'Extraterritoriality in the EU Data Privacy Law: The Weak Spot Undermining the Regulations' (2015) 5 *International Data Privacy Law* 226-234 at 234.

[78] Lee Bygrave *Data Privacy Law: An International Perspective* (2014) at 199.

Bygrave characterised article 4 as plausibly the most problematic and baffling of all the DPD provisions.[79] It presented the greatest number of challenges and questions. Additionally, Kristopher Kuner, commenting on the abandoned EU DPD, believes that EU data protection legislation should be interpreted broadly to prevent circumvention.[80] There are numerous examples of globally active internet intermediaries seeking to avoid the jurisdiction of the courts by invoking the business structure they have assumed. In *A v New Zealand Ltd*[81], for instance, Google New Zealand successfully maintained that the plaintiff had an improper defence since its ultimate parent company, Google Inc. (incorporated and based in the US), owns, and oversees the search engine.[82]

In a much more recent case of *Yahoo!, Inc. v. LICRA* [83], a French court ordered Yahoo! Inc. to ban French surfers from viewing Nazi memorabilia on yahoo.com. Yahoo! Inc's contention was that the site was on a California server and designed for the American market. This, however, did not convince the court, nor did the fact that Yahoo! Inc's French subsidiary offered a site customised for French surfers. It found that Yahoo.com's injury, regardless of jurisdiction, occurred in France. This example illustrates potential conundrums connected with article 4 of the EU DPD, especially with the borderless nature of the internet.

In essence, one of the weaknesses of the DPD is that it could not reach a controller processing EU data solely outside the EU, even if the controller has an entity in the EU that is unaffiliated with the processing activity.[84] As soon as technological advancements started to enable remote data processing, the DPD's scope could be easily circumvented.[85] As a solution, Article 3 of the GDPR is intended to prevent any effort to evade EU data protection laws. Thus, Article 3 (1) defines the geographical scope of the GDPR as the processing of personal data in the context of the operations of a controller's or processor's establishment in the Union, regardless of whether the processing takes place in the Union or not.

---

[79] Ibid.

[80] Christopher Kuner 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2021) Last accessed from *http://eprints.lse.ac.uk,* on 27 March 2021.

[81] *A V Google New Zealand Ltd (2012) NZHC 2352 (4).*

[82] See also Dan Jerker B Svantesson op cit note 77 at 229.

[83] *Yahoo!, Inc. v. LICRA 169 F. Supp. 2d 1181, 1186 (N.D. Cal. 2001).*

[84] Azzi op cit note 54 at par. 5ff.

[85] Ibid.

The applicability to processors is new and creates a basis for independent obligations pertaining to processors. The GDPR may, however, also apply to a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU. This is a new and substantial extension to the scope of the regulation and is likely to have a significant impact on its implementation.[86]

According to Svantesson, Article 3(2) of the GDPR utilises the 'targeting' test that has been established in European consumer law through the decisions in the joint cases *Pammer v. Reederei Karl Schluter GmbH & KG11 and Hotel Alpenhof Gesellschaft v. Oliver Heller*.[87] In its ruling, the European Court of Justice (ECJ) found that the following criteria should be used to determine whether a trader has targeted its activities to the member state of the consumer's domicile:

> '[B]efore concluding any transaction with the customer, it is obvious from these websites and the trader's overall behaviour that he/she planned to conduct business with consumers domiciled in one or more member States, including the Member State of the customer's domicile, meaning that the trader intended to enter into a contract with them.'[88]

It has been commended that it is prudent to borrow legal solutions from other domains, and there are many commonalities between consumer protection law and data privacy law. [89] In addition, several prominent authors have supported the targeting test. For example, Reed concedes:[90]

> '[A] vendor who targets the customers of a certain state online has temporarily joined the trade community of that state. Due to this, the vendor is likely to recognise the power of that state's legislator over its dealings and will so willingly offer the required protection.'[91]

---

[86] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) last accessed from *https://edpb.europa.eu accessed* on 05 May 2021.

[87] Dan Jerker B Svantesson op cit note 77 at 229. *Joined Cases C 585/08 and C144/09 [95] Pammer v Reederei Karl Schluter GmbH & KG11 and Hotel Alpenhof GesmbH v Oliver Heller.*

[88] Ibid.

[89] Svantesson op cit note 77 at 235.

[90] Chris Reed *Making Laws of the Cyberspace* (2012) at 225.

[91] Ibid.

Perhaps the most hotly discussed question among many privacy and data protection scholars has been whether personal data is growing too broad in terms of its extraterritorial reach. Mirra Burri has argued that this contention is aggravated by starkly different perceptions and strong opinions on what privacy is and how it ought to be protected in the various EU Member States.[92] This essentially explains the protracted drafting and adoption processes that predated the GDPR, as well as the compromises that its final version entails. Bygrave, for instance, views this regulatory overreach as problematic.[93] This perspective is held by several renowned commentators, including Maier[94], Kuner[95], Moerel[96], and Gömann.[97]

Critics of extraterritoriality have argued that one of its drawbacks is that its enforcement is often confined to territorial limits.[98] Kuner, for example, argues that 'laws that lack the means of being enforced undermine the legal system.'[99] It may look futile to claim that 'country A' will have jurisdiction over certain matters if actual constraints preclude the courts of country A from exercising effective jurisdiction in such circumstances.[100] Conversely, a claim that country A's laws apply to specific fact patterns may be of little value if country A lacks the capacity to enforce its law.[101] This, in Kohl's exquisite language, the 'achilles heel' of extraterritoriality, has been and continues to be a significant and persuasive

[92] Mira Burri and Rahel Schar 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing their Fitness in a Data Driven Economy' (2016) 6 *Journal of Information and Policy* 479-511 at 488.

[93] Lee Bygrave 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16 *Computer Law and Security Review* 252-257at 252.

[94] Benhard Maier 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 *IJLIT* 161-162.

[95]Christopher Kuner 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18 *International Journal of Law and Information Technology* 227-247.

[96] Lokke Moerel 'The Long Arm of the EU Data Protection Law: Does the Data Protection Data Protection Directive Apply to the Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1 *International Data Privacy Law* 28–46 at 46.

[97] Gömann, M 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 *Common Market Law Review* 567 – 590 at 568.

[98] Dan Jerker B Svantesson 'A Jurisprudential Justification for Extraterritoriality in (Private)International Law' (2015) 13 *Santa Clara Journal of International Law* 1-56 at 4.

[99] Kuner op cit note 95 at 227.

[100] Ibid.

[101] Ibid.

argument against extraterritoriality.[102] It is submitted that this exposition, though with merit, fails to recognise contemporary alternatives to enforcement that are available to states.

Notably, proponents of the inevitable extraterritorial reach of data protection legislation, because of the global nature of the internet, say that there are both direct and indirect enforcement methods. It has been argued that because of its novel and sophisticated nature, while traditional methods of enforcement might not be effective for data processors who do not present in a country, there are alternatives to direct or indirect enforcement. Thus, a direct solution would be to involve the role of representatives, cooperation between jurisdictions, and possible international measures against non-compliers. Several experts have highlighted the probable use of collaboration agreements like the mutual legal assistance agreement ('MLA').[103]

In addition, various alternative enforcement tools, such as interdicts, could possibly be used to authorise the blocking of the operator's or its partners' websites or corresponding web connections (in terms of interdicts applied to internet service providers).[104] Svantesson calls these measures 'market-destroying' since they are meant to punish businesses.[105] It involves restricting the party from doing business inside the jurisdiction or rendering the party's dues/obligations unenforceable within the jurisdiction.[106] The effect of this approach is contingent on the market's significance to the operator.[107] Svantesson, however, overlooked the classical justifications for punishment: that is, for deterrence, retribution, prevention, and reform.

Azzi has argued that those who believe that the EU cannot enforce the GDPR beyond Europe, should be mindful that extraterritorial claims, even if unenforceable, may nevertheless have an actual impact.[108] She has further argued that, a number of jurisdictions

[102] Uta Kohl *Jurisdiction and the Internet: Regulatory Competence Over Online Activity* (2007) at 26.

[103] Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its theoretical Justification and Its practical Effect on U.S. Businesses' (2014) 50 *Stanford Journal of International Law* 55-99 at 98.

[104] Ibid.

[105] Ibid.

[106] Azzi et al op cit note 54 at 135.

[107] Ibid.

[108] Ibid.

with extraterritorial data protection laws acknowledge that, despite enforcement issues, extraterritorial data protection laws act as a deterrent for foreign data processors to participate in unlawful processing and provide a level playing field for local companies vis-à-vis foreign companies. Moreover, as noted by Svantesson, although the legal system is generally undermined by law that cannot be enforce; *'morally justifiable legislation, even if it cannot be enforced, has the peculiarity that cannot and should not be disregarded.'*[109]

In terms of the bulk of the literature reviewed, many jurisdictions adopting data protection laws, have expanded the scope of application to have an extraterritorial reach. Although other jurisdictions like South Africa lag. The South African POPI Act, like the Namibian Data Protection Bill is also modelled on the former EU DPD of 1995. The territorial scope of the POPIA is addressed in section 3(1)(b) and applies to the processing of personal information, 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.'

As deduced from this provision, processing activity must regularly be connected to the territory of South Africa in order to apply the POPIA, which is quite a challenging requirement as the processing of personal information crosses borders easily via the internet and by using other technological means such as cloud services.[110] Additionally, the South African POPI Act, also follows the trend of only allowing data to be transferred to countries that provide adequate protection to avoid circumvention and data being gravitated towards data havens. Thus, section 72 of the POPI Act states that a ;'*responsible party may no transfer personal information about a data subject to a third party who is in a foreign country unless such country provides for adequate protection.'*

3.4 Methodology

The research takes a doctrinal methodological approach. As traditionally understood, doctrinal research is aimed at the systematization and critique of a defined body of positive

---

[109] Dan Jerker B. Svantesson op cit note 103 at 59.

[110] Elizabeth De Stadler and Paul Esselaar *A Guide to the Protection of Personal Information Act* (2015) at 1.

law.[111] Technically speaking, the doctrinal method is a two-part source of locating 'the law' and then analysing the texts. Therefore, it might be argued that doctrinal research has aspects of both qualitative and quantitative methodologies within it.[112]

Various sources were accessed for this research. This includes textbooks, scholarly journal articles, and unpublished articles. Because this research is modern, urgent, and important, conventional literature cannot adequate ly address it. Therefore, the research also integrates conveniently available, dynamic, and copious material acquired over the internet via desktop research.[113] These include online publications, journals, conference papers, workshop proceedings, etc.[114]

4. CONCLUSION

So far, this chapter has focused on introducing major concepts and a contextual background along with the rationale of the study. Chapter 1 brings clarity to the concepts of privacy and data protection and considers the differences between them. Additionally, this chapter also contains the problem statement, research objectives, and the methodology employed in the study. In addition, this chapter provides an overarching review of the literature that supports the study's research questions and stated concerns. The last part of the chapter lays down the theoretical and analytical framework of the analysis. This was a was accomplished by a comprehensive discussion of the global debates on the governance of TBDF.

To conclude this section, the literature identifies that the increased importance of data and data flows, including across borders, in the world economy is undeniable. Data is becoming an important economic asset that can be used to create value and foster economic growth.[115]The proliferation of digital industries has led to concerns regarding the misuse of personal data. The resultant risks have sparked ethical and legal concerns across the globe,

[111] Theunis Roux 'Judging the Quality of Legal Research: A Qualified Response to the Demand for Greater Response to the Demand for Greater Methodological Rigor' (2014) 24 *Legal Education Review* 1-29 at 3.

[112] Terry Huptchinson and Nigel Duncan 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 *Deakin Law Review* 83–120 at 116.

[113] Clever Mapaure op cit note 48 at 38.

[114] Ibid.

[115] UNCTAD op cit note 9 at 3.

prompting the adoption of data protection laws and the regulation of TBDF. Below is a summary of the arrangement of this research:

CHAPTER 2: BORDERLESS BORDERS AND DATA PROTECTION

This chapter places Namibia within the context of worldwide data protection in a digital economy. Having established what data and transborder data flows are, the chapter will define major concepts that will be analysed, including data protection, data, TBDF, data subject, data controller, and data processors. Descriptively, the chapter discusses the international jurisprudence on data protection law and TBDF. It begins with a short synopsis of the historical background and the origins of data protection law as well as the regulation of TBDF. In addition, the chapter outlines the international and regional regulatory frameworks in place for data protection and the regulation of TBDF. Lastly, this chapter will focus on the predominant regulatory typologies of the world's leading economies, namely: The United States of America ('US'), China, and the EU.

CHAPTER 3: DATA PROTECTION IN NAMIBIA

This chapter discusses Namibian law regarding the right to privacy and its historical context. To do so, the chapter chronicles the normative foundations of the right to privacy in Namibia, from ancient Roman antecedents through the colonial period to the right to privacy guaranteed by the Constitution today. This analysis will trace the evolution of Namibia's right to privacy. The chapter also describes how the common law and the constitutional right to privacy influence the current Data Protection Bill. This chapter critically analyses the Data Protection Bill's provisions dealing with TBDF. It further illustrates how the African regional data privacy instruments and RECs influenced its final text. The chapter concludes by highlighting the gaps in the Namibia Data Protection Bill relevant to TBDF and how they might be addressed through the comparative analysis that follows.

CHAPTER 4: OECD GUIDELINES ON DATA PROTECTION: A COMPARATIVE STUDY

The current international legal framework for data protection and privacy is founded on instruments such as the 1980 OECD Guidelines. The purpose of this chapter is to discuss the guidelines on TBDF laid down by the OECD with the intention of drawing positive lessons for Namibia.

CHAPTER 5: DATA PROTECTION IN EU: A COMPARATIVE STUDY FROM THE DPD TO THE GDPR

The European data protection regulation offers an excellent 'environment' for Namibian comparison and reference. Since the Namibian Data Protection Bill includes TBDF components like the old EU DPD, Namibian lawmakers may benefit from the EU's matured jurisprudence. This chapter traces the development of Data Protection in the European Union. It discusses the foundational pillars and purposes of data protection law in the EU. The chapter achieves this by tracing the historical accounts of Europe's data protection laws from one of the worst episodes in the history of civilization, the holocaust.

Chapter 5 further explores the jurisprudence of the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (ECJ) on the right to data protection. Data protection has been the subject of significant CJEU case law, and the Court's jurisprudence has changed substantially. Second, the chapter explores legal research and case law on the 1995 DPD, highlighting its shortfalls and explaining why it was superseded by the GDPR. In addition, this section also discusses the widespread internet data surveillance conducted by US intelligence agencies, as disclosed by Edward Snowden, and how it informed the current provisions in the GDPR regulating TBDF.

With the implementation of the GDPR, several jurisdictional issues that existed under the DPD have been resolved. In terms of prescriptive jurisdiction, the GDPR applies extraterritoriality to any organisation that provides goods or services to EU nationals (article 3(2)). This notion is in doctrine defined as the targeted approach. [116] The perspective taken in this paper is for Namibia to consider amending section 2 of the Bill by incorporating article 3(2) of the GDPR de lege frenda. This will allow for data protection to 'travel' with personal data wherever it goes in a globalised world.

CHAPTER 6: DATA PROTECTION IN SOUTH AFRICA: A COMPARATIVE STUDY

The chapter explores the theoretical, legislative, and policy background of the South African Data Protection Law from a comparative perspective. It aims at answering questions

[116] Marina Škrinjar Vidović 'EU Data Protection Reform: Challenges for Cloud Computing' (2016)12 *CYELP* 171-206 at 195.

regarding the regulation of TBDF as well as the background or rationalisation of the position of the statutes and policies in South Africa. This jurisdiction has been chosen for specific reasons. Namibia and South Africa are not just neighbours, but also developing member nations of SADC and SACU, indicating a level of integration based on comparable economic and social systems.

Furthermore, when South Africa was granted the mandate over Namibia by the League of Nations, it also assumed legislative powers over Namibia.[117] The two countries likewise have hybrid legal systems with common law and civil law foundations. To date, Namibian privacy laws are essentially comparable to South African privacy laws.[118] As previously stated in this paper, it is widely acknowledged that data processing of an individual's personal information constitutes a danger to the individual's right to privacy.[119] Having said that, this comparative study would be incomplete if it did not consider South Africa's advances in data protection and the control of TBDF.

CHAPTER 7: SUMMARY, CONCLUSION, AND RECOMMENDATIONS

This chapter examines whether the Namibian Data Protection Bill is likely to remedy the problems that continue to challenge the efficacy of data protection law in numerous jurisdictions, which is a dead letter of the law due to the borderless nature of the internet. The approach chosen in this paper is one of a comparative analysis of how this problem has been dealt in other jurisdictions, primarily referencing: the OECD Guidelines, the GDPR and the POPI Act. The Chapter highlights the prescripts laid down in these instruments and appraise them to the Bill.

Finally, the chapter addresses some general recommendations for Namibia. It suggests ways to enhance and improve the Namibian Data Protection Bill by drawing positive lessons from the GDPR, POPI Act and the OECD Guidelines. These proposals are made with a view to strengthening and improving Namibia’s data protection legislative framework. The GDPR have long been regarded as the gold standard all over the world. Although the analysed

[117] SK Amoo *Introduction to Namibian Law* (2008) 60.

[118] Ibid.

[119] Roos, A ‘Data protection: Explaining the international backdrop and evaluating the current South African position’ (2007) *SALJ* 400-436 at 421.

regulatory regimes varied, this dissertation draws the corollary that a broader EU-style territorial scope (like Article 3(2)) in the Data Protection Bill.

CHAPTER 2

Borderless Borders and Data Protection

1. DEFINING DATA PROTECTION AND TRANSBORDER DATA FLOWS

With the continued blurring lines between the real and virtual worlds, data protection laws, including the regulation of TBDF, appear more imminent than ever in Namibia. This section situates Namibia within the wider global context of data protection. To begin with, this section defines the basic concepts used in this dissertation, such as data protection laws, data, and TBDF, data subject, data controller and data processor. Having defined the major concepts used in this paper, this chapter will proceed in highlight the major prevailing regulatory typologies governing TBDF in a digital economy as well as the corresponding regulatory framework from an international and regional perspective.

Data protection laws are rules that regulate the different stages in the processing of data and accordingly address the way in which data is gathered, registered, stored, exploited, and disseminated.[120] These laws are aimed at safeguarding the rights and interests of individuals in their role as data subjects when others process their data.[121] For a long time, the regulation of transborder data flows has been a feature of data protection law. Transborder data flow is becoming very important in research and policy. There is currently consensus on the most basic elements of the process. However, the definition of transborder data flow remains elusive.[122]

Data, according to the OECD, is a collection of unprocessed points which, once processed and analysed, becomes information.[123] The nature of data is that it is intangible and non-rival. This means that a lot of people can use data simultaneously.[124] TBDF are international communication. Although the term cross-border data flow is more common, the

[120] Naude, A and Papadoulos, S 'Data Protection in South Africa: The Protection of Personal Information Act 4 2013 in light of recent international Developments' (2016) 79 *THRHR*1-18 at 2.

[121] Ibid.

[122]UNCTAD op cit note 9 at 52.

[123]Ibid.

[124] Ibid.

term TBDF is used in this paper. The term 'transborder data flow' can be traced back to the OECD guidelines.[125] The terms TBDF and cross-border data flow are used interchangeably to indicate the same thing. The UNCTAD contends that, depending on the context, either term may be used to refer to "the electronic transfer of personal or non-personal data across national boundaries for processing or retaining in computer files."[126]

The OECD Guidelines define TBDF as the 'movement of personal data across national borders.'[127] The Council of Europe Convention defines TBDF as 'the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view of it being automatically processed'. [128] The Business Software Alliance[129] defines TBDF as 'a transfer of data between servers located in different countries.' In the modern world, the transmission of data over a national border can be done using several different mediums.[130] The information flowing over these networks is varied: banking and other financial data, corporate information relating to production and strategic planning, records relating to individuals, and information products (online databases, data banks, and full text systems) all move around the world in response to the demands and needs of other organisations and individuals.[131]

For the purposes of this dissertation, the definition provided by the Council of Europe is deemed more appropriate to the issues discussed herein, because it employs the words 'whatever medium' which reflects the true nature of transborder data flows. This is particularly important when it comes to TBDF over the internet, which challenges the efficacy

---

[125] Ibid.

[126] Ibid.

[127] Article 1 of the OECD Guidelines op cit note 39. See also Guynes, J.L., Guynes, S.C. & Thorn, R.G 'Conquering international boundaries that restrict the flow of data' (1990) 6 *Information Strategy: The Executive's Journal* 27-32 at 27.

[128] (CoE Convention, Article 12). See also Waples, E. & Norris, D.M 'Information systems and transborder data flow' (1992) 43 *Journal of Systems Management* at 28-30 at 28.

[129] Business Software Alliance 'Cross-border Data Flows' (2017) last accessed from *https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf* on 11 September 2022.

[130] UNCTAD op cit note 9 at 52.

[131] Gisela Moohan, Elizabeth Morton, Sally Rimmer, Giulio Romano & Paul F. Burton 'Transborder Data Flow: A Review of Issues and Policies' (2007) 37 *Library Review* 27-37 at 27.

of data protection laws. Normally, such data would be stored or reprocessed in a nation other than the one from which it originated.[132] Furthermore, data transmission can be done electronically and instantly via cables or satellite, or it can be done more slowly by physically transferring magnetic tapes, disks, cards, or other comparable medium.[133]

The terms data subject, data controller, and data processor are all defined in the Namibian Data Protection Bill. Section 1 of the Bill defines data subject as 'an identifiable natural person to whom the personal data relates.' The section goes on to define 'identifiable person' as:

> *'(a) 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 or her physical, physiological, mental, economic, cultural or social identity;*
>
> *(b) to determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person.'*

Additionally, section 1 also defines the term data controller, is defined as:

> *'any natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data. Where the purpose and means of processing are determined by or by virtue of an act, decree or ordinance, the controller is the natural person, legal person or public body that has been designated as such by or by virtue of that act, decree or ordinance;'*[134]

Whereas the term data processor is defined as data processor is defined as 'a person who processes personal data on behalf of the controller.'[135]

2. INTERNATIONAL AND REGIONAL REGULATORY FRAMEWORKS ON TRANSBORDER DATA FLOWS

[132] Article 12 of the Council of Europe Convention on the Automatic Processing of Data.

[133] Ibid.

[134] Section 1 of the Namibian Data Protection Bill.

[135] Ibid.

International jurisprudence on data protection law and the regulation of TBDF cannot be fully understood without an exposition of the origins of data protection law. The first data protection legislation was introduced in the German State of Hesse in 1970.[136] Sweden was the first country to introduce national data protection legislation in 1973, with Germany and France following suit in 1977 and 1978, respectively. [137] According to Greenleaf, during the last five decades since the adoption of data privacy legislation, various parts of the world have been the most agile 'boom zones' in the global dispersion of data privacy laws.[138] These laws are now found in 143 countries, with the EU being the world's strictest and most influential data protection regime.[139]

Outside of its territorial borders, Namibia is subject to certain data privacy obligations, which must be considered when evaluating all the factors influencing national data privacy law.[140] These international and regional initiatives are intended to increase interoperability between data protection regimes and to eliminate trade barriers.

2.1 International Instruments

International human rights law protects the right to privacy under various instruments such as the ICCPR and the UDHR. According to Kuner, international regulation on TBDF exists largely at the regional level, and there is no multinational instrument of truly global scope dealing with the subject.[141] However, there are two crucial international instruments on TBDF, namely: The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ('Convention 108') and the OECD Guidelines discussed earlier in chapter 1.

[136] Lynskey op cit note 2 at *46.*

[137] Kuner,C *Transborder Data Flows and Data Privacy Law* (2013) at 26.

[138] Greenleaf G & Cottier B 'Comparing African data privacy laws: International, African and regional commitments' (2020) 32 *UNSWLRS* 1-39 at 3.

[139] Ibid.

[140] Ibid at 11.

[141] Kuner op cit note 135 at 26.

2.1.1 *The ICCPR and other UN Instruments*

The UN has a long history of advocating the right to privacy through its human rights treaties; notably, through articles 12 and 17 of the UDHR and the ICCPR, respectively. Namibia is one of the African countries that have ratified the ICCPR.

General Comment No. 16 on Article 17 of the ICCPR states that every individual has the right to be protected against arbitrary or unlawful interference with his privacy, family, home, or correspondence, as well as unlawful attacks on his honour.[142] According to the Committee, this right must be protected against all such interferences and attacks, whether they originate from state authorities or private individuals. [143] The obligations imposed by this article require the State to adopt legislative and other measures to implement the prohibition of such interferences and attacks and to protect this right.[144] Regarding the protection of personal data and state party obligations, paragraph 10, states, among other things, that:[145]

> 'The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, *must be regulated by law*. Effective measures must be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process, and use it, and is never used for purposes incompatible with the Covenant.'

Additionally, during the years 2013-2015, the United Nations bolstered its privacy protection efforts with two high-profile initiatives. The first was the release of a 'Digital Rights statement'. The second initiative was the appointment of a Special Rapporteur on the right to privacy.

---

[142] UN Human Rights Committee (HRC) 'CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (1988) last accessed from h*ttps://www.refworld.org/docid/453883 f922.html* on 14 June 2022.

[143] Ibid par. 1.

[144] Ibid.

[145] Ibid par.10.

In December 2013, the UN General Assembly approved resolution 68/167 on the Right to Privacy in the Digital Age,[146] expressing concern about monitoring and interception of communications' repercussions on human rights. The General Assembly emphasised that offline rights must be safeguarded online and urged all states to preserve and defend digital privacy. The General Assembly urged all states to evaluate their surveillance, interception, and personal data collection methods, practices, and legislation. It urged governments to fulfill their human rights duties fully and effectively under international law.

Similarly, the UN also created a Special Rapporteur on privacy.[147] The UN Human Rights Council appoints a Special Rapporteur to investigate and report on a particular problem regarding privacy. The Special Rapporteur is mandated by Human Rights Council Resolution 28/16 to:

> 'a) examine trends, developments, and issues pertaining to the right to privacy and offer recommendations to guarantee its promotion and preservation. g) report on suspected breaches of the right to privacy, including surveillance, as stipulated in article 12 of the UDHR and article 17 of the ICCPR.'

2.1.2 Organisation for Economic Cooperation and Development Guidelines, 1980

The OECD was the first organisation to endorse privacy protection principles, by recognising both the need to facilitate TBDF as a foundation for economic and social development, and the risks associated with them. The OECD privacy framework was developed in 1980 and was updated in 2013 to modernise its approach.[148] The original framework is the first international agreement on how to best balance effective privacy protection with the free flow of personal data. The framework has served as a key reference for many national regulatory and self-regulatory instruments, as well as many national regimes. Details on these guidelines will be discussed in chapter 4.

[146]Last accessed from *https://digitallibrary.un.org/record/764407?ln=en* on 30 July 2022.

[147] Ibid.

[148] Last accessed from at *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf* on 17 March 2022.

2.1.3 Council of Europe Convention 108

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981) ('Convention 108'), building on the OECD's work, was signed by the Council of Europe member states in 1981. The signing was to reconcile the fundamental values of respect for privacy and the free flow of information between countries.[149] The Convention serves as the first example of a regional agreement that seeks to establish minimum data protection standards.[150] Being the world's only legally enforceable multilateral instrument on data protection, Convention 108 currently comprises 55 state parties, eight of which are non-European. [151]

In relation to TBDF, Convention 108 guarantees respect for the right to data protection of individuals, regardless of country or domicile. Article 12 of the Convention prevents parties from restricting TBDF based on privacy concerns unless the non-contracting state does not afford 'equivalent protection'. [152] The equivalence principle is a basic requirement for TBDF.[153] According to Lingjie Kong,[154] the rationale for such a principle is for all contracting states, having subscribed to the common core of data protection provisions set out in the Convention, to offer a certain minimum level of protection.[155]

2.1.4 Council of Europe Convention 108 +

Even though Convention 108 has a broad international character, the convention continues to be a living instrument, having been revised several times. A week before

---

[149] UNCTAD op cit note 9 at 163.

[150] See Details of Treaty No.108 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'(1981) last accessed from *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108* last accessed on 15 June 2022.

[151] Lee A. Bygrave 'The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospect' (2021) 40 *Computer Law and Security Review* 1-13 at 11. See also UNCTAD op cit note 9 at 184.

[152] Lingjie Kong 'Data Protection and Transborder Data Flow in the European and Global Context' (2010) 21 *The European Journal of International Law* 441-456 at 442.

[153] Ibid.

[154]Ibid.

[155] Ibid.

the GDPR went into effect on May 25, 2018, the Council of Europe completed the 'modernisation' of Convention 108 on 18 May, when the parties to the existing Convention agreed to a Protocol amending it.[156] The new version of the Convention is now being called '108+' to distinguish it. It is the mother of the GDPR.[157] In October 2018, countries could sign and ratify the Protocol (CETS No. 223) that amends Convention 108. Since then, many countries have ratified it.[158] The United Nations Special Rapporteur on the right to privacy has encouraged 'all United Nations Member States to ratify Convention 108+' citing the convention's 'distinctive ability to become the international framework on data protection.'[159]

The amending protocol streamlines two fundamental goals: cross-border data movement and data protection.[160] It is important to take note of the changes to the territorial scope of the new Convention 108+, which offers a wider range of application similar to Article 3(2) of the GDPR discussed earlier in the research.[161]

2.2 Regional Instruments

2.2.1 African Charter on Human and Peoples' Rights

Created in 1981, the African Charter on Human and Peoples' Rights ('ACHPR' or 'Banjul Charter') lays down minimal standards and freedoms for the promotion and protection of human rights in Africa.[162] It has been signed and ratified by all African states except South Sudan.[163] While modelled after comparable international or regional instruments, such as the ICCPR or the European Convention on Human Rights ('ECHR'), the ACHPR does not explicitly protect the right to privacy, or to private

[156] Graham Greenleaf 'Modernised Data Protection Convention 108+ and the GDPR' (2018) 154 *Privacy Laws & Business International Report* 1-3 at 1.

[157] Ibid.

[158] Ibid.

[159] Ibid at 185.

[160] Ibid.

[161] Ibid at 2.

[162] Greenleaf et al op cit note 136 at 17.

[163] Ibid.

life.[164]Various provisions stipulate, however, that human beings are sacrosanct, that their dignity is inherent, and that they should not be unjustly denied of their rights.[165] Nevertheless, the unfortunate and conspicuous absence of an explicit safeguard has been largely remedied by the African Charter on the Rights and Welfare of the Child, which expressly protects the privacy of kids (Article 10).[166]

2.2.2 Malabo Convention

In 2014, the African Union ('AU') passed the Convention on Cybersecurity and Personal Data Protection ('Malabo Convention').[167] It intends to regulate the collection and processing of personal data of AU member states. Signatories to the Convention agree to enhance the protection of personal data and to reveal privacy infringements 'without prejudice to the principle of free flow of personal data'.[168] Furthermore, it mandates every Member State to create an independent and autonomous data protection institution.[169]

The Convention also establishes detailed requirements for the collection and processing of personal data, such as subject consent, the legality of purpose and procedure, and openness.[170] It ensures the data subject has the right to information, access, objection, and erasure. Members of the African Union may join the Convention voluntarily, unlike the GDPR.[171] According to Greenleaf, fifteen signatories must ratify the Convention before it takes effect.[172] As of June 2020, the only countries that had

[164] Ibid.

[165] African Charter on Human and Peoples Rights (1981) last accessed from *http://www.achpr.org/instruments/achpr* on 11 July 2022.

[166]Greenleaf et al op cit note 136 at 17.

[167]Ibid at 12.

[168] Ibid at 13.

[169] See also *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection* on 28 March 2022.

[170] Greenleaf et al op cit note 136 at 17f.

[171] Ibid.

[172] Ibid.

ratified it were Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, and Senegal.[173]

2.2.3 SADC Uncitral Model on Data Protection

The Southern African Development Community (SADC) is comprised of 15 nations in southern and central Africa as well as the Indian Ocean. Seven of these nations have data protection laws (Angola, Lesotho, Madagascar, Mauritius, Seychelles, and South Africa and Zimbabwe only for their public sector), and four of which have current bills (Zambia, Tanzania, Swaziland, and Namibia).[174] Work on SADC-wide data protection laws and regulations has already begun with the help of the Telecommunications Union ('ITU'). The SADC Model Law on Data Protection is an initiative of the EU and the ITU Harmonisation of ICT Policies in Sub-Saharan Africa ('HIPSSA').[175] According to the ITU, the HIPSSA initiative was launched to aid African regional economic communities ('RECs') and regional regulatory authorities in sub-Saharan Africa in unifying ICT policies and laws.[176]

2.3 Conclusion

As it has been noted in the section, data protection is closely tied to one of our basic human rights, the right to privacy. The notion of data protection arose in the 1970s in response to fears that the exponential surge in personal data processing might compromise privacy rights. In recent decades, it's been generally recognised that regulating the use of personal data is essential to privacy. Despite the global significance of the problem, there are no globally mandated standards at the UN level. The OECD principle(non-binding) and Convention 108 (binding) are two important international instruments on TBDF.

In addition, this section covered Namibia's international data privacy obligations, which impact national legislation. The international human rights

[173] Ibid.

[174] Ibid at 23.

[175] Ibid.

[176] Last accessed from *https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx o*n 13 September 2022.

agreements referenced in this section, like the ICCPR, require governments to take adequate steps to guarantee that personal data does not come into the hands of people not authorised by law to receive, handle, or use it. It has also outlined the requirements for managing and handling personal data in OECD Guidelines and Convention 108's (and its amending protocol). These two instruments have influenced global lawmaking. To date, OECD Guidelines have been implemented in non-OECD nations.[177] Convention 108's neutral, principle-based approach attracted over 30 countries. Moreover, forty countries have accepted Convention 108+'s amending protocol as of January 2022.[178] Both instruments say and don't say much. Chapters 4 and 5 cover these instruments in greater detail.

In the next section, I analyse the major regulatory typologies of TBDF by the world's three largest economies: the European Union (EU), the United States of America ('US'), and China. Adopting one of the three key regulatory frameworks for the regulation of TBDF will bring any country closer to a regulated data privacy regime.

3.REGULATORY OBJECTIVES: A TYPOLOGY OF REGULATORY APROACHES USED BY THE WORLD'S LEADING ECONOMIES

The United Nations Conference on Trade and Development ('UNCTAD') 2021 Digital Economy report is used as an authoritative and leading source in this section. This is because it is customary for the UNCTAD to always take developing countries' viewpoints, which in this case, Namibia can draw some positive lessons from.[179] Notably, the work of other renowned academics and data protection specialists, such as Kuner[180], Schwartz[181], Bennet[182],

[177] Ibid.

[178] Ibid.

[179] UNCTAD op cit note 9.

[180] Kuner op cit note 135.

[181] Paul M. Schwartz and Karl-Nikolaus Peifer 'Transatlantic Data Privacy Law' (2017) 106 *The Georgetown Law Journal* 123–27.

[182] Steven Bennett 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 *Berkeley Journal of International Law* 161-195.

Voss[183], etc., has been used to expand on the UNCTAD research and provide a more complete picture of the various regulatory typologies.

As part of its ongoing obligations, UNCTAD assists developing nations in participating more fairly and equitably in the global economy. It convenes panels to debate issues such as Africa's developmental challenges and the digital economy, among many. According to the UNCTAD report,[184] past structural injustices against poor nations are being translated; their views are marginalised in international talks, and their data is being abused without sufficient oversight. Data-driven digital technologies will have a disproportionately negative impact on these labour-intensive countries.[185]

As noted earlier in this chapter, TBDF has become a critical component of international trade and digital services. Although data-related legislation has recently received growing attention from policymakers, academics, and the international press, it has been around for some time.[186] To begin, this paper places its discussion of TBDF regulation in the wider economic and geopolitical framework by laying out the various regulatory typologies that countries have for regulating transborder data flows.[187] According to the UNCTAD, key economic and geopolitical actors in the digital economy have varying ways of managing TBDFs.[188] Widespread discord and anomalies characterise the regulations of TBDFs and the digital economy at global, regional, and national levels.[189]

Much has been stated about the need for an international, interoperable internet that can reach global audiences, link digital global value chains, and access huge international markets. [190] To encourage economic progress while protecting individuals' privacy, law makers must shape domestic legislation. A balanced approach to data protection is generally

[183] W. Gregory Voss 'Obstacles to Transatlantic Harmonisation of Data Privacy Law in Context' (2019) 2 *Journal of Law* 405-463.

[184]UNCTAD op cit note 9 at 175.

[185] Ibid.

[186] Ibid.

[187] Ibid

[188]Ibid at xviii.

[189] Ibid.

[190] Ibid at 100.

advocated.[191] According to UNCTAD, the ultimate model adopted at the national and international levels will impact not just trade, innovation, and economic development but also a variety of concerns pertaining to the division of digitalisation's benefits, human rights, law enforcement, and national security.[192] Countries have a variety of regulatory goals for regulating TBDFs, including the protection of privacy and other human rights, national security, and economic growth.[193]

UNCTAD has also acknowledged that, in the absence of a competent international structure to govern these flows, nations have little choice but to limit data transfers as they see fit.[194] Academics like Gisela Moohan, Elizabeth Morton, Sally Rimmer, Giulio Romano, and Paul F. Burton all argue that, ideally, restrictions on TBDF should be flexible enough not to impede the normal conduct of business.[195] Moreover, legislation should be clearly expressed, otherwise it is subject to interpretation by administrators.[196] Equally, the cost of compliance with legal requirements should not be disproportionate to the benefits such legislation produces, and it is necessary that countries make clear their stance on data protection/privacy as soon as possible.[197]

Namibia must assess the domestic benefits and risks associated with TBDF at both the societal and individual levels. A regulatory framework should ideally be designed in such a way that it can effectively protect its citizens' data while allowing data to cross borders in a way that promotes trade and innovation. The following consideration should be considered in choosing an approach for the regulation of TBDF, namely:

- To safeguard the right to privacy;
- To mitigate the risk of unethical and malicious use of personal data;
- To increase trust in the digital economy and reduce uncertainty;
- To minimise the negative externalities;

[191] Ibid.

[192] Ibid at 99.

[193] Ibid.

[194] Ibid.

[195] Gisela Moohan et al op cit 131 at 27ff.

[196] Ibid.

[197] Ibid.

- To allow digital transformation to take place;
- To make it easier to capitalise on opportunities created by TBDF;
- To consider the strategic economic role of data.

With that said, ultimately, any country wishing to move closer to a regulated data privacy regime should engage the three major regulatory models on the regulation of trans-border data flows developed by the world's largest and most powerful economies.[198] Regulations on TBDF are based on various regulatory objectives, including those related to the protection of privacy and other human rights, law enforcement, and national security; as well as economic development objectives.[199] Countries employ a variety of legal and regulatory tools to achieve this. Determining which structure is optimal for controlling data flows internationally remains an onerous task.[200] This section looks at the various rationales for regulating TBDF in the world's leading economies.

Worldwide, three main governance approaches are of influence, namely that of the United States of America ('US') (a market-orientated/laissez-faire approach), China (a complex mixture of security-orientated and digital development approach), and the EU (a right-orientated approach).[201] This section outlines the key regulatory models on TBDF. To begin, the geopolitics of these regulatory approaches differ considerably. Each is guided by the needs and circumstances specific to them. Therefore, it is crucial to outline the differences and nuances that exist between them. The purpose of this section is to outline the broader framework of major approaches, noting disparities that may lead to bottleneck issues of compatibility or interoperability or raise fears about the fragmentation of the online realm at the global level.[202] Ultimately, bottleneck issues may have an impact on developing nations.

3.1 The United States Market-Oriented Model

The US model, albeit simplified, relies on private-sector data control with no geographic transfer restrictions on TBDF except concerning storing some

[198] Ibid.

[199] Kuner op cit note 135 at *3*.

[200] UNCTAD op cit note 9 at xviii.

[201] Ibid.

[202] Ibid.

governmental records.[203] The legal scholar Steven Bennett emphasises that US privacy law has largely developed in a patchwork with a reactive array of state and federal statutes and common law doctrines.[204]

In comparison to the EU model, there is no federal law covering all aspects of data privacy in the US. Instead, relevant provisions are strewn about in a plethora of laws governing various topics and industries.[205] According to Franz-Stefan Gady, the United States relies on a patchwork approach-sectoral laws combined with industry self-regulation.[206] They often have fewer limitations and offer less protection than the EU. Because of this light-touch approach, all data, including personal data, can travel freely across borders with few regulatory constraints (if any). The United States' regulatory approach to TBDF is motivated by a desire to maintain its leadership in the global digital economy while also expanding into new areas.The US largely relies on industry self-regulation in the field of data privacy protection, which provides companies with wide leeway in their usage of personal data to test new business practices, possibly resulting in privacy violations.[207] This has resulted in a 'positive feedback loop', which means that the more data that US companies can collect, the better for their data products and, as a result, the greater their ability to succeed in global markets.[208] The US self-regulatory nature of TBDF outside of sectoral law provisions is reflected in what is known as laissez-faire ideology.[209] The notion of laissez-faire is 'an ideology resisting governmental intervention in economic activities above the minimum required for the protection of peace and property rights'.[210]

---

[203] UNCTAD Digital Report op cit note 8. The United States has enacted strong data localisation laws for defense-related data, mandating that any firm providing cloud services to the Department of defense keep its data solely in the United States.

[204] Steven Bennett op cit note 180 at 169.

[205] Emmanuel Pernot-Leplay 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U' (2020) 8 *Penn State Journal of Law and International Affairs* 49-67 at 53.

[206] Franz-Stefan Gady op cit note 203 at 15.

[207] Franz-Stefan Gady 'EU/U.S. Approaches to Data Privacy and the "Brussels Effect": A Comparative Analysis' (2014) 4 *Georgetown Journal of International Affairs* 12-23 at 13.

[208] Ibid.

[209] Voss op cit note 181 at 435.

[210] Ibid.

A comprehensive data protection system has long been opposed in the United States due to political opposition to a strategy that would impose greater governmental control on market participants.[211] Congress and the U.S. government did not desire to enact an omnibus EU-style privacy law. Indeed, at the time, top US technology corporations were fiercely opposed to such a rule. It was assumed that government regulation of privacy would eventually hamper the expansion of the digital marketplace.[212] In 1997, a vice president of American Express stated, 'We feel that government control of privacy on the Internet and other online domains is extremely dangerous, given the fast evolution of new technology'.[213] This position was embraced by the Clinton administration, which endorsed industry self-regulation.[214]

According to Voss, critics deem this regulatory approach a failure owing to a lack of accountability and transparency, incomplete fulfillment of strong privacy requirements; incomplete fulfillment of strong privacy requirements free-rider issues, and insufficient monitoring and enforcement, all of which are designed to avoid government regulation.[215] Self-regulation is when companies take on government regulatory functions, resulting in a lack of government accountability and no conflict resolution mechanism in cases of breaches, among others.[216] An example is the Equifax[217] and Uber[218] data breaches, which affected a total of 200 million people in

[211] Global Digital Partner op cit note 4 at 21.

[212] Gregory Shaffer op cit note 11 at 44.

[213] Ibid.

[214] Voss op cit note 181 at 435.

[215] Ibid.

[216] Ibid.

[217] Ibid. Equifax, the third largest credit bureau in the United States, announced a data breach in July 2017 that compromised the data of 143 million data subjects. See Ping Wang & Robert Morris 'Cybersecurity Incident Handling: A Case Study of the Equifax Data Breach' (2018)19 *Issues in Information Systems* 150-159 at 156.

[218] In October 2016, Uber hid a significant global data breach that affected 57 million users and drivers. See JM Robbins & AM Sechooler - Once More unto the Breach: What the Equifax and Uber Data Breaches Reveal about the Intersection of Information Security and the Enforcement of Securities Laws' (2018)4 *Criminal Justice* 4-7 at 4f.

2017. [219] Despite the surge in data breaches in the US, the legal system has not adapted to safeguard consumers. [220]

Perhaps instinctively, commercial interests have supported this self-regulation as noted above. [221] Data Protection Law experts Professors, Schwartz and Peifer contend that in the United States, some view EU data protection as a kind of trade protectionism or as the product of misdirected envy of successful US Internet firms.[222] President Barack Obama's assessment of European investigations into Facebook and Google was as follows: 'oftentimes, what is portrayed as high-minded positions on problems is just geared to advance their business interests' (sic).[223] In addition, there is a belief in the United States that its approach to data protection is significantly more innovative than that of the European Union, which is perceived to have stifling regulations for digital companies.[224] In spite of this, at a global level this self-regulatory system has been widely criticized since government representatives of the people and data subjects remain absent. Consequently, many scholars throughout the world currently believe that this self-regulation has failed.[225]

3.2 The Chinese National and Public Security Model

The Chinese approach stresses government control over data.[226] Effective as of 2017, China's Cybersecurity Law prohibits the transmission of personally identifiable data and 'important' data internationally for operators of 'critical information infrastructures' (albeit with limited exemptions).[227] In contrast to the US model, which

[219] Gregory Gaglione 'The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America' (2019) 67 *Buffalo Law Review* 1133-1212 at 1133.

[220] Ibid at 1134.

[221] Voss op cit note 181 at 435f.

[222] Paul M.Schwartz et al op cit note 179 at 157.

[223] Ibid at 158.

[224] UNCTAD op cit note 9 at 102f.

[225]Ibid.

[226] Ibid.

[227] Chander A & Ferracane M 'Regulating Cross-border Data Flows – Domestic Good Practices. In: Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic

prioritizes private sector data control, China's approach prioritizes data control primarily by the government.[228] Such a draconian regulatory approach entails a full or partial prohibition on TBDF on grounds of public safety, national security, and strict political control over the local Web.[229]

It has been argued that such data localisation can cause inefficiencies and is likely to have a negative economic impact.[230] Economies stand to reap multiple benefits if they act on creating an open, competitive marketplace for trans-border ICT services by removing several barriers like data localisation.[231] However, if data localisation becomes the de facto solution to the absence of internationally interoperable privacy regimes, then many of the benefits of the global internet and the increased trade it brings will be at risk.[232]

3.3 The European Union's Rights-Based Model

The EU encourages individual data control.[233] It advocates a strict regulatory approach to the data-driven digital economy based on EU basic rights and values. [234] It's human-centric since it emphasises protecting individual privacy.[235] It falls in the middle of the regulatory spectrum and typically comprises conditional transfer requirements. The EU seeks to construct a unified digital market where digital goods and data can flow freely under a set of laws. These laws are meant to safeguard people, corporations, and governments from abuse arising from data collection, processing, and commercialisation. [236]

Interdependence' (2019) last accessed from *http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf. on 30 August 2022.*

[228] UNCTAD op cit note 9 at 102.

[229] Ibid.

[230] Ibid.

[231] Chander op cit note 223 at 19.

[232] Ibid.

[233] Ibid at 102 ff.

[234] Ibid.

[235] Ibid.

[236] Ibid.

3.4 Recommendations for an EU Model: The Allure of the Middle Ground?

According to Gisela Moonhan and others, the idea of an unrestricted flow of data across national borders is a complex one that involves balancing the interests of individuals, corporations, and nations.[237] It is important to note that not all the regulatory systems and mechanisms recognize data protection as fundamental right.[238] For example, the fundamental goals of both the US and Chinese models are to achieve economic growth while maintaining security constraints. [239] The EU's core aim is to prioritise fundamental rights to data privacy. Essentially, this right-based terminology fosters the link between data subjects and the EU institutions that defend their rights.[240]

For instance, the GDPR is designed to safeguard the fundamental right to data protection while allowing for the free movement of data throughout the EU. In contrast, US law protects the individual as a privacy consumer.[241] In the US, a person is depicted as a player in market transactions. Within this market-based framework, the person is a seller of a commodity: her personal data.[242] The United States lacks a basic right to data protection comparable to that of the EU.[243] In a nutshell, the former promotes security and economic development, while the latter advocates for people's basic liberties.

The preceding sections have outlined the major TBDF regulatory typologies undertaken by the world's leading economies, which have served as key reference points for a more focused discussion of the Namibian's data protection law. In the following section, I will explain which model is recommended for Namibia and why. This section will argue that lax data protection measures put the right to privacy

[237] Gisela Moohan et al op cit note 131 at 36.

[238] Monika Zalnieriute 'Transborder Data Flows and Data Privacy Law' (2014) 30 *Computer Law & Security Review* 104–108 at 105.

[239] Ibid.

[240] Paul M. Schwartz et al op cit note 179 at 121.

[241] Ibid.

[242] Ibid.

[243] Ibid.

and other rights at risk. In addition, lax data protection regimes allow for the establishment of 'data havens' where personal data can be stored without protection, particularly if data exports are not regulated at all.

As noted above, the concept of data protection emerged in the 1960s in response to worries that the rapid expansion in the processing of personal data could lead to abuses of the right to privacy of persons. According to Global Digital Partner, there are four important factors that determine whether a country has a human rights framework that respects human rights:[244]

> *"1) the existence of a data protection law;*
> *2) the incorporation of internationally agreed minimum data protection standards in the law;*
> *3) the extent of the coverage of the data protection law; and*
> *4) the existence of an enforcement, or regulatory, authority."*[245]

The Digital Global Partner goes on to rightfully argue that only if a country has all four elements in place can it be deemed to be human rights-respecting.[246] Below, elements one and three are considered applicable to a discussion on TBDF, in the form of key guiding questions, which have been applied in a comparative fashion. At the onset, it is essential to note that the European model is preferred for Namibia for three reasons: (1) it is comprehensive (2) human-rights respecting and (3) technologically neutral.

To put the above mentioned in context, first, I argue that the European model is preferred because of its omnibus legislative approach, which encompasses both the public and private sectors.[247] As we saw in the preceding part, a data protection model may either be comprehensive like the EU model, meaning the regulation applies

[244]Global Digital op cit note 4 at 52.

[245]Ibid.

[246] Lucas Bergkamp 'EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' (2002) 18 *Computer Law & Security* 31-47 at 31.

[247]Toriqul Islam Md et al op cit note 6 at 538. See also Paul Schwartz 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* 771-818 at 771ff.

to both the commercial and public sectors, or it can be sectoral, meaning that only certain sectors are regulated like the US model.[248]

It is submitted that the EU model is in alignment with the right to privacy enshrined in Article 17 of the ICCPR, which draws no distinction between impacts on privacy caused by the public sector, private sector, or other actors.[249] Thus, the Human Rights Committee's General Comment on the right to privacy makes it quite clear that such data protection laws must apply to all personal data, whether collected, kept, or utilised by public authorities or private people or organisations.[250] According to Jamison, patchwork data protection laws make compliance difficult, costly, and arguably improbable for interstate and international businesses.

Second, the European Union, emphasises individual data control.[251] Consequently, it proposes a robust and strict regulatory approach to the data-driven digital economy, based on the preservation of the European Union's basic rights and values to privacy and to data protection. This is considered a human rights-centric approach since it lays a high focus on protecting individual privacy.[252] Worth noting is the fact that the Charter of Fundamental Rights is viewed as a crucial constitutional document inside the EU, which explicitly guarantees the right to data protection in article 8.[253] This sets the EU Charter apart from other international human rights documents, as it will be seen in chapter 5 of this dissertation.[254]

Lastly, the EU's approach is preferred for Namibia because not only does it emphasise the inalienable right to privacy, but it also allows for data to flow across national borders in a controlled environment. This is the technological neutral argument I have brought forth. The EU law safeguards not only privacy and data protection, but

[248] Global Digital Partners op cit note 4 at 58.

[249] Ibid. See also *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/USA/INT* on 12 July 2022.

[250] Ibid.

[251] Ibid.

[252] Ibid.

[253] Paul M. Schwartz et al op cit note 179 at 125.

[254] Ibid.

also the free flow of information. [255] Rightfully so, the EU model has earned itself a noble title as the world's golden standard for data protection and the regulation of TBDF. Accordingly, followed worldwide.[256] More recently, the UN Special Rapporteur on 'the right to privacy', for example, remarked that:[257]

> '[T]he protection of personal information online should be a priority with the adoption of provisions equivalent or superior to the GDPR, for those countries that are not parties to the Regulation.'

For the reasons mentioned above, the EU's approach is deemed comprehensive[258], human rights-centric[259], technology neutral, and holistic. It does not permit companies to profit from tracking, analysing, and quantifying every 'consumer' without accountability in cases of breaches, and it does not permit authoritarian or democratic states to build 'surveillance societies'.[260] Moreover, the European approach does not allow for a blanket prohibition (absolute political control over the internet) of TBDF under the disguise of public security, national security.

From a Namibian viewpoint, there was widespread violation of rights safeguarding information in Namibia pre-independence. However, most obnoxious laws have since been repealed. The political, social, and economic underpinnings of the apartheid government in Namibia were an institutionalised violation of fundamental human rights, such as the right to privacy. Systemic and deliberate denial of fundamental human rights, therefore, was the basis of apartheid. Consequently, respect for the fundamental human rights enshrined in the Namibian Constitution has been prioritised in the aftermath of colonial domination and apartheid. As Mohammed AJ held in the case of *S v Acheson:*[261]

---

[255] Ibid at 130.

[256] Ibid at 536.

[257] Ibid. See also Cannataci J 'Report of the Special Rapporteur on the Right to Privacy' (2019) last accessed from *https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur* on 12 July 2022.

[258] Lucas Bergkamp op cit note 244 at 31.

[259] Ibid.

[260] Lyon, D *Surveillance Society: Monitoring Everyday Life* (2001) at 27.

[261] *S v Acheson 1991 NR 1 (HC)*

> ‘The Namibian Constitution of a nation is not simply a statute which mechanically defines the structures of government and the relations between the government and the governed, it is a 'mirror reflecting the national soul', the identification of the ideals and aspirations of a nation; the articulation of the values bonding its people and disciplining its government.’

The balanced approach preferred is one that prioritises fundamental human rights, considering Namibia's apartheid history on the one hand, while also taking into cognisance the economic imperatives of transborder data flow from a developing country’s perspective on the other hand. Moreover, one of the primary tenets derived from the ‘fundamental rights’ notion is that privacy should be inalienable and non-negotiable.[262] In other words, the law should prohibit a person from voluntarily relinquishing some or all of his private rights. Similarly, states have a positive obligation to enact laws that safeguard the right to privacy. Consequently, any regulation that allows privacy to be jeopardised or compromised in the name of economic progress or national security violates this fundamental principle of human rights. To this end, the current author is mindful of the opening statements to the preamble of the Namibian constitution that state:

> ‘Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is indispensable for freedom, justice, and peace.’[263]

3.5 Final Remarks

In conclusion, this section has detailed several provisions and initiatives recently undertaken in the world’s leading economies, which provide important points of reference for a more focused discussion of Namibian data-related and TBDF legislation. It has been noted that the motivations behind emerging data protection laws in a globalised economy are manifold but can be grouped into three non-exhaustive categories: human rights, economical, and national security. Access to the global digital market means enabling seamless trade and e-commerce across borders, geographies, and jurisdictions. Therefore, it is imperative that lawmakers

[262] Lucas Bergkamp op cit note 244 at 34.

[263] Constitution of the Republic of Namibia last accessed from *https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf* on 15 June 2022.

mould their domestic laws in a way that facilitates economic growth whilst offering enough protection to citizens' rights to privacy.

This section has noted that the United States and the European Union have traditionally held widely differing views on data privacy.[264] While the US was adopting sectoral data privacy laws, the European Union turned to omnibus legislation, instead.[265] It does not come as a surprise that the US's technology sector has been exceptionally successful in developing data-driven products and services that have successfully infiltrated the majority of the world's markets.[266] However, as indicated in this section, this piecemeal approach is becoming increasingly problematic in a world where information technology is quickly expanding and touching numerous areas of privacy legislation.[267] Moreover, the reactive, adaptive process taken by the US courts makes it difficult to rationally or efficiently address digital privacy issues.[268]

Similarly, the European approach does not permit a blanket ban (total political control over the internet) on TBDF under the pretext of national security. On the contrary, it allows for data to cross borders in a well-controlled environment. Given that Namibia is a developing nation, data localisation is likely to result in inefficiencies and negative economic effects.

This section has concluded that the European model is recommended for Namibia due to its holistic nature for three reasons: (1) it is comprehensive, (2) it respects human rights, and (3) it is technologically neutral.

---

[264] Avner Levin & Mary Jo Nicholson 'Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground' (2005) 2 *University of Ottawa Law & technology journal* 357-395 at 357.

[265] W. Voss et al op cit note 181 at 420. Voss defines an Omnibus data privacy legislation as: 'one statute typically regulates the processing of personal information in public and private sectors alike. In the absence of more specific legislation, the general information privacy law in Europe sets the initial terms for the processing, storage, and transfer of personal information. The omnibus law is often accompanied, moreover, by more specific privacy laws.' See also Shaun G. Jamison, 'Creating a National Data Privacy Law for the United States' (2019)10 *Cybaris Intellectual Property Law Review* 1-41 at 1.

[266] UNCTAD op cit note 9 at 100.

[267] Levin et al op cit note 160 at 361.

[268] Ibid at 362.

4.CONCLUSION

The chapter began by describing and defining data and TBDFs. It situates the right to privacy and, in turn, data protection in international human rights law by means of a comprehensive examination of the regulatory frameworks from an international and regional backdrop.The chapter then highlighted the predominant regulatory typologies for regulating TBDF in a digital economy. In exploring this topic, this chapter has analysed the respective legal identities constructed around data privacy and the regulation of TBDF by the world's leading economies. This was accomplished by comparing the legislative approaches of the United States, China, and the EU. The chapter has identified major and profound differences in the three regulatory regimes. This chapter argued that the EU's balanced approach is preferable. The approach protects individual privacy rights while also promoting economic progress.

Furthermore, it has been argued that lax data protection measures put the right to privacy and other rights at risk. Lax data protection regimes allow for the establishment of 'data havens' where personal data can be stored without protection, particularly if data exports are not regulated at all. The chapter has emphasised that ultimately, regulatory models chosen at the national level will affect not only trade, innovation, and economic development, as well as the distribution of digitalisation's benefits, human rights, and law enforcement. The following section will critically analyse data protection and TBDF in the Namibian context.

CHAPTER 3

Data Protection in Namibia

---

1. INTRODUCTION

As social media platforms increase, more Namibians live online. Facebook, Snapchat, Twitter, WhatsApp, and Google can access users' contacts, photos, location, audio, and videos. Similarly, many customers utilise websites that monitor their surfing behaviour to catalogue their interests and demands. While these functions may seem innocuous, mobile apps and websites capture, process, and share users' personal data behind the scenes. Additionally, data breaches and cybercrimes are widespread in Namibia, yet data subjects remain with little to no recourse.

As this chapter will show, Namibia has no data protection legislation, other than a small section on data subject rights and protection in the Credit Bureau Regulations General Notice No. 5518 of 2014. Apart from the constitutional right to privacy, there are no restrictions on data collection or sharing at the national or international levels. However, since individuals and corporations worldwide started digitising their daily lives, data collection, processing, and sharing have become hot topics. As noted in chapter 1, the Namibian constitution recognises the right to privacy. Privacy is an important component of one's personality. Protecting personal data and controlling TBDF is vital for an individual's right to privacy. It protects a person's personal data while it's being collected, kept, utilised, or shared abroad.

A person's right to privacy includes having control over personal information and being able to conduct personal affairs without intrusion. Throughout Namibia, governmental and commercial entities have easy access to personal data due to a lack of regulation. Personal data may be distributed and abused internationally without safeguards. In Chapter 1, it has been noted that data protection is such an important aspect of the right to privacy. Chapter 2 noted how lax data protection standards can jeopardise the right to privacy and other rights. To this end, to comprehensively analyse the rights to privacy, data protection, and the regulation of TBDF in Namibia, it is necessary to look at the scope of the right to privacy under common law and the Namibian Constitution.

This chapter first provides a general introduction and historical background to Namibian law's provision for the right to privacy by tracing the right to privacy from Roman-

Dutch law times through colonial occupation to the present-day constitutional right to privacy. Here, the chapter provides some highlights on how the development of the common law and the constitutional right to privacy inform the current Data Protection Bill. Secondly, the chapter critically analyses the draft Data Protection Bill and the provisions relating to the control of transborder data flows. In part, this analysis traces the influence that the African regional data privacy instruments and the RECs, in particular, SADC, have on Namibia as well as the EU DPD of 1995.

2. DATA PROTECTION: A HUMAN RIGHTS ISSUE

In Chapter 1, I have noted that data protection is inextricably linked to one of our fundamental human rights, the right to privacy, as enshrined in Namibia's constitution, article 13. According to experts, it is linked to other human rights such as freedom of expression and non-discrimination.[269] Data protection laws were created in the first place to address the challenges and risks that increased processing of personal data posed to the right to privacy. Technically speaking, the data user/responsible party's processing of information endangers personality in two ways:[270]

> *'a) First, compiling and disseminating personal information poses a direct threat to the individual's privacy;*
> *b) second, acquiring and disclosing inaccurate or misleading information may result in his identity being stolen.'*[271]

In some jurisdictions, such as the EU, progress has been made toward the recognition of data protection as a distinct and separate human right, as will be seen in chapter 5. The foundation of European data protection law is the notion that people should oversee their own personal information.[272] This control has been termed as 'informational self-determination'. Information privacy was defined by Westin in 1968 as the right to select what personal

---

[269] Global Digital Partners op cit note 4 at 27.

[270] South African Law Reform Discussion Issue Paper No 109 (Project 124) *Privacy and Data Protection* (2005) par. 1.2.3.

[271] Ibid.

[272] Florent Thouvenin 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021)12 *JIPITEC* 246-256 at 246.

information about me is known to whom.[273] Borrowing from the work of Jan Henrik Ziegeldorf and others on privacy and the IoT, this dissertation adopts the definition of privacy, which captures in essence the idea of informational self-determination by enabling the subject to:[274]

'(i) to assess his personal privacy risks,

(ii) to take appropriate action to protect his privacy, and

(iii) to be assured that it is enforced beyond his immediate control sphere.'

Similarly, the 2012 Association of Southeast Asian Nations ('ASEAN') Human Rights Declaration also makes specific reference to data protection in Article 21, noting that 'every person has the right to be free from arbitrary interference with his or her privacy, family, home, or correspondence, including personal data.'[275] Be that as it may, whether data protection is considered a component of the right to privacy or a separate human right, strong and effective data protection contributes to the protection of other human rights as well. In this chapter, I examine why data protection is such an important aspect of the right to privacy, as well as its content and its place in the Namibian system.

3. THE DEVELOPMENT OF THE RIGHT TO PRIVACY IN NAMIBIA

The recognition of the right to privacy is deeply rooted in history. Namibia was declared a German Protectorate in 1884 and a Crown Colony in 1890, and thereafter became known as South West Africa.[276] The territory remained a German colony from 1884 until 1915, when it was occupied by South African forces. From 1920 onwards, the territory became a Protectorate,

---

[273] Jan Henrik Ziegeldorf, Oscar Garcia Morchon & Klaus Wehrle 'Privacy in the Internet of Things: threats and challenges' (2014)7 *Security Comm. Networks* 2728-2742 at 2729. See also this definition adopted by Paul M. Schwartz 'Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology' (2011)15 *William and Mary Law Review* 351- 387at 368; Kenneth A Bamberger & Deirdre K Mulligan 'Privacy in Europe: Initial Data on Governance Choices and Corporate Practices' (2013)85 *The George Washington Law Review* 1529-1664 at 1539.

[274] Ibid.

[275] Last accessed from *https://asean.org/wp-content/uploads/2021/01/6_AHRD_Booklet.pdf* last accessed on 08 June 2022.

[276] Sam K Amoo & Isabella Skeffers *'The Rule of Law in Namibia'* (2006) last accessed from *https://www.kas.de/c/document_library/ on 27 June 2021.*

or a Mandated Territory of South Africa in terms of the Peace Treaty of Versailles.[277] South Africa was granted the mandate over Namibia by the League of Nations, it also assumed legislative powers over Namibia.[278]

Namibia achieved its independence in 1990 after a long and protracted struggle, on both diplomatic and military fronts, for the achievement of self-determination and sovereignty. Because Namibia and South Africa share the same legal heritage, Namibian privacy law is substantially identical to previous South African law. To prevent the creation of a legal vacuum on the eve of independence, Article 140 of the Constitution provides, inter alia, that all laws which were in force immediately before independence shall remain in force.

Furthermore, in terms of Article 131 of the Constitution, the rights and freedoms contained in Chapter 3 are entrenched (this includes the right to privacy), and the provisions may not be repealed or amended insofar as such repeal or amendment detracts or diminishes from such rights and freedoms. The Namibian legal system is characterised by legal pluralism.[279] It is an amalgamation of Westminster-style constitutional law, Roman-Dutch common law, customary law, and international law.[280] This research refers to informational privacy, which is related to the right to determine when, how, and to what extent information about an individual is communicated to others. It is generally accepted that data processing of individual personal information poses a threat to the individual's right to privacy. Neethling defines privacy as:

> *'.... An individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.'*

[277] Ibid.

[278] Administration of Justice Proclamation 21 of 1919.

[279] Geraldine Mwanza Geraldo and Isabella Skeffers *'Researching Namibian Law and the Legal System'* last accessed from *https://www.nyulawglobal.org/globalex/Namibia.html* on 28 June 2021.

[280] Ibid.

Roos extends this description of privacy provided by Neethling and states:[281]

> *'In other words, the essence of an individual's interest in privacy is his or her power of self-determination over the scope of the information to be excluded from the knowledge of others. Therefore, a person's right to privacy implies that he or she should have control over his or her personal information.'*

The legal protection of privacy in Namibia is drawn from several sources, including common law (typically under delict law), the Namibian Constitution, and legislation. The following is a discussion of Namibia's sources of privacy.

3.1 Common Law

The introduction of Roman-Dutch law as the common law of Namibia is closely interrelated to the political and historical development of Namibia.[282] The Roman-Dutch law was formally introduced as the common law of Namibia (previously known as South West Africa) by Proclamation 21 of 1919, which provided, inter alia, that the Roman-Dutch law was to be applied in the territory as existing and applied in the Province of the Cape of Good Hope, and the proclamation remained the legal basis for the application of the common law.[283] In addition to this, Article 66 of the Namibian Constitution stipulates that the common law of Namibia in force on the date of independence shall remain valid to the extent to which such common law does not conflict with the constitution.

The origin of the right to privacy in Namibia can be traced back to the Roman-Dutch law delictual action, *actio inuriarium*. Separate personality rights are recognised and protected under Roman-Dutch law, including the rights to corpus (physical-mental integrity), *libertas* (physical freedom) and *fama* (reputation), as well as the rights relating to dignitas, which is regarded as a collective term for all other personality rights, inter alia, the rights to dignity, privacy, and, to a lesser extent, feelings and identity.[284] The concept of *dignitas* serves as a basis for the recognition of further rights of personality, and the extension of personality

---

[281] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007)124 *SALJ* 421 – 422.

[282] SK Amoo op cit note 274 at 60.

[283] Ibid.

[284] Hercules Booysen 'Succession to Delictual Liability: Namibian Precedent' (1991)*24 The Comparative and International Law Journal of Southern Africa* 204-214 at 205.

protection in so far as this may be necessary.[285] Under common law, the elements of an infringement of privacy that must be alleged and proven by a plaintiff include:[286]

(a) An invasion of privacy;

(b) wrongfulness; and

(c) fault in the form of intention or negligence.

3.2 The Namibian Constitution

The Namibian Constitution is a product of a struggle for sovereignty and human rights.[287] This is reflected in the first provision, which states that Namibia is a sovereign, secular, democratic and unitary state founded upon the principles of democracy, the rule of law, and justice for all. Namibia places an enormous premium on the protection of people's fundamental rights, including the right to privacy, which is derived from common law. This is a legacy of democracy and a universal characteristic of all democratic nations.

The protection and respect for people's privacy constitutes a fundamental value ingrained in the *grundnorms* of all democratic societies.[288] It is central to the protection of human dignity and forms the basis of any democratic society. The drafters of the Namibian constitution undoubtedly believed that the recognition of inherent dignity and equal inalienable rights of all members of the human family was indispensable for freedom, justice, and peace in an independent Namibia.[289] The Constitution of the Republic of Namibia guarantees the protection and respect of the rights to privacy under Article 13, which states that:

> *'No persons shall be subject to interference with the privacy of their homes, correspondence or communications save in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.'*

---

[285] Ibid at 206.

[286] David McQuoid-Mason 'Invasion of Privacy: Common Law v. Constitutional Delict - DoesIt Make a Difference' (2000) 2000 *Acta Juridica* 227-261 at 229.

[287] Sam K Amoo et al op cit note 274 at 61.

[288] Sisa Namandje *Privacy and Rationality Standard in Namibia* (2021) at 1.

[289] Ibid.

Privacy has granted a deeper meaning by the Namibia courts. In the 2015 case of *ES v AC*[290], the Court found that 'individual free choice and self-determination are themselves fundamental constituents of life' and concluded that 'moral autonomy is of central importance to the protection of *human* dignity and liberty in free and open democracies such as ours.'[291] It is however, worth noting that the constitutional right to privacy is, like its common law counterpart, not an absolute right but may be limited in terms of the law of general application and has to be balanced with other rights entrenched in the Constitution.[292] Article 22 of the Namibian constitution provides for the limitation of fundamental rights and freedoms. The scope of constitutional permissible restrictions on fundamental rights and freedoms was restated by the Namibian court in *S v Kauesa*:[293]

> '[I]n a democracy, basic rights and liberties must be limited. Restrictions are necessary for Namibia's sovereignty and integrity, national security, public order, decency, or morality, or for contempt of court, defamation, or incitement to commit an offense. Restrictions on fundamental rights and freedoms must be necessary in a democratic society. Not only must they be necessary in a democratic society, but they must also be required in the interests of sovereignty and integrity of Namibia, national security, public order; decency, or morality, or in relation to contempt of court, defamation, or incitement to commit an offence.'

It is common knowledge that fundamental rights, such as the right to privacy, can be curtailed and are prone to abuse, lest the Namibian courts strictly construe these limitations.[294] To this end, it is important to note that the Namibian Constitution does not countenance the restriction of fundamental rights and freedoms on grounds other than those mentioned in Article 22. Moreover, the party relying on the law which supports the restriction of rights bears the onus of proving that the restriction is constitutionally justified.[295]

4. CRITICAL ANALYSIS OF THE PROPOSED LEGISLATION: THE DATA PROTECTION BILL, 2013

The Namibian Data Protection Bill provides for the creation of a Data Protection Authority. Furthermore, the Bill intends to regulate how personal data should be used, processed, and

---

[290] ES v AC 2015 (4) NR 921 (SC) at par.72.

[291] Ibid.

[292] Article 22 of the Namibian Constitution.

[293] *Kauesa v Minister of Home Affairs (SA 5 of 1994) [1995] NASC 3 (11 October 1995).*

[294] Namandje op cit note 286 at 9.

[295] Ibid.

collected. This is to safeguard the right to privacy entrenched in article 13 of the Namibian constitution.[296] The Bill also provides for the protection of Namibian citizens against the abuse of their data and personal data and to regulate TBDF.

The Namibian Ministry of Communication and Information Technology has been collaborating with the ITU in the drafting of the Data Protection Bill as part of the HIPSSA Project, which fosters the use of coherent ICT policies and regulatory frameworks.[297] The HIPSSA project was discussed earlier in chapter 2. The aims of the proposed Bill are to give effect to the fundamental right to privacy by safeguarding personal data when it is handled by public and private entities.[298] The bill also aims to develop techniques and processes that are consistent with global standards on data protection.[299]

The legislative proposals culminating in the Data Protection Bill, set to be tabled in parliament, are ultimately the foundational stone of any claim that Namibia is moving towards a regulated data protection era. Despite all these tangible gains, the Bill is still faced with problems of incoherence, inconsistency, and contestation. Example, the Bill sparked an uproar from civil society when it was originally released in early 2017. The Namibian Institute of Public Policy and Research ('IPPR') has expressed concern that the Data Protection Bill lacks coherence and consistency with global data protection trends and standards.[300]

The shortcomings of the Data Protection Bill's architecture revolve around limitations in providing comprehensive and effective protection for data subjects regarding the control of TBDFs. Data protection law pursue dual goals.[301] First, it seeks to preserve the right to privacy (right-based). The second goal is to facilitate the free flow of data (economical).[302] The limitation on the scope of the Bill, which will be discussed below, puts it in a bottleneck conundrum posed by developing technologies that have hampered the efficacy of data

[296] Long title of the Namibian Data Protection Bill, 2013.

[297] Pria Chetty op cit note 25.

[298] Ibid. See also the preamble of the Data Protection Bill.

[299] Ibid.

[300] Links op cit note 37.

[301] Lynskey op cit note 2 at 46.

[302] Ibid.

protection laws in other countries for a long time.[303] As introduced earlier in Chapter 1, the relevant sections on TBDF are section 2 and 48 of the Data Protection Bill. Particularly, section 2(2)*(b)* of the Bill as quoted earlier states that the Bill applies to 'the processing of personal data by a controller who is not permanently established in Namibia, if the means used, which can be automated or other means is located in Namibian and is not merely for the purpose of transit of personal data through Namibia.'

In interpreting this section, the term 'means located in Namibia' refers to physical equipment such as main-frame computers and servers.[304] In this case, a local representative must be appointed.[305] This method presents a lacuna in the law when corporations handle personal data without Namibia-based equipment. Section 48 covers the transfer of data to a non-SADC nation without adequate protection. This provision prohibits such transfers unless consent is given, it is essential for the performance or completion of a contract, or it is in public interest.

It is argued that the provisions of the Namibian Data Protection law dealing with TBDF create an asymmetry in regulatory treatment pertaining to the data processing by foreign processors who do not have means situated in Namibia. The Data Protection Bill fails to regulate the conduct of data controllers who are not established in Namibia and who do not have access to processing 'means' situated in Namibia but offer goods or services to Namibian customers or monitor the activity of Namibian data subjects. This 'soft approach' amounts to uneven treatment and leaves local data processors at a competitive disadvantage vis-a-vis international data processors.'

In its present form, the Data Protection Bill does not effectively regulate TBDF. The idea of tying the law to national boundaries no longer corresponds to the data processing activities of the 21st century. In the past, the data controller, the data subject, and the data processing methods were frequently in the same country.[306] However, the expansion of e-

[303] See also Svantesson op cit note 77 at 236.

[304] Section 2 of the SADC Unictral model similarly provides that: A wider territorial scope of the processing of personal data by a controller who is not permanently established on [given country] territory, if the means used, which can be automatic or other means is located in [given country] territory'.

[305] See Greenleaf op cit note 136 at 13.

[306] Azzi et al op cit note 54 at 128.

commerce, new technology, and evolving multinational organisational structures have made international data processing and transmission more important.[307]

Additionally, reading the Namibian Data Protection Bill reveals that the provisions dealing with TBDFs resemble, although to a lesser degree, the EU DPD of 1995. In May 2018, the GDPR superseded the DPD.[308] The EU reformed its outdated data protection laws to accommodate the ever-evolving data protection challenges inherent in social networks, e-commerce, cloud computing, and location-based services.[309] Due to globalisation and the fast growth of technology, notably the internet, the 1995 DPD no longer offered legal certainty, according to the EU's explanatory memorandum.[310] When the DPD was adopted in 1995, the internet was young, and its drafters could not anticipate its impact on personal data processing.[311] As a result, there was legal ambiguity and a widespread public perception that there were significant risks associated with online activity.[312] According to the DPD reform package, these cutting-edge technologies demand a robust, coherent data protection framework coupled with rigorous enforcement.[313] Chapter 5 discusses the EU's data protection reform.

One can hardly compare today's global and all-encompassing web to the young internet of 1995, as data privacy expert Yves Poullet has noted.[314] Before satellite and LAN/WLAN technologies, point-to-point transfers between corporations or governments utilising physical infrastructures like servers, magnetic tapes, discs, cards, or other analogous media attached to territory represented the bulk of data flows in the early days of the

---

[307] Ibid.

[308] Last accessed from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en on 20 June 2021. See also

[309] EU 'Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM/2012/011 final - 2012/0011 (COD) **l**ast accessed from *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011* on 20 June 2021.

[310] Ibid at 3f.

[311] Ibid.

[312] Ibid.

[313] Ibid.

[314] Yves Poullet 'Is the General Data Protection Regulation the Solution?' (2018) 34 *Computer Law & Security Review* 34 (2018) 773–778 at 774.

internet.[315] Today's web merges endless large capacity of computers (big data), networks, and the infinitely little 'chips' in our wallets, in our glasses, or even in our bodies and brains.[316] Although this seems exaggerated, it's true. Thus, technological advances allow for data to be processed seamlessly and concurrently in various locations, sent for storage throughout the globe, recombined quickly, and transferred across international boundaries by people carrying mobile devices.[317]

To reiterate, globalization and rapid technological change, especially networked technologies, have profoundly disrupted conventional business models.[318] The confluence of disruptive technologies has accelerated the movement of machine-readable data across national borders.[319] With the internet, data may be sent electronically and swiftly through cables or satellites. IoT, cloud computing, genetic modification, nanotechnology, biotechnology, IT, and cognitive sciences have multiple applications.[320] In today's world, the applications are multiplied thanks to the IoT, cloud computing, genetic manipulation, and the contributions of nanotechnology, biotechnology, information technology, and cognitive sciences.[321] These cross-cutting technologies are called 'disruptive technologies'.

Marcelo Corrales and others, contend that most of these technologies depend on cloud computing. In 2006, Eric Schmidt made the following statement in relation to software as a service: 'you never pay them a visit; you never see them. However, they are out there.'[322] Edoardo Celeste and Federico Fabbrini define cloud computing as flexible, location-independent access to computer resources that are swiftly and seamlessly supplied or released on demand.[323] Dropbox, Google applications, and Microsoft 365 are typical cloud computing

---

[315] Gisela Moohan et al op cit note 131 at 27.

[316] Yves Poullet op cit note 312 at 774.

[317] Ibid.

[318] Marcelo Corrales op cit note 7 at 1.

[319] Ibid.

[320] Gisela Moohan et al op cit note 131 at 27.

[321] Ibid.

[322] Marcelo Corrales op cit note 7 at 2.

[323] Edoardo Celeste & Federico Fabbrini 'Competing Jurisdictions: Data Privacy Across the Borders' in Theo Lynn, John G. Mooney, Lisa van der Werff & Grace Fox *Data Privacy and Trust in Cloud Computing* (2021) at 48.

platforms.[324] Cloud computing reduces the need to invest in costly hardware and software, set up and manage on-site data centers, racks of servers, and 24-hour energy for power and cooling, etc.[325] The rise of cloud computing, however, undermines the effectiveness of data protection laws tied to territorial borders. This is because the cloud, as its name implies, is location independent, and it allows organisations and consumers to access data stored anywhere in the world.

The GDPR aimed to account for the changing digital environment. Marina Krinjar Vidovi argues that outdated laws foster anarchy and leave people unprotected.[326] Its territorial reach is based on 'establishment' (article 3(1)) and 'targeting' criteria (article 3(2)).[327] The targeting test allows for the extraterritorial application of the GDPR to processors not established in the EU.[328] The ensuing consequence of this new feature of the GDPR is that it accepts the realities of the 21st century data processing activities and therefore offers comprehensive protection to data subjects. The GDPR is an essential step toward greater personal data protection in a fluid technological world, and Namibia stands to draw positive lessons from it.

In this paper, I argue that the internet's borderless nature makes domestic data protection regulations tied to territorial borders less credible. Extending the reach of data protection laws that go beyond a domestic scope would guarantee full basic rights protection and level the playing field for data processors that are not established in Namibia in the context of global data flows. Modern technology has changed dramatically in recent years. Because the internet has no boundaries and is widely used, the Namibian Data Protection Bill should be amended to fit the new digital environment and protect Namibians' right to privacy. This paper proposes implementing the targeting test laid down in Article 3(2) of the GDPR as one such amendment. This test is part of the GDPR's new striking features meant to adapt to the digital age.

---

[324] Ibid.

[325] Last accessed from *https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits* on 23 August 2022.

[326] Marina Škrinjar Vidović op cit note 116 at 203.

[327] EDB Guidelines op cit note 86.

[328] Ibid.

The OECD Guidelines presumed that data flows should be allowed in general, but acknowledged the ability of governments to restrict them in certain circumstances, such as when the receiving country 'does not yet observe these Guidelines substantially or when the re-export of such data would circumvent its domestic privacy legislation.' [329] The traditional justification for TBDF regulations is that local data protection regimes would be weakened in the absence of constraints on third-party countries. Similar to how money ends up in tax havens, personal data may wind up in nations with the weakest or, more likely, no data protection rules. In the context of this tax analogy, nothing may prevent foreign data processors from circumventing local data protection regulations by gravitating personal data to data havens. In this light, the Namibian Data Protection Bill in its current shape may be readily circumvented.

In conclusion, given today's continuously interconnected planet and mass TBDF, it's necessary to harmonise national data protection legislation with international standards.[330] Domestic legal disparities may impede the free flow of personal data across borders; countries believe that harmonising national data protection laws is critical to protecting the right to privacy and avoiding international data flow bottlenecks.[331] As indicated above, the Data Protection Bill deviates from international data protection standards.

5. CONCLUSION

This chapter provided a general introduction and historical background to Namibian law's provision for the right to privacy. The Namibian constitution guarantees the right to privacy in Article 13, but the country lacks a comprehensive data protection legal framework. The Namibian government released a draft Data Protection Bill in 2013.The Bill has been criticised for lacking coherence and consistency with global standards. This chapter critically analyses the Data Protection Bill and the provisions relating to the control of transborder data flows. It traces the influence that the African regional data privacy instruments and the RECs have on Namibia and the EU DPD of 1995.

[329] Guideline 17. OECD op cit note 39 at 24.

[330] OECD Guidelines op cit note 39.

[331] Ibid.

The Namibia Data Protection Bill is aimed at being an omnibus data protection legislation for the country. The evaluation of the bill carried out in this section reveals that the Namibian Data Protection Bill corresponds to the 1995 EU DPD, the former global yardstick for data protection laws. However, the EU has since abandoned the DPD because it has failed to address the evolving advances in technology. It seems that Namibia has jumped onto a data protection bandwagon riddled with obsolete laws. In particular, the technical architecture of cloud computing, the internet of things, social media, etc. creates a series of jurisdictional challenges for data protection law limited to territorial borders. Ultimately, adopting antiquated laws will only foster lawlessness, and it will leave Namibian citizens' data exposed to possible abuse. This paper argues that adopting a broadened territorial scope is an essential step toward greater personal data protection in a fluid technological world.

This section also considers OECD recommendations that advise countries to restrict transborder data transfers where the recipient country does not observe its guidelines, or when the re-export of such data would circumvent its own privacy legislation. In this light, the arguments presented herein are that the Namibian Data Protection Bill, in its present state, creates a lacuna that may easily allow for its circumvention. By expanding its territorial reach, the Data Protection Bill would safeguard Namibians against circumvention. Although the OECD is an intergovernmental organisation and its recommendations are non-binding, the researcher believes they can assist Namibia better draft provisions for the Data Protection Bill's territorial reach. The next chapter explores the OECD Guidelines, the first to approximate regulation in this area and the first of the three international standards under review.

CHAPTER 4

OECD Guidelines, 1980: A Comparative Study

1. INTRODUCTION

As discussed in Chapter 2, the existing international legal framework for data protection and privacy is based on instruments such as the 1980 OECD Guidelines on Governing the Protection of Privacy and Transborder Flows of Personal Data (the 'OECD Guidelines'). The OECD is an inter-governmental organisation that has 36 members, 27 of which are from Europe, and hopes to grow.[332] All OECD members have comprehensive data privacy legislation (except for the United States in the private sector).[333]The OECD Guidelines served as a foundation for the EU DPD 95/46/EC and the APEC Privacy Framework (2004).[334] Broadly, the Guidelines have also influenced business practices and individual expectations.[335]

According to Greenleaf, the OECD Guidelines were established concurrently with the Council of Europe's data protection Convention 108 of 1981, with significant interaction between the committees responsible for each instrument, and they share many of the same ideas as Convention 108.[336] The two, taken together, make up the 'first generation' of international data privacy rules.[337] The OECD's headquarters are in Paris.[338]

---

[332] List of OECD Member Countries (OECD, 2013) *http://www.oecd.org/general/listofoecdmembercountries-ratificationoftheconventionontheoecd.htm*: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israël, Italy, Japan, Ko-rea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. The European Commission is entitled to take part in the work of the OECD.

[333] Graham Greenleaf 'It's Nearly 2020, so what Awaits the 1980 OECD Privacy Guidelines?' (2019) 159 *UNSWLRS* 1-11 at 3.

[334] The OECD Privacy Framework op cit note 39.

[335] Ibid.

[336] Ibid.

[337] Ibid.

[338] The Organization for Economic Cooperation and Development's main goals are to:

'(a) to achieve the highest sustainable economic growth and employment and a rising standard of living in

The OECD's Committee for Science Policy established a Computer Utilisation Group in 1969, which published a study in 1971 on 'Digital Information and the Privacy Problem', among other initiatives.[339] In 1974, a seminar was held on 'Policy Issues in Data Protection and Privacy', where the term 'transborder data flows' was first used in an international context. In 1976, the Committee on Scientific and Technological Policy merged its Computer Utilisation Group and its Scientific and Technical Information Policy Group into a new working party on Information, Computer, and Communications Policy.[340] With this move, the OECD was the first to combine all those different fields into one policy.

Legal expert Maria Tzanou notes that the OECD Guidelines take an economic approach to data protection.[341] This arises from its goals, which are to enhance economic and social well-being. So, the OECD is an economic organisation that evaluates productivity and global trade and investment flows, analyses economic issues, and is generally not engaged in human rights activities.[342] However, for the first time, an OECD Symposium was convened in Vienna in September 1977 on 'TBDF and the Protection of Privacy', where privacy protection and international communications issues were discussed altogether.[343] In a statement by Louis Joinet, who subsequently helped draft the OECD Guidelines, it was noted:

> '[E]conomic information is economic power, as information is power. Information has economic value, and the capacity to store and analyse specific types of data may provide one nation with technical and political advantage over another. This may result in a loss of national sovereignty because of transborder data flows.'[344]

Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy; (b) to contribute to sound economic expansion in Member as well as non-Member countries in the process of economic development; and (c) to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.'

[339] OECD 'Guidelines Governing the Protection of Privacy and Transborder Flows of Data' (1980) last accessed from *https://0-www-oecd--ilibrary* on 10 April 2022.

[340] Ibid

[341] Maria Tzanou op cit note 31 at 14f.

[342] Ibid.

[343] *https://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm* last accessed on (10 April 2022).

[344] Ibid.

The synergistic effect of this symposium turned out to be powerful, and subsequently, it was agreed that guidelines on this subject should be drafted at the OECD level. On September 23rd, 1980, the OECD Council approved these guidelines. Australia, Canada, Ireland, and the United Kingdom governments have abstained for the present.[345] The Guidelines are annexed to a recommendation of the OECD's Council and are complemented by an Explanatory Memorandum commenting on them in some detail.

This chapter examines the origins and relevance of the 1980 Guidelines, as well as their minimal revision in 2013.[346] Greenleaf argues that several 2013 guidelines were meant for non-OECD countries to minimise data export restrictions.[347] Namibia, which is not an OECD member, may certainly learn valuable lessons from the OECD Guidelines. This chapter compares the Namibian Data Protection Bill with the first of three international standards, that is, the OECD guidelines. The chapter is broken down into four parts: substantive scope, risks, the 2013 revision, and shortcomings of the 2013 revision.

2. SUBSTANTIVE SCOPE OF THE OECD GUIDELINES ON TBDF

The OECD privacy guidelines are the first global approach to TBDF regulation. The 1980 guidelines are a non-binding set of guidelines that member nations may enact. Its objectives are two-fold in nature. First, they ensure minimum privacy and personal data protection standards are observed.[348] Second, eradicating, as much as possible, conditions that would drive countries to limit TBDF for reasons relating to such flows.[349] Preparing quasi-legal norms has not been a feature of the operations of the OECD.[350] But as national and local privacy laws based on informatics (and especially TBDF) grew quickly, it became clear by the middle of the 1970s that inconsistency would have a negative impact on the economy and society.[351]

At the time, the absence of uniform regulations was feared to lead to inefficiencies and constraints on the intended flow of data as well as bureaucratic machinery to reconcile the

[345] Ibid.

[346] See Greenleaf op cit note 331 at 3.

[347] Ibid.

[348] Michael Kirby op cit note 61 at 234.

[349]Ibid at 235.

[350] Ibid.

[351] Ibid.

incompatible legal obligations of data processors and consumers.[352] It was believed that if a common legal framework was established at an international level, and followed at the national level, regulatory inefficiencies, or at the very least, glaring differences could be avoided.[353] At the same time, the basic right to privacy could be upheld in multiple jurisdictions regardless of the international nature of the technology.[354]

The eight core guidelines of national application in part two of the OECD guidelines (principles 7–14) form the backbone of the guidelines. These are the concepts of data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[355] In addition to this, the Guidelines include four fundamental principles of international application (principles 15–18) governing the free flow of personal data and legitimate restrictions on such data exports. The primary provisions dealing with TBDF in the 1980 OECD Guidelines are as follows:[356]

> '[M]ember countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure. (Guideline 16) ….and a Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.' (Guideline 17)

The main thrust of these principles is that member countries should avoid imposing restrictions on the free flow of personal data among themselves, while also acknowledging that data export restrictions can be justified, as set out in three exceptions in Guideline 17, the first of which is when the other member country "does not yet substantially observe these guidelines."[357] They also acknowledge the economic and social benefits of transborder data

[352] Ibid.

[353] Ibid.

[354] Ibid at 236.

[355] Greenleaf op cit note 331at 3f.

[356] OECD Guidelines op cit note 39.

[357] Greenleaf op cit note 331 at 4.

flows, and as the world economy becomes more globalized, the freedom to transfer personal data globally is becoming increasingly important in fostering economic and social growth.[358]

Although the OECD recommendations were not binding, they have influenced the development of national and subnational laws and policies. In Australia, the Privacy Act 1988 sets out 'privacy principles', which amount to an adaptation of the OECD guidelines.[359] In Canada, the Canadian Privacy Act and the complementary Access to Information Act came into force on July 1, 1983.[360] The Canadian Privacy Act affords rights to citizens and permanent residents to examine information about themselves under the control of federal institutions. It replaced and expanded provisions in the Canadian Human Rights Act. The Canadian Privacy Act embodies the eight OECD principles. Those principles have also been adopted in Canada by private-sector organisations.

3. RISKS AND UNDERLYING POLICIES

According to the OECD, the abundance and persistence of personal data have elevated the risks to individuals' privacy.[361] Personal data is increasingly being used in ways that were not anticipated when it was collected. Almost every human action creates a digital data trail, making it easier to track people's movements. Personal data security breaches are common. These increased risks signal the need for more effective safeguards to protect privacy.[362]

Several initiatives have been undertaken in recent years to address new and heightened privacy risks, especially in the context of cross-border data flows. The regulations guiding the control of TBDF are based on the perceived dangers associated with the TBDF of personal data. According to Kuner, these dangers can be related to the four policy reasons, namely: '(1) avoiding the circumvention of national data protection and privacy legislation, (2) protecting

[358] Ibid.

[359] Ibid.

[360] Ibid.

[361] *https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf* last accessed on (14 April 2022).

[362] Ibid.

against data processing hazards in other countries, (3) addressing challenges in claiming data protection and privacy rights overseas, and (4) boosting consumer and individual trust.'[363]

4. REVISED OECD GUIDELINES, 2013

By 1995, it was clear that the OECD guidelines were insufficient to offer adequate regulation in an ever-changing digital world. As early as 1999, they were criticised as an inadequate standard,[364]including by the chair of the committee that drafted them.[365] Nearly four decades have passed since 1980, and the international context has developed to include the GDPR, Convention 108+, and regional agreements.[366] These instruments provide far more stringent requirements than the OECD guidelines.[367] The review of the OECD Guidelines was born out of the Seoul Declaration for the Future of the Internet Economy, which was adopted in June 2008.[368] The Seoul Declaration calls for the OECD to assess the application of certain instruments, including the Privacy Guidelines, in light of 'changing technologies, markets, and user behaviour and the growing importance of digital identities'.[369]

In the past 40 years, the volume and usage of personal data have changed significantly, due in part to the widespread availability of fixed and mobile internet-connected computers. The need to revise and modernise the 1980 OECD guidelines was driven by the ongoing nature of technological advances and an anticipated expansion of TBDF.[370] The shortfalls of the initial guidelines included the lack of limitations on personal data exports in instances where the recipient country did not provide adequate protection. The 1980 OECD guidelines took a far lighter approach, requiring the blocking of data exports as a default legal position. Kuner summarises the significant changes since the Guidelines were adopted to include:

---

[363]Kuner C 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future '(2011)187 *OECD Digital Economy Papers* 1-40 at 31f.

[364] Roger Clarke 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) last accessed from *http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html* on 11 April 2022.

[365] Greenleaf et al op cit note 331 at 4.

[366] Ibid at 1.

[367] Ibid.

[368] See *https://www.oecd.org/digital/consumer/40839436.*pdf 12 April 2022.

[369] Ibid.

[370] Ibid.

'*(a)The increasing economic value of data processing (b)internet-based data transfers are ubiquitous (c)greater individual participation in transborder data flows (d) the development of new technologies and business models for processing personal data has led to an increase in the direct participation of individuals in the cross-border transfer of their data and, (e)the shifting function of geography.'*[371]

From 2011-2013, the OECD's Working Party on Information Security and Privacy (WPISP), chaired by Canada's Privacy Commissioner at the time, assembled a panel of non-governmental experts to review the Guidelines and publish a report.[372] Based on the expert group's work, the WPISP offered amendments, which were adopted by the Committee for Information, Computer, and Communications Policy (ICCP) before ultimate ratification by the OECD Council.[373] The OECD updated its original guidelines from 1980, which became the first internationally accepted privacy standard, on September 9, 2013. The revised Guidelines include two themes:

'(1) The necessity for a pragmatic, risk-management-based approach to the implementation of privacy protection; and (2) the need to increase global privacy protection through enhanced interoperability.'[374]

The revised Guidelines do not change the core 'Principles of National Application' at all from the 1980 version (described above), but do add some useful new content on implementation, plus some new weaknesses (see below). Part four of the revised OECD guidelines talks about the basic principles of international application dealing with free flow of data and legitimate restrictions. It states, inter alia, that:

'Revised Guideline 16 - that a data controller remains accountable for personal data under its control without regard to the location of the data.
Revised Guideline 17-A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement

---

[371] Ibid.

[372] Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines (OECD,11 October 2013) last accessed from h*ttp://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecdprivacy-guidelines_5k3xz5zmj2mx-en* on 11 April 2022.

[373] OECD 'Privacy Guidelines and Supplementary Explanatory Memorandum' (2013) last accessed from *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf* on 11 April 2022.

[374] Ibid.

mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

Revised Guideline 18-Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.'

The most essential insight from the revised guidelines is that member states should not impede the cross-border flow of personal data by imposing limitations vis-a-vis other member states, provided that the receiving state also abides by the guidelines and has adequate enforcement measures in place.[375] According to these revised guidelines, any restrictions on transborder flows of personal data should be proportionate.[376] Furthermore, the revised guidelines call on member states to: 'develop national privacy strategies; adopt laws protecting privacy; establish privacy enforcement authorities; encourage and support self-regulation through, for example, codes of conduct; and provide a reasonable means for users to exercise their rights, among other measures.'[377]

These revisions seek to strengthen privacy enforcement and modernise the OECD's approach to international data flows. For example, the Revised Guidelines include references to 'risk' and 'proportionality'. This signals a focus on a risk-based approach. The OECD recommends that any restrictions on TBDF imposed by member countries should be proportionate to the privacy risks associated with the personal data (i.e., considering the sensitivity of the data, the purpose and context of the processing).

5. SHORTCOMINGS OF THE REVISED GUIDELINES

The 2013 OECD revised guidelines are, however, not without controversy. For example, Greenleaf argues that the 1980 Guidelines required members to 'take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure'.[378] This is completely removed from the 2013

[375] Last accessed from *https://unctad.org/system/files/official-document/der2021_en.pdf* on 29 September 2022.

[376] Ibid.

[377] Ibid.

[378] Greenleaf op cit note 331 at 9.

Guidelines, which considering the Snowden revelations, is a very convenient result for many OECD member governments, and a very poor result for other countries and their citizens.[379]

Be that as it may, the OECD is currently reviewing, and perhaps revising, its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, originally made in 1980 and revised once in 2013.[380] It is thus an appropriate time to assess the Guidelines' relevance, as well as the prospects for this revision to make them more relevant to the future of data privacy regulations. Greenleaf goes on to argue that even though the 2013 guidelines downplay the relevance of legislative execution in favour of non-legislative methods.[381]

The 1980 Guidelines included in the Recommendations by the Council 'that Member countries consider in their domestic legislation' the Guidelines and in the Guidelines concerning national implementation, that they 'endeavour to adopt appropriate domestic legislation' to implement them. The 2013 Guidelines, however, omit all of this, instead advising that member nations apply the guidelines via procedures that include all relevant stakeholders. This means that a pledge to create data protection legislation adopting the Guidelines is no longer required under the revised version. Consequently, regulatory approaches such as patchwork data protection laws in the US are more easily justified as being adequate.

6. CONCLUSION

The contemporary global legal framework for data protection and privacy is founded on instruments such as the 1980 OECD Guidelines, as noted in this chapter. Today, all OECD nations have robust data privacy laws that adhere to its principles (with the exception of the United States in the private sector). The Guidelines have served as a framework for other international instruments, such as the EU DPD of 1995 and the APEC Privacy Framework. This chapter examined the origins and importance of the 1980 Guidelines, as well as their extremely limited amendment in 2013. However, 1980 is over four decades ago, and the international environment now includes the GDPR, Convention 108+, and regional instruments

[379] Ibid.

[380] See OECD 'OECD work on privacy '*http://www.oecd.org/sti/ieconomy/privacy.htm* - The review is mentioned but no documentation is yet public.

[381] Greenleaf op cit note 331 at 10.

and standards which are much stronger than the Guidelines. Therefore, this chapter also examined the Guidelines' continued relevance and how Namibia can draw positive lessons from them.

As a first point of reference, guideline 15 of the OECD guidelines requires that member countries take into consideration the implications for other member countries of domestic processing and re-export of personal data in order to ensure harmonisation of laws and reduce barriers due to differing legislative provisions. The central tenet of the OECD guidelines as far as TBDF is concerned is that countries should avoid imposing restrictions on the free flow of personal data among themselves while recognising that data export restrictions can be justified, as outlined in guideline 17.Thus, guideline 17 states that countries are allowed to prohibit transborder data transfers where the recipient country does not follow its rules or when re-exporting such data would circumvent its own domestic privacy legislation.

In 2013, the OECD revised its guidelines. This is the first revision of the Guidelines since 1980, and it analyses them in light of changing technology, markets, and usage behaviour and the rising relevance of digital identities.[382] The OECD acknowledged that point-to-point transfers between firms or governments comprised the bulk of data flows in 1980.[383] Today, mobile devices may analyse data simultaneously in many places, store it globally, instantly combine it, and transport it across boundaries.[384] Businesses and individuals may access data stored anywhere utilising cloud computing. The revision was, however, criticised for not offering enough guidance in an era of digitalisation.

Be that as it may, although the OECD is an intergovernmental organisation and its recommendations are non-binding in nature, the researcher believes it can help Namibia on laws relating to the regulation of transborder data in the Data Protection Bill. Lastly, as discussed in the preceding chapter, the OECD was the first organisation to approximate laws in this area, followed by the European Union in 1981 with Convention 108 of the Council of Europe.[385] Data protection and the regulation of TBDF in the EU resemble several underlying

[382] The OECD Privacy Framework op cit note 337.

[383] Ibid.

[384] Ibid.

[385] UNCTAD Digital Economy Report op cit note 9 at 166.

principles of the 1980 OECD Privacy Guidelines, albeit to a certain extent.[386] In the chapter that follows, I will present the EU data protection law.

[386] Ibid.

CHAPTER 5

Data Protection in the EU: A Comparative Study From the DPD to the GDPR

---

1. INTRODUCTION

Laws governing TBDF in the EU have evolved concurrently with the broader field of personal data protection, of which it is a well-defined subset.[387] According to Mark Phillips, the law considered to be the first data protection statute, adopted in 1970 in the German Federal State of Hessen, did not address international data transfer.[388] But those who followed, both in Europe and elsewhere, quickly realised that it was futile to develop a framework to protect personal data if such safeguards could be easily bypassed by gravitating the data of the individuals it was intended to protect to a different jurisdiction that had lax laws on data protection. This chapter looks at the regulation of TBDF in the EU, with a particular focus on the targeting test provided for in Article 3(2) of the GDPR and the default legal position.

The EU's personal data protection principles are widely adopted by most countries around the world, according to Sulivan.[389] This includes both developing and developed countries.[390] Most countries' laws are based on the Directive from 1995, which was the forerunner of the GDPR, which went into effect in 2018.[391] The extent of the adoption varies, with some countries closely following the DPD (and hence most of the GDPR), while others have adopted key elements. The notable exception is the US, which has not generally followed the EU model of data protection as noted in Chapter 2.

---

[387] Mark Phillips 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)' (2018) 137 *Human Genetics* 575–582 at 575.

[388] Ibid.

[389] Clare Sullivan 'EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era' (2019) 35 *Computer Law and Security Review* 380-397 at 380. See also Paul M. Schwartz op cit note 245 at 771.

[390] Ibid.

[391] Ibid.

According to Mercer,the widespread acceptance of the EU model is motivated by pragmatic considerations.[392] The EU requires countries that seek to conduct business with the EU to have data protection standards that are equivalent.[393] Goldsmith and Tim Wu, a policy advocate, and Columbia University Law School professor, argue that the EU has become the effective sovereign in this field. This is because it implements a unilateral worldwide privacy rule because of Europe's immense market strength, and it has particular concern for the privacy of its citizens.[394] Because the EU is a highly important marketplace for international companies, many companies do not have the option to 'completely withdraw from the EU market'.[395]

The perspective taken in this paper is that the EU model offers more positive lessons than merely exerting dominance on the world. On the contrary, as noted in chapter 2, lax data protection standards can jeopardise the right to privacy and other rights. The EU's approach is deemed comprehensive, neutral, and holistic, which may explain why it has earned so much popularity since its inception. The EU emphasises individual data control.[396] Consequently, it proposes a robust and strict regulatory approach to the data-driven digital economy, based on the preservation of the European Union's basic rights and values. This is called a human-centered approach because it puts a lot of emphasis on protecting the privacy of each person.[397]

Professor and author Paul Schwartz, a specialist in information privacy, correctly asserts that there are two factors that have aided the spread of EU data protection law throughout the world.[398] The first element has to do with legal substance. Public opinion on consumer privacy has significantly changed. Public discourse and prominent people in many non-EU jurisdictions now recognise the benefits of EU-style data protection.[399] In addition to its substantive advantages, the EU has benefited from the accessibility of its omnibus

[392] Shannon Togawa Mercer 'The Limitations of European Data Protection as a Model for Global Privacy Regulation' (2020) 114 AJIL Unbound 20-25 at 20.

[393] Merlin Gomman op cit note 97 at 568.

[394] Jack Goldsmith and Tim Wu *Who Controls the Internet? Illusions of a Borderless World* (2016) at 176.

[395] Paul Schwartz op cit note 245 at 778.

[396]Global Digital Partner op cit note 4 at 58ff.

[397]Ibid.

[398] Paul Schwartz op cit note 245 at 771.

[399] Ibid.

legislative approach, which has attracted other jurisdictions to its highly adaptable legal model. The world has spoken, and the EU is reaping the benefits of its success in the market for regulatory concepts and good lessons.[400]

This chapter introduces the EU's approach to regulating personal data and TBDF and surveys the normative foundations of the European Union's data protection law. Furthermore, the chapter explains the genesis of the Data Protection Directive 95/46/EC of the European Parliament, and of the Council on the protection of individuals regarding the processing of personal data, and on the free movement of such data (the 'DPD') and its successor, the GDPR. It is critical that policymakers and legislators are familiar with the finer nuances of GDPR before they commence policy or lawmaking processes; this will go a long way in enhancing laws that seek to protect the rights of citizens in an environment where data is traversed with a single click across national borders.

An analysis of the recent data protection reform in the EU will be conducted. The chapter introduces the drivers of the reform by examining a few seminal EU Court of Justice judgments, the shortcomings in the 1995 Data Protection Directives, and how the Snowden revelations helped shape the current GDPR to introduce the reform's drivers. It will highlight the key changes that the new General Data Protection Regulation brings about, assess their implications, and seek to situate them in the wider context of the digital economy and its governance, regarding the regulation of TBDF.

2. A HUMAN RIGHT TO DATA PROTECTION

At the outset, it is noted that the right to privacy is a key concept in EU law and has been given significant weight, which reflects deep cultural values and understandings.[401] According to Chris Jay Hoofnagle and others, the EU data privacy law fulfills constitutional obligations that are profound and crucial to the self-conception of a new political body in the information era.[402] In relation to this constitutional obligation, Stefano Rodotà, one of the authors of the European Union's Charter of Fundamental Rights, explained that:[403]

---

[400] Ibid.

[401] Mira Burri et al op cit note 92 at 481.

[402] Chris Jay Hoofnagle et al op cit note 5 at 66.

[403] Ibid. See also S Rodotà 'Data Protection as Fundamental Human Right' in S Gutwirth, Y Poullet, P De Hert, C de Terwangne, and S Nouwt (eds) *Reinventing Data Protection?* (2009).

> '[T]he basic right to personal data protection may be seen as a pledge comparable to that made by the monarch to his knights in 1215, in the Magna Charta, that they would not be unjustly incarcerated or tormented-"nor will go upon him nor send upon him". The habeas corpus should be reconfigured and translated from the physical body to the digital body. In view of the rising focus on respecting the human body, the inviolability of the person must be reaffirmed and enhanced in the cyber sphere.'[404]

To render the digital body sacrosanct and building upon the Council of Europe's European Convention on Human Rights, which safeguards the right to private and family life, its Article 8, the Charter of Fundamental Rights of the EU ('CFR')[405] enshrines the right to the protection of personal data. The CFR is viewed as a crucial constitutional document inside the EU.[406] After the Lisbon Treaty was ratified by EU member states in 2009, the CFR became part of the EU's constitutional law.[407] This sets the EU Charter apart from other international human rights documents in that it safeguards the right to privacy and the right to data protection through separate articles (Articles 7 and 8), thereby making it sui generis. Article 8, entitled "Protection of Personal Data", stipulates that:

> '(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 based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data that has been collected concerning him or her, and the right to have it rectified.'

According to Burri and Schar, this distinction is no coincidence. It reflects the heightened concern of the EU and translates into a positive duty to implement effective protection of personal data and to regulate the transmission of such data.[408] In 1997, the European Court of Human Rights in *Z. v. Finland*[409] said that 'the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life'. Similarly, in the case of *Biriuk v. Lithuania*,[410] the applicant was an HIV-

[404] Chris Jay Hoofnagle et al op cit note 5 at 66ff.

[405] Ibid.

[406] Paul M. Schwartz op cit note 179 at 125.

[407] Ibid.

[408] Mira Burri et al op cit note 92 at 480.

[409] *Z. v. Finland (1998) 25 EHRR 371.*

[410] *Biriuk v. Lithuania Case C-23373/03*.

positive lady residing in the hamlet of Kraštų. Her health status was published in a local newspaper as provided by the local hospital without her consent or knowledge. The European Court of Human Rights held that this was a blatant violation of the woman's right to privacy and an 'outrageous abuse of press freedom'. The court also held that the exploitation of her personal information had resulted in her public ridicule and banishment from local social life.

Additionally, the individual's fundamental rights must be safeguarded even in the absence of sensitive information or harm. Schwartz and Karl-Nikolaus Peifer, law professors and privacy experts, note that the European Court of Justice emphasised this point in two landmark privacy rulings: *Google Spain, Google Spain SL and Google Incorporated v Agencia Española de Protección de Datos ('AEPD') and Costeja González*,[411] dubbed the 'right to be forgotten' ruling, and *Maximillian Schrems v Data Protection Commissioner*[412]('Schrems I'), celebrated (or criticised) as the decision that plunged the Safe Harbor agreement.[413]

In Google Spain, the European Court of Justice remarked that the data subject's basic rights are not predicated on whether the inclusion of the information in question causes the data subject harm. Rather, the processing of personal data entails an inherent danger to the data subject's rights and, due to this risk, may only be conducted if the law authorises it and governs how the information will be used. In the case of *Schrems I* case, the European Court of Justice similarly stated:

> '[T]o establish an infringement with the basic right to privacy, it is irrelevant whether the information in question .... is sensitive or whether the affected individuals have endured any negative effects because of this intrusion.'[414]

3. HISTORY OF THE EUROPEAN DATA PROTECTION LAW

The gathering of personal data is not a recent phenomenon. Individual record-keeping dates to the dawn of civilisation.[415] Wayne Madsen notes that the Roman Empire maintained

---

411 *Case C-131/12 Google Spain, Google Spain SL and Google Incorporated v Agencia Española de Protección de Datos ('AEPD') and Costeja González*

412 *Case C-362/14 Maximillian Schrems v Data Protection Commissioner*

413 Paul M. Schwartz et al op cit note 179 at 127.

414 Shcrems supra note 411.

415 Roos Anneliese 'The law of data (privacy) protection: a comparative and theoretical study' (Unpublished thesis of the University of South Africa, 2009) last accessed from http://hdl.handle.net/10500/1463 on 05 July 2022.

comprehensive tax records on its inhabitants, who were identified through a census.[416] Understanding the history of data protection initiatives in the EU assists in elucidating the evolution of data privacy and protection in the EU. The history of the EU's data protection efforts, the evolution of privacy rights, and the ramifications of specific rules can help place recent events in context. Europe has long been at the forefront of data privacy and related regulation. This is partly due to a better awareness of how data has been abused historically and in the present day.[417]

A look at the history of European data privacy demonstrates that this practice has its origins in post-World War II privacy standards.[418] Still bleeding from the Nazi tyranny and determined to keep the government out of the house, Europe placed a premium on personal data.[419]Writing on the historical narratives of Europe's privacy stewardship, Rossi Agustin argues that there are two prevailing cultural accounts.[420] The first and most common variation, known as the 'fascist legacies theory', contends that because of the previous century's totalitarian and fascist experiences, Europeans have learned to defend and safeguard their privacy.[421]

The second is the 'European dignity' explanation, which compares how Americans and Europeans handle privacy.[422] According to Whitman, Europeans consider privacy to be a matter of dignity and honor, whereas Americans consider it a matter of liberty.[423] Whitman adds that European conceptions of privacy date back to the late eighteenth century, particularly

[416] Wayne Madsen *Handbook of Personal Data Protection* (1992) at 7.

[417] Rossi Agustín 'How the Snowden Revelations Saved the EU General Data Protection Regulation' (2018) 53 *International Spectator* 95-111 at 96. See also Olivia B. Waxman 'The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights: That Outlook Has a Disturbing History' (2018) last accessed from *https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/* on 15 June 2002.

[418] Lucas Bergkamp op cit note 244 at 32.

[419] Ibid.

[420] Rossi Agustín op cit note 416 at 96f.

[421] Ibid.

[422] Ibid.

[423] James Q. Whitman 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151-1196 at 1161.

German Kantian conceptions of personality, which place a higher emphasis on the right to manage one's public image, and French notions of dignity and honour.[424]

Germany is the epicentre of data privacy in Europe.[425] This has roots in the country's darkest years of Nazi rule.[426] Germany went from being the infamous abuser of personal data to setting new global norms. Giving Facebook and Google access to personal data may seem like a 21st-century thing, but Nazi Germany faced a similar dilemma before World War II.[427] In the 1930s and 1940s, Nazi Germany collected personal data using census cards and Hollerith machines.[428] This was used to categorise Germans by race, sexual orientation, politics, talents, and religion.[429] The following years of detention, torture, and murder of people based on these classifications have been immortalized as the Holocaust, one of the darkest times in contemporary history.[430]

Since the late 1980s, when it began working on data protection legislation, the EU Commission has been positively inclined with privacy issues. While data protection regulations at a domestic level have established an adequate level of protection for personal data in the EU, international agreements have significantly aided in the development of national data privacy laws that are compatible with one another.[431] In this regard, Convention 108 was adopted at an international level as the first international agreement on data protection and TBDF open for signature, as discussed in Chapter 2.[432]

---

[424] Ibid at 1162

[425] Andy Green 'Nazi Data Science: The Dark History that Led To Modern Data Laws' (2020) last accessed at *https://www.magellantv.com/articles/nazi-data-science-the-dark-history-that-led-to-modern-data-laws* last accessed on 15 June 2022.

[426] Ibid.

[427] Ibid.

[428] Olivia B Waxman op cit note 416.

[429] Ibid.

[430] Ibid.

[431] Berkay Karadogan 'GDPR and COnvention 108 Article' (2019) Last accessed from *https://www.researchgate.net/publication/336512782_GDPR_and_COnvention_108_Article* on 23 June 2022.

[432] Ibid.

Meanwhile, the urge for harmonisation of data protection legislation within the confines of the EU led to the adoption of EU-based legislation. In the realm of data protection, the EU advanced by replicating the legislation of France, Germany, Sweden, and a few other nations from the 1970s.[433] Abraham Newman described this first step as the regional translation of domestic legislation established in the 1970s in various European nations.[434] In 1995, when some EU Member States had already passed privacy legislation, the EU issued the DPD, which created its comprehensive data protection framework.[435] Below (Figure 1) is a timeline illustrating the evolution of data privacy and TBDF laws in the EU over time.

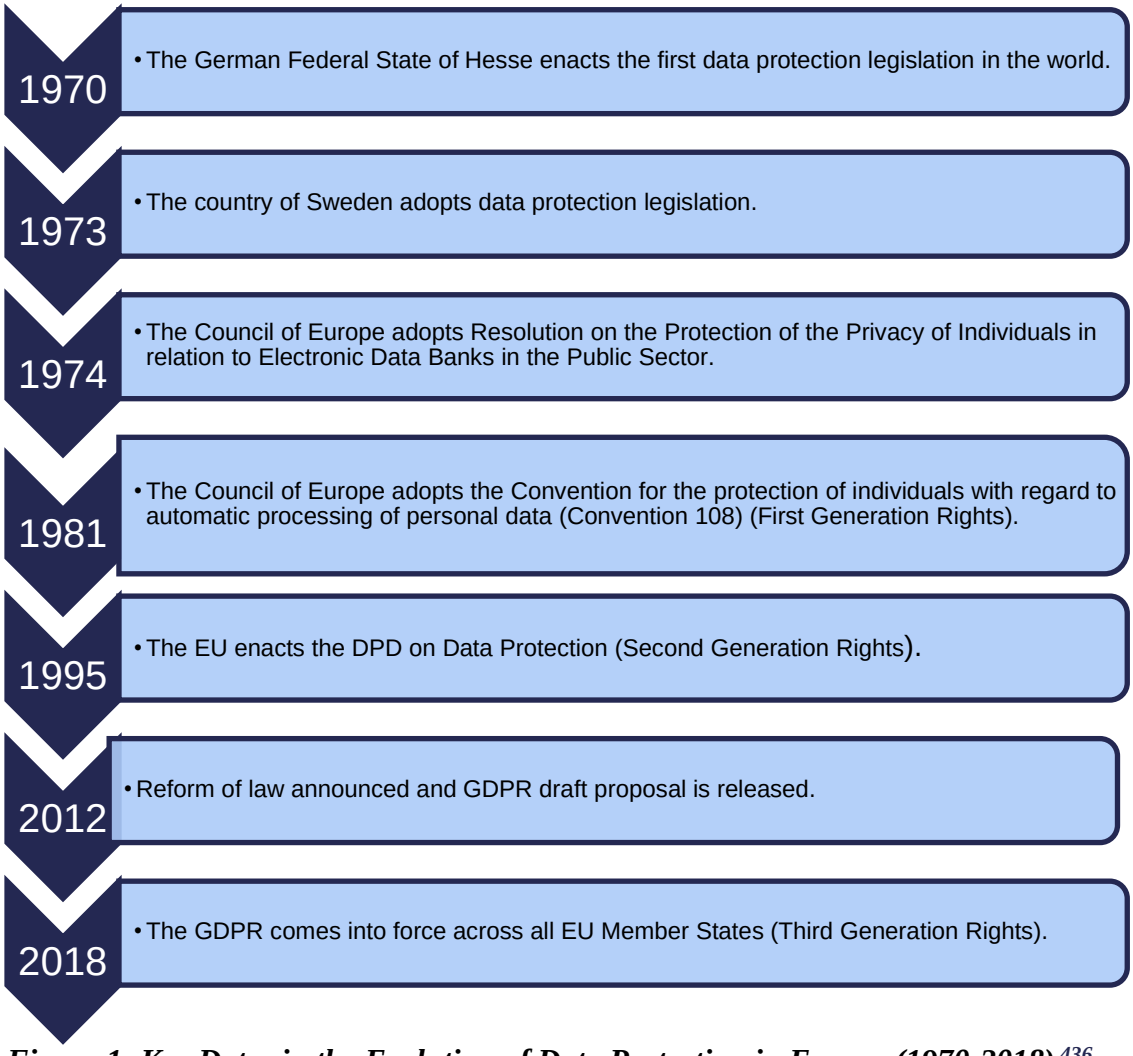


Figure 1: Key Dates in the Evolution of Data Protection in Europe (1970-2018) [436]

[433] Schwartz op cit note 245 at 810.

[434] Ibid.

[435] Berkay Karadogan et al op cit note 430 at 1f.

[436] Global Digital Partners op cit note 4 at 18.

Final Remarks

Throughout this part, we have seen that the EU has enshrined the protection of privacy as a fundamental human right in a plethora of post-World War II legislative instruments.[437] The horrific events and atrocities of this period, when large databases of personal data were used to segregate societies, target minority groups, and facilitate ethnic cleansing, demonstrated how dangerous allowing public intrusion into the private sphere could be.[438]

In the 1950s, Germany and Sweden were the pioneers in enacting the first privacy laws in Europe. However, there was minimal harmonisation of these laws at the EU level. Some Member States established stringent limits and procedures, whilst others did not.[439] This variation stifled the expansion of the internal market. In this setting, the DPD was conceived as an internal market device intended to facilitate cross-border commerce by harmonising data privacy laws.[440] In the following section, I examine the EU Data Protection Directive, its regulation of transborder data flows, and the shortcomings that led to its replacement by the GDPR.

4. EUROPEAN DATA PROTECTION DIRECTION, 1995

Since the DPD was passed in 1995, the EU has had data protection legislation safeguarding the fundamental data protection rights of EU citizens. The EC feared in 1990 that the EU's single market would be hampered by different national legislation on data protection.[441] A proposition for a DPD was presented in the same year. After five years of deliberation, the final DPD was ratified in 1995. The DPD established an omnibus regime that applied to a wide range of

[437] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri 'Review of the European Data Protection Directive' (2009) last accessed from *https://www.researchgate.net/publication/265450064_Review_of_the_European_Data_Protection_Data Protection Directive* last accessed on 21 June 2022.

[438] Ibid.

[439] Ibid at 6.

[440] Ibid.

[441] Paul Voigt & Axel von dem Bussche *The EU General Data Protection (GDPR): A Practical Guide* (2017) at 1.

businesses and government agencies. For the DPD to be effective, member states need to enact enabling legislation.

The DPD includes 34 articles on data quality, special processing categories, data subject rights, confidentiality, security, liability and sanctions, codes of conduct, and supervisory authorities.[442] It shares key principles with other legal texts, notably the Asia-Pacific Economic Forum ('APEC') and the 1980 OECD Guidelines.[443] One of its fundamental aspects is that it is based on the idea of personal data and not privacy. [444] Neil Robinson and others have argued that the DPD's regulations may be applied to the processing of data that poses no threat to individuals' privacy.[445] The Directive serves several functions, including the protection of privacy. Its policies foster free expression, eradicate prejudice, and boost efficiency.[446]

In the case of *Digital Rights Ireland,*[447] the court found that the DPD entails an extensive and particularly serious interference with Articles 7 and 8 CFREU. Furthermore, there were no defined substantive and procedural conditions with regard to access to the data; nor were objective criteria for the determination of the retention period laid down.[448] Neither did the DPD provide any adequate safeguards to ensure effective protection of the data retained against the risk of abuse or against any unlawful access to and use of that data.[449]

As a starting point, the relevant provision of the DPD dealing with its territorial scope is Article 4, which was referred to in chapters 1 and 3.[450] Thus, in terms of this article, the place of establishment of the controller or processor of personal data is the most significant

---

[442] Neil Robinson op cit note 436 at 7.

[443] Ibid at 7.

[444] Ibid.

[445] Ibid.

[446] Ibid.

[447] *Joined Cases C-293 & C-594/12 Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl, and others.*

[448] Ibid.

[449] Ibid at 485 and par. 66.

[450] See exact wording of section at 44.

determining element in determining whether the DPD rules apply.[451] Regarding the analogous clause of Directive 95/46, the CJEU explained in the Costeja[452] decision that:

> '[P]rocessing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.'

Equally important for the purposes of TBDF is the 'default legal position' established by the Directive, which stipulates that TBDF is not permitted unless the third nation ensures an acceptable degree of protection.[453] In terms of Article 25 of the EU Directive, it provides that the European Commission ('EC') may decide, upon approval of a qualified majority vote of Member States,[454] to prohibit all data transfers to a third country, including the United States, if the Commission finds that the third country does not ensure an adequate level of protection of data privacy rights.[455] Article 25 of the EU DPD provides:

> *'Member States shall provide that the transfer to a third country of personal data which is undergoing processing or is intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.'*

By reference to Convention 108, the EU DPD establishes a comparable legal framework for the transfer of data across borders.[456] The EU system aims to meet both the Directive's goals i.e., free flow of data and effective protection of individual privacy. The disparity in data protection levels across Member States may hinder the transfer of personal data from one state to another. This disparity may also impair the pursuit of a variety of

---

[451] Dário Moura et al op cit note 6 at 31.

[452] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Case C131/12*.

[453] Foivi Mouzakiti 'Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive' (2015) 1 *Europe Data Protection Law Review* 39-51 at 40.

[454] Ibid.

[455] Ibid.

[456] Lingjie Kong op cit note 150 at 443.

economic activities at the level of the community, skew competition, and hinder authorities from carrying out their responsibilities under community legislation.[457] In order to guarantee a minimal degree of data protection at the community level, national data protection laws, regulations, and administrative requirements must be coordinated and harmonised.[458]

If the EU determines that a country offers an acceptable degree of safeguards for personal data, it may get the same status as a member state for data transfer; otherwise, it is prohibited. The adequacy of data transmission is defined by its nature, its location of origin, its destination, and its laws.[459] According to Lingjie Kong, such a legal regime creates a barrier to the personal data of EU citizens and an 'iron curtain' for data transfer outside the Union.[460]

Considering that the majority of third nations have been deemed inadequate, the DPD identifies exceptions to the rule, including the use of standard contractual clauses, consent, and codes of conduct. [461] Data transferors are encouraged to provide sufficient safeguards for personal data, through which data may be transferred to third countries that do not maintain an adequate data protection level. Such an approach should be restrictively interpreted and applied. In other words, adequacy in the level of data protection is the principle, while the above cases are exceptions. In summary, there are three legitimate grounds for the transfer of data outside the European Union: (a) the destination country is qualified by the European Union as providing adequate protection of the data (Article 25(2)); (b) the data transfer belongs to the exceptional cases listed in (Article 26(1)*(c)*); and (c) adequate protections is provided by the use of standard contractual clauses (Article 28(3)), consent (Article 7), certifications (Article 42) and codes of conduct (Article 40).[462]

---

[457] Paragraph 8 of Data Protection Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995 *last accessed from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN* on 23 June 2022.

[458] Ibid.

[459] Anneliese Roos 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 11 *PELJ* 62-109 at 63.

[460] Lingjie Kong op cit note 150 at 443.

[461]Ibid.

[462] Ibid.

The DPD was formed when information processing merged file systems and computer mainframes.[463] The inherent risks associated with this paradigm could be readily handled by outlining the responsibilities and processes associated with each function.[464] Its principal goals were to build a unified European market for the free flow of personal data and to unify the domestic laws of EU members to preserve the data subject's right to privacy.[465] Alas, the EU never thought to create a legal model capable of addressing future data processing and privacy issues.

In a networked global society, personal information is continually collected, improved, modified, exchanged, and reused. What is continuously apparent is that the technological realities of the 21st century need a well-adjusted data protection regulation to effectively address the burgeoning risks of abuse. The next section gives a synopsis of the shortfalls of the DPD and its subsequent reform. Furthermore, the section presents the drivers of the EU data privacy law reform by analysing a handful of significant EU Court of Justice decisions.

5. SHORT COMINGS OF THE DPD

The DPD was quickly plagued by difficulties. Chris Hoofnagle argues that the DPD did not completely integrate national privacy regulations, and even within Europe, nations acted opportunistically to woo big tech with signals of lax enforcement and lucrative tax structures.[466] Among nations devoted to privacy, enforcement was still poor, with the French fining Facebook just 150,000 euros in 2017.[467] This enforcement void gave Europe the reputation of a place with regulations, but no actual police.[468]

Since this was a directive and not a regulation, EU Member States were required to establish their own laws to implement its objectives.[469] Directives are EU's edicts that require member states to create national law in accordance with the DPD (by a process known as

[463] Neil Robinson et al op cit note 436. See also Kuner op cit note at 361 at 10f.

[464] Ibid.

[465] Ibid.

[466] Chris Jay Hoofnagle et al op cit note 5 at 71.

[467] Ibid.

[468] Ibid.

[469] David Bender 'GDPR Harmonisation: Reality or Myth?' (2018) last accessed from *https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/* on 27 June 2022.

'transposition'). [470] Member states incorporated their own bells and whistles while implementing the DPD. [471] Inconsistencies produced complexity, legal ambiguity, and administrative costs. [472] This affected people's confidence, trust, as well as the economic edge of the EU's economy. The 'harmonisation' brought about by the DPD consequently fell far short of what the EU envisaged. A regulation like the GDPR, however, is not required to be transposed, like a directive.

Other than the issue of divergence in enforcement between various Member States, the EU DPD has been in place since 1995.[473] In an environment as dynamic as the internet, this means that the DPD has become archaic, especially with the significant changes that have occurred since the commercialisation of the internet in the mid-1990s.[474] As the realities of data collection, processing, storage, and use evolved, it became increasingly clear that digital technologies brought with them, in addition to their benefits, hitherto unforeseen privacy threats.[475]

In EU circles, the ease with which data may flow across borders has been a particular cause of concern. To provide context for the views about the regulation of TBDF, it is important to recall the goals of Article 4 as stated in the travaux préparatoires and the preamble of the Directive.[476] These objectives are twofold: (1) to avoid a scenario in which the data subject is outside any system of protection, and (2) to avoid a situation in which the same data-processing activity is controlled by the laws of multiple countries' enforcement void.[477] This gave Europe the reputation of a place with regulations but no actual police.[478] This part provides a chance for reflection on whether the DPD was able to achieve its stated objectives.

[470] Foivi Mouzakiti op cit note 452 at 46.

[471] Bender op cit note 468 at 39.

[472] Ibid.

[473] Mira Burri et al op cit note 92 at 480.

[474] Ibid.

[475] Ibid.

[476] Ibid.

[477] Ibid.

[478] Ibid.

The difficulties of implementing privacy legislation in third-party countries have become very clear. It goes without saying that when the DPD was enacted, the internet was still growing, and we now live in a world where all of this is becoming particularly crucial. There was, and presently is, a need for greater protections that provide effective outcomes in practice. The problems posed by new technology and globalisation necessitate some inventiveness to provide more effective protection. To contextualise practical situations that challenge the efficacy of data protection, we consider the fundamental distinction between two kinds of TBDF and highlight the inefficiency of the DPD that will be discussed below. [479]

With respect to the preceding, the first scenario is typical and prevalent.[480] A person, a firm, or administration in Europe exports data for a variety of reasons, such as to fulfill a contract on behalf of a client, to ensure in a third country the processing of certain technical applications (back up or storage of data), to build a common database of employees in multiple countries, etc. [481] The second scenario is less obvious; owing to the global nature of modern networks and the lack of infrastructural boundaries, individuals from outside the EU may directly compromise the privacy of EU citizens by propagating malware, conveying data to third parties via invisible hyperlinks, or addressing unsolicited letters over the internet, etc.[482] The latter case differs from the first since the privacy problems are directly caused by foreign parties (not established in the EU), and not the European data controllers.[483]

According to Poullet, the distinction between the two TBDF hypotheses will result in differing provisions.[484] The first circumstance is governed by the General DPD and its two guiding principles, as stated in Recitals 56 and 57: '*Whereas the protection of individuals guaranteed in the Community by this Data Protection Directive does not prevent transfers of personal data to third countries which ensure an adequate level of protection;* '[485]The latter circumstance is, however, not covered by the DPD.

---

[479] Yves Poullet op cit note 312 at 144.

[480] Ibid.

[481] Ibid.

[482] Ibid.

[483] Ibid.

[484] Ibid.

[485] Last accessed from *https://eur-lex.europa.eu/legal-co tent/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN* on 26 June 2022.

As was mentioned in the preceding section, the DPD was drafted at a period when data processing utilised file systems and computer mainframes.[486]Technically speaking, the DPD did not cover instances of data processing outside the EU's territorial borders. However, the first form of extraterritorial extension of EU data protection is judicially driven.[487] A case in point is the *Google Spain case*[488] which demonstrated a trend toward expanding the territorial reach of the application of EU data protection legislation to include controllers with a principal establishment outside the EU.

In Google Spain, the CJEU interpreted for the first time the provision of the DPD specifying its geographical scope (Article 4) to extend the application of EU data protection law to a US-based, non-EU data controller.[489] In the Weltimmo case, the Court reaffirmed the Google Spain case's expansive approach to territoriality and emphasised a general attitude of flexibility toward the entirety of Article 4(1)a:[490]

> '[I]n the light of the objective pursued by Directive 95/46, consisting of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, the words 'in the context of the activities of an establishment' cannot be interpreted restrictively.'[491]

While the EU DPD regime expressly allows for two possibilities for the application of EU data protection law to a controller established in a third country, either on the basis of the use of equipment within the EU[492] or pursuant to public international law in terms of Article 4(1)*(c)*, neither of these options is intended to include the processing of data performed outside

---

[486]Neil Robinson et al op cit note 436.

[487] Maja Brkan 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23 *Maastricht Journal of European and Comparative Law*812-841 at 829. See also Burri et al op cit note 92 at 482 and Gomann, M op cit note 81 at 570.

[488] *Case C-131/12, Google Spain SL v. Agencia Espan˜ola de Proteccio´n de Datos (AEPD)*

[489] Emmanouil Bougiakiotis 'One law to rule them all? The reach of EU data protection law after the *Google v CNIL* case' (2021) 42 *Computer Law & Security Review* 1-13 at 2.

[490] Paul de Hert & Michal Czerniawski 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 *International Data Privacy Law* 230-243 at 233.

[491] *Case C230/14 Weltimmo sro v Nemzeti Adatvedelmi és Információszabadság Hatóság at para 25.*

[492]Article 4(1)(b)

of the EU.[493] Rather, rationally based on the preliminary question presented by the referring court, the CJEU read Article 4(1)*(a)* of the DPD to require compliance with the DPD if data is processed "in the course of the operations of the controller's establishment inside the EU.[494] While a textual interpretation of this article may not include processing outside of EU territory, the Court relied on a teleological interpretation of this provision to establish that the DPD should have a 'particularly broad territorial scope' in order to prevent data subjects from being deprived of the protection provided by the Directive. [495]

6. SAFE HARBOUR AGREEMENT AND THE SNOWDEN REVELATIONS: A WAKE-UP CALL FOR THE GDPR

According to Foivi Mouzakiti, the architecture of the EU DPD has been unable to meet the demands of the twenty-first century.[496] The EU Commission announced a data protection reform in 2012 that is a top priority for its legislative agenda. Nonetheless, it is the 'Snowden revelations' that propelled the regulation of transborder data transfers to the forefront of the data protection conversation. Since then, there have been numerous discussions regarding the legitimacy of the so-called Safe Harbour Agreement.[497]

As it has been noted in Chapter 2, the US and the EU have traditionally held widely differing views on data privacy.[498] While the US was adopting sectoral data privacy laws, the EU turned to omnibus legislation, instead. Notably, the EU did not deem the safeguards provided by US law to be 'adequate'.[499] This is even though the EU-U.S. economic connection is estimated to entail $260 billion in yearly digital services trade.[500] At the time, disparities in

[493] Maja Brkan op cit note 486 at 830.

[494] Ibid.

[495] Ibid.

[496] Foivi Mouzakiti op cit note 452 at 39.

[497] Rossi Augustin op cit note 416 at 100.

[498] Avner et al op cit note 262 at 357.

[499] Foivi Mouzakiti op cit note 452 at 39.

[500] Paul M Schwartz op cit note at 179. See also Penny Pritzker and Andrus Ansip 'Making a Difference to the World's Digital Economy' (2016) last accessed from *https://www.commerce.gov/news/blog/2016/03/making-difference-worlds- digital-economy-transatlantic-partnership [https://perma.cc/QS9J-M3P3]* on 11 July 2022.

the regulatory environment of the world's biggest trading blocs, threatened critical international data flows.[501]

Against this background, in 2000, the Safe-Harbour Agreement was adopted. It was created to guarantee that US corporations adequately respect the privacy of EU consumers when processing their data domestically.[502] De facto, albeit not de jure, this was a decision made by the Commission, which designated businesses as 'safe harbours' if they agreed to adhere to specific data protection rules and submit to the US Federal Trade Commission ('FTC') oversight.[503] It has been established that in the fifteen years of the agreement's existence, just four allegations of violations from EU data protection authorities have been received.[504] Critics point out that the small number of legally significant cases may also indicate the Safe Harbour's limited effectiveness because it makes it more difficult for impacted people to file complaints.[505]

While there has long been a controversy over the effectiveness of the Safe Harbour, the 'Snowden revelations' regarding the wholesale surveillance of EU citizens by the NSA brought the agreement under scrutiny. The 2013 revelations by Edward Snowden that revealed the scope and depth of surveillance by the United States National Security Agency were unquestionably an important, albeit unrelated, development (NSA).[506] The Washington Post and The Guardian unveiled top-secret information leaked by an unidentified NSA whistleblower on June 7, 2013. Shortly afterward, Edward Snowden was identified as the whistleblower.[507]

They revealed that the NSA in the United States and the General Communications Headquarters (GCHQ) in the United Kingdom were actively collecting data from the databases of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple, and other

[501] Ibid.

[502] Ibid.

[503] Ibid.

[504] Susan Landau 'Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations' (2014) 12 *IEEE Security & Privacy* 62-64 at 62.

[505] Rossi Augustin op cit note 416 at 104.

[506] Ibid.

[507] Ibid.

(US-based) internet players.[508] Consequently, as per the allegations, a number of electronic communications corporations that participated in the Safe Harbour program employed a variety of security mechanisms that monitored, collected, and processed the personal data of EU citizens. Timothy Garton Ash, a renowned British historian, wrote in The Guardian in June 2013:

> 'Edward Snowden's revelations about massive data-mining by American and British spying agencies show that most of the sources they are digging into are privately owned [. . .]. This commercial accumulation of intimate personal information is worrying. The reassurance we are offered from Facebook, Google and others – "trust us" – is not good enough. After all, it now turns out they've been sharing some of it with the spooks.'[509]

In response to these revelations, the European Parliament ('EP') directed the LIBE Committee to investigate extensive electronic surveillance of EU citizens.[510] Commenting on the revelations, Foivi Mouzakiti rightfully argues that the notion of an 'Orwellian world' has no place in a democratic society.[511] Similarly, Professor Schwartz argues that, when widespread and covert surveillance becomes the norm, the act of speaking or listening will no longer be private.[512] To this end, during the voting process of the EU data protection reform, the LIBE Committee made it quite apparent that the proposed reforms, especially those pertaining to data transfers to nations outside of the EU economic area, were a response to 'the mass surveillance operations' unveiled by the media.[513] Thus, it is clear that these events led to the erosion of trust between the EU and the US in respect of transatlantic data flows.[514]

Similarly, following the Snowden revelations, Max Schrems, an Austrian attorney, filed a complaint against Facebook in 2013 to prevent the transfer of personal data from Ireland

---

[508] Ibid

[509] Ibid at page 105.

[510]Commission, Press Release, [P/I 2/46] 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses'(2012) last accessed from *https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46* on 19 July 2022.

[511] Foivi Mouzakiti op cit note 452 at 40. An 'Orwellian world' is described as a political system in which the government tries to control every part of people's lives.

[512] Paul M. Schwartz 'Privacy and Democracy in Cyberspace' (1999) 52 *Vanderbilt Law Review* 1609-1701 at 1651.

[513] Commission, Press Release op cit note 476.

[514] Ibid.

to the United States.[515] The lawsuit was filed because of Edward Snowden's disclosures, including the accusation that Facebook USA cooperated in the NSA's PRISM monitoring program. Schrems stated that the absence of adequate safeguards violated the Irish Data Protection Act and the EU DPD.[516] In this case, on October 6, 2015, the CJEU invalidated an earlier EU-U.S. data-sharing framework, the Safe Harbor Framework. The courts found that it did not provide privacy protections 'substantially equivalent' to those granted by EU legislation for EU data subjects.[517]

This section has examined the EU's 1995 DPD, which ensures the protection of citizens' fundamental data protection rights. Less than twenty years after its enactment, EU policymakers deemed the 1995 DPD to be obsolete.[518] The framework for TBDF in the EU, which is 20 years old, could not handle the requirements of the 21st century.[519] What was once a positive development is now an obsolete piece of legislation. Since 1995, the average person's life has shifted from occasional internet use to one that is inextricably linked to information technology. This part introduced the drivers of the reform by examining legal scholarship on the matter and several significant EU Court of Justice decisions.

Divergence in transatlantic legislative frameworks for data protection is not a phenomenon peculiar to the last decade.[520] Ongoing advances in borderless disruptive technologies, like cloud computing, heighten the possibility of conflicts in the different regulatory approaches.[521] If that is not problematic enough, the Snowden revelations made the reform even more imperative. Rossi Agustin argues that Snowden's revelations of rampant spying altered the discourse around the GDPR in the EU Parliament.[522] Prior to the revelations, corporations influenced the privacy landscape in Europe.[523] But when Snowden's revelations

[515] Mira Burri et al op cit note 92 at 485.

[516] Supra note 388.

[517] Ibid.

[518] Rossi Augustin op cit note 416 at 100.

[519] Foivi Mouzakiti op cit note 452 at 39.

[520] Edoardo Celeste et al op cit note 321 at 44.

[521] Ibid.

[522] Rossi Augustin op cit note 416 at 104.

[523] Ibid.

exposed the graveness of internet privacy issues, the influence of companies declined.[524] Ultimately, privacy activists were able to incorporate their views into the GDPR's final text.[525]

The Snowden revelations were very instrumental in shaping the nature and scope of the GDPR. In this context, the following section examines the key regulatory changes that the GDPR implements, evaluates their implications, and attempts to contextualise them within the broader context of the digital economy and its stewardship, particularly regarding the free flow of data.

7. THE GENERAL DATA PROTECTION REGULATIONS

According to Buri, after roughly five years of intense work, followed by heated political debates and widespread social endorsement, the EU's data protection reform has finally become a reality.[526] The EU passed the GDPR on April 14, 2016, as part of its Digital Single Market Strategy.[527] The GDPR superseded the antiquated DPD from 1995 and became effective on May 25, 2018.[528] A key objective of the EU's GDPR is to reconcile or bring the data protection legislation of the 28 EU Member States into accord with one another. Technically speaking, the GDPR is a Regulation according to Article 288(2) of the Treaty on the Functioning of the European Union ('TFEU').[529]

The GDPR is the EU's response to the problems posed by the outdated Data Protection Directive, as mentioned in the previous section. Thus, the difficulties posed by technological

---

[524] Ibid.

[525] Ibid.

[526] Mira Burri et al op cit note 92 at 479. See also Paul de Hert & Vangelis Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer law & security review* 179–194 at 179.

[527] Christina Breunig & Martin Schmidt-Kessel 'Data Protection in the Internet: National Report Germany' in Dário Moura Vicente and Sofi a de Vasconcelos Casimiro (Eds) *Data Protection in the Internet* (2020) at 183.

[528] Ibid. Under Article 88, DPD 95/46 is repealed and references to it are to be construed as references to the Proposed Regulation. See Kristopher Kuner 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) 11 *Privacy & Security Law Report* 1-15 at 14. Damian A. Tamburri 'Design Principles for the General Data Protection Regulation (GDPR): A formal Concept Analysis and its Evaluation' (2020) *91Information Systems* 1-14 at 3.

[529] Jonas Baumann and Nazreen Ismail 'The (Extra-)territorial Scope Rules of the New European Data Protection Law from a Private International Law Perspective—A Model for South Africa?' (2021) 54 *Comparative and International Law Journal of Southern Africa* 1-49 at 5.

advancements and globalization necessitate a great deal of inventiveness in order to provide more adequate protection.[530] The GDPR was created with two major goals in mind.[531]First, to address the need for modernised and enhanced data protection regulations capable of protecting EU data subjects against the privacy challenges of the 21st century, such as the recent surveillance activities discussed above.[532] Second, to present a set of well-defined, coherent, and adaptable rules.[533] The second purpose supports the transition from a DPD to a Regulation, which is directly applicable to all members.[534] A Regulation to replace the 1995 DPD implies, prima facie, that prior harmonisation issues will cease to exist.[535] After highlighting the fundamental flaws of the 1995 Data Protection Directive, the following sections will assess whether the reform addresses these deficiencies while achieving its objectives.

*7.1 Long Arm of the GDPR: Redefining the Territorial Scop*e

In May 2018, the EU adopted the GDPR, which broadened the territorial scope of the EU data protection law to cover some processing activities of data processors and controllers in foreign countries.[536] Many see this as a major step forward in terms of protecting people's fundamental rights and levelling the playing field for businesses competing in the EU's market.

Personal data presents various regulatory dilemmas. For example, if companies are able to freely transmit personal information out of the EU to 'data havens' where there are no regulations or weak regulations, the EU's privacy efforts will fail.[537] Just like the DPD, the GDPR places restrictions on the transfer of personal data beyond the EU.[538]According to the recently published guidelines by the European Data Protection Board ('EDB') on Guidelines on the territorial scope, Article 3 of the GDPR establishes the territorial scope of the

[530] Foivi Mouzakiti op cit note 4452 at 46.

[531] Ibid.

[532] Ibid.

[533] Ibid.

[534] Ibid.

[535] Paul de Hert et al op cit note 525 at 180f.

[536] Merlin Gömann op cit note 97 at 567.

[537] Chris Jay Hoofnagle et al op cit note 5 at 73.

[538] Ibid.

Regulation, which marks a substantial advancement of EU data protection law compared to the framework established by the DPD.[539] In part, the GDPR upholds decisions reached by EU legislators and the CJEU in the context of the DPD.[540] Nonetheless, salient new features have been included, which provide for a broader territorial scope that will be discussed in this section. With that said, Article 3 states, inter alia, that:

> '(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> (2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b)the monitoring of their behaviour as far as their behaviour takes place within the Union..'[541]

It is worth noting that the territorial scope of the updated Council of Europe Convention 108 (Convention 108+) is also in the same orientation.[542] These developments at the EU and Council of Europe levels are consistent with the EU Court of Justice's ruling on the territorial scope of the DPD in the Google Spain case. According to Paul de Hert, Article 3(2) of the GDPR transcends territoriality by basing its territorial reach on the destination approach. [543] In addition, there must be a significant relationship between the activity and EU territory. Article 3(2) of the GDPR is seen by insiders as one of the more important 'achievements' of the reform.[544]

Whilst the primary goal of Article 4 of the DPD was to define which national law of a Member State is applicable, Article 3 of the GDPR defines the territorial scope of a directly

---

[539] EDB Guidelines op cit note 86.

[540] Ibid at 4.

[541] Official text last accessed from *https://gdpr-info.eu/* on 29 September 2022.

[542] Paul de Hert op cit note 489 at 230.

[543] Ibid. See also Google Spain supra note 453. and Weltimmo supra note 456.

[544] Ibid at 238. See also Graça Canto Moniz 'Finally: a coherent framework for the extraterritorial scope of EU data protection law' (2018) 4 *UNIO - EU Law Journal* 105-115 at 106.

applicable text.[545] In addition, while Article 4 of the DPD alluded to the 'use of equipment' on Union territory as a premise for bringing controllers 'not based on Community territory' within the scope of EU data protection law, no such reference appears in Article 3 of the GDPR. The latter reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirements, a level playing field for companies active on the EU markets, in a context of worldwide data flows.

Article 3 of the GDPR creates the territorial reach of the Regulation based on two key parameters: the 'establishment' criterion (Article 3(1)), and the 'targeting' criterion (Article 3(2)). If either of these conditions is met, the applicable GDPR regulations will apply to the relevant processing of personal data by the controller or processor concerned. In addition, Article 3(3) confirms the applicability of the GDPR to processing where Member State law applies under public international law.

While the term 'primary establishment' is specified in Article 4(16), 'establishment' is not defined for the purposes of Article 3(1). Nonetheless, Recital 22 specifies that 'establishment' implies: 'the effective and real exercise of activities through stable arrangements.'[546] The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.[547] For example, an automobile manufacturer with headquarters in the United States has an office in Berlin that oversees all its operations in Europe, including marketing and advertising. Considering the nature of the automobile manufacturer's economic activity, the Berlin branch can be regarded as a stable arrangement that engages in actual and effective operations. Consequently, the Berlin branch could be regarded as an establishment in the Union for the purposes of section 3(1) of the GDPR.

In relation to the targeting criterion established by Article 3(2) of the GDPR, seeks guarantee that individual personal data is still safeguarded in a global data economy. EU legislators have established safeguards, such that all data processors must adhere to the GDPR if processing the personal data of European consumers under the *lex locus solutionis* (law of the place where the relevant performance occurs). This definition is significant because it

[545] Ibid.

[546] Ibid.

[547] Recital 22 of the GDPR.

expands the territorial reach of European data protection laws beyond 'data controllers' and 'data processors' who are not established in the EU.

As noted in the preceding section, Article 3 of the GDPR applies to all data controllers and processors inside and outside the EU who process the personal data of EU residents. Target-based jurisdiction is new to EU data protection legislation.[548] It is undoubtedly a component of what Kuner refers to as the 'Copernican revolution'.[549] Consequently, the GDPR's reach is extended to encompass the whole world, inclusive of all data processors who process data of European citizens regardless of their location. This notion is known synonymously as 'extraterritoriality', 'extraterritorial application', or 'extraterritorial jurisdiction', which can be bluntly described as an application of the law that seeks to control, or directly affect the activities of an object outside of the territorial borders of the state making the assertion.

The precise naming of Article 3(2) of the GDPR remains elusive. As a result, some scholars refer to Article 3(2) as the 'targeting test'[550] while others refer to it as the 'marketplace principle'.[551] Because there is no settled term for Article 3(2) for the purposes of this dissertation, the two terms will be used interchangeably. Firstly, as noted above, extraterritoriality is foreseen in cases of offering goods or services in the EU from abroad in Article 3(2)*(a)* of the GDPR.[552] This is an example of targeting. Non-EU actors are brought under the GDPR when they offer goods or services to EU data subjects.[553]

Secondly, Article 3(2)*(b)* clearly intends to apply to third-country operators of social networks, online suppliers of services such as e-mail accounts, operators of search engines and websites, the vast majority of which habitually monitor the behaviour of internet users.[554] The

[548] Paul de Hert op cit note 489 at 238.

[549] Ibid.

[550] See EDB Guidelines op cit note 86 at 14, Dan Jerker B Svantesson op cit note 77, Paul de Hert op cit note 440 and Benjamin Greze 'The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives' (2019) 9 *International Data Privacy Law* 109-128.

[551] Christina Breunig et al op cit note 526 at 209. See also Gilad Katzav 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Personal Information Act' (2022) 139 *SALJ* 432-470 at 433ff.

[552] Paul de Hert op cit note 489 at 238.

[553] Ibid.

[554]Ibid.

nature of the processing activity which can be considered as behavioural monitoring is further specified in Recital 24 which states that:

> '[I]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours, and attitudes.'[555]

According to the European Data Protection Board ('EDB'), the applicability of Article 3(2)(b) when a data controller or processor observes the behaviour of data subjects within the Union might potentially embrace a wide variety of monitoring operations. This may include in behavioural advertisement, geo-localization operations, particularly for marketing, online tracking via cookies or other measures such as fingerprinting, online services for personalised nutrition and health analytics – CCTV, market research and other behavioural studies based on specific personas, and monitoring or frequent reporting on the health condition of a person.[556]

The EDB has recently clarified that the need for the data subject to be situated in the Union must be assessed at the time when the relevant trigger activity occurred, i.e. when goods or services are offered or when behaviour is observed, independent of the duration of the offer made or monitoring done.[557] The EDB further clarified that, in connection to processing activities relating to the provision of services, the provision is directed at actions that actively, rather than unintentionally or incidentally, target EU citizens.[558] As a result, if the processing relates to a service that is solely available to persons outside the EU but is not removed when such individuals enter the EU, the GDPR will not apply to the processing.[559]

The effect of this on global scale is that any non-compliance with the GDPR results in penalties of up to €20 million, or 4% of annual turnover. This is not a theoretical notion, but a reality. To date, a substantial number of fines have already been issued on several international

[555] EDB Guidelines op cit note 86 at 19.

[556] Ibid at 20.

[557] Ibid at 15.

[558] Ibid.

[559] Ibid.

corporations, including Google[560], Facebook[561], Uber and Equifax to name a few.[562] Numerous multinational corporations that conduct business in the EU or deal with the personal data of EU citizens will therefore be subject to this new regulation. As of this writing, Advocate General Saugmandsgaard's brief observation Schrems II, delivered on December 19, 2019, represents the most recent engagement with Article 3 in a case before the CJEU. He stated that:

> *'[P]ursuant to Article 3(1) of the GDPR, that regulation shall apply to any processing carried out in the context of the operations of an establishment of a controller or processor in the Union, irrespective of whether the processing occurs in the Union or not.'*[563]

7.2 The Conundrums of Extraterritorial Enforcement: Mission Impossible?

The inclination toward exercising extraterritorial jurisdiction in data protection and the regulation of TBDF is anticipated to place the topic of enforcement at the forefront of public discourse.[564] Benjamin Greze and others have claimed that the GDPR's extraterritorial reach and article 3(2), disregard the enforcement component.[565] Others, however, have referred to this as 'bark jurisdiction' when the prospect of TBDF enforcement is neither genuine nor severe.[566]

---

[560] The French data protection regulator (CNIL) issued a hefty fine to Google Ireland on January 6, 2022. The fine pertains to how YouTube's cookie consent processes are implemented by Google Europe. The Google Ireland fine was one of two penalties issued in the same case; the other was made against Google LLC of California (which operates Google Search) last accessed from *https://www.tessian.com/blog/biggest-gdpr-fines-2020/* on 01 September 2022.

[561] Ibid. The French data protection regulator, CNIL, imposed Facebook's second largest GDPR penalties on January 6, 2022. This €60 million fine was imposed on the social media powerhouse for failing to secure adequate cookie consent from its users. Concerns centred mostly on the ambiguous way Facebook offered a cookie opt-out.

[562] Paul de Hert op cit note 489 at 238.

[563] *C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*

[564] Benjamin Greze op cit note 549 at 109.

[565] Ibid.

[566] The term 'bark jurisdiction' emenates from the English idiom, 'all bark and no bite' which literally means that someone (in this instance the law) is full of big talk but lacking action, power, or substance.See also Dan Jerker B. Svantesson op cit note 103 at 83ff.

Despite the enforcement problems, the benefits of the extraterritorial reach of the GDPR are two-fold. First, there is symbolic value in seeking to regulate globally, and second, it has a deterring effect on foreign firms.[567] To achieve the desired consequences of legislation, however, a credible enforcement threat is essential.[568] Uta Kohl has argued that 'it is enforceability that really matters, not actual enforcement'.[569] In addition, the impact of reputational harm in the case of non-compliance should not be underestimated, as the infamous Yahoo! Inc. discussed earlier in this research has illustrated.[570] Fascinatingly, Yahoo! Inc. cooperated with the French ruling notwithstanding the absence of a credible threat of enforcement in the United States.[571]

While enforcement is often seen as the data protection law's Achilles heel, it is not entirely ineffectual. In contrast, according to Brian Daigle and Mahnaz Khan, a review of data on GDPR penalties between 2018 and 2021 suggests that the biggest fines issued to date for GDPR non-compliance were assessed against U.S.-based corporations, particularly those in the technology sector.[572] They contend that EU DPAs have expanded their enforcement activities against US technology firms, notably in 2020-21, therefore increasing the frequency and severity of GDPR-compliant fines.[573] Corporations in the United States have seen that EU DPAs are no longer afraid to deploy harsh enforcement against large technology companies and other significant organisations.[574]

---

[567] Ibid at 112.

[568] Ibid.

[569] Uta Kohl op cit note 102 at 205.

[570] Supra note 83.

[571] Benjamin Greze op cit note 549 at 109f.

[572] Brian Daigle and Mahnaz Khan 'The Changing Tides of Data Protection Regulation and Enforcement in Europe'(2022) last accessed from *https://www.usitc.gov/publications/332/working_papers/changing_tides_of_gdpr_enforcement_trends_final-compliant_1.pdf* on 03 September 2022.

[573] Ibid.

[574] Ibid.

7.3 Ex ante Adequacy Requirements for TBDF

If information can simply be moved to a 'data haven' with fewer or no restrictions, the EU's strict data protection regulations may be rendered futile.[575]As a result, the GDPR creates a framework for data transfers across borders. By default, the GDPR allows for the conditional transfer of data. Exports are authorised where the EU has determined that the third country provides a sufficient level of protection. This is also known as ex-ante adequacy requirements.[576] The GDPR then specifies what criteria should be used to determine whether a jurisdiction offers enough protection for personal data. The three-step exam includes considerations such as:

> '(i) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including public security, defence, national security, and criminal law as well as effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred; (ii) existence and effective functioning of one or more independent supervisory authorities; and (iii) international commitments the third country has entered into in relation to the protection of personal data.'

Despite being extensive, the rules can be summed up as follows. In two circumstances, transfers are permitted. The EC can assess the legal systems of other nations and determine if they are adequate. To date, only eleven jurisdictions-Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay-have received the Commission's approval. Such approval is typically only conferred following protracted negotiations in which the concerned nation updates its domestic data protection laws to a level that is almost as protective as the EU's data protection regulations. This relates to Article 45, which, among other things, states that:

> *'A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.'*

As stated previously in this chapter, the US and the EU are the world's biggest net exporters of digitally enabled services. The EC adopted the 'Privacy Shield' after the invalidation of the

[575] Chris Jay Hoofnagle et al op cit note 5 at 73.

[576] Jan Xavier Dhont 'Schrems II. The EU adequacy regime in existential crisis?' (2019) 26 *Maastricht Journal of European and Comparative Law* 597-601 at 598f.

Safe Harbor Framework (because of Schrems I). Since 2016, the EU-U.S. Privacy Shield has enabled these transfers by implementing safeguards and protections for the privacy of EU data subjects. In July 2020, the European Court of Justice in Schrems II once again invalidated the Privacy Shield for being inconsistent with European Union data protection laws.[577]

In Shrems II, the CJEU found that US data monitoring legislation did not give similar protections to those in the European Union and was inconsistent with EU rights, such as Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333.[578] In light of the ruling, the Privacy Shield Agreement no longer permits the transfer of personal information. In the aftermath of Schrems II, the United States and the EC announced on March 25, 2022 that they have reached an agreement in principle on a new 'Trans-Atlantic Data Privacy Framework' that will promote trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in its Schrems II ruling in July 2020.[579]

The Trans-Atlantic Data Privacy Framework is the result of over a year of exhaustive talks and represents an unprecedented commitment by the United States to undertake reforms that would increase the privacy and civil liberties protections applicable to US signals intelligence activities.[580] Ultimately, these impending reforms will support all commercial transfers of EU personal data to the United States, including those based on the EU-US Privacy Shield, Standard Contractual Clauses, and Binding Corporate Rules. Moreover, the Trans-Atlantic Data Privacy Framework will enable the EC to make a new adequacy decision, which will authorize the transfer of EU personal data to the United States in accordance with EU legislation under the EU-US Privacy Shield.[581]

8. CONCLUSION

This chapter examined the development of EU data protection laws. It defined its fundamental objectives and underpinnings. It chronicles the beginnings of Europe's data

[577] Supra note 524.

[578] Ibid.

[579] European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework last accessed from *https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087* on 13 September 2022.

[580] Ibid.

[581] Ibid.

protection laws from the Holocaust, one of the darkest episodes in human history. In the 1950s, Germany and Sweden became the first European nations to implement privacy legislation in response to these events. However, there was limited EU-level harmonisation of these laws. As the chapter notes, these disparities impeded the growth of the domestic market. In this context, the DPD was designed to ease cross-border business by harmonising EU data protection rules.

As shown in this chapter, the right to data protection is a bona fide fundamental right with autonomous worth. The jurisprudence of the ECHR and ECJ on the right to data protection was examined in greater detail. Data protection has been the subject of significant ECJ case law, and the Court's data protection-related jurisprudence has witnessed a dramatic shift. In recent years, some of the most significant advances in European data privacy law have been witnessed since the European Union implemented the DPD in 1995. These include the adoption of the GDPR by the EU, the invalidation of the US–EU Safe Harbor Agreement by the Schrems I decision, its subsequent replacement by the Privacy Shields (invalidated by Schrems II), and lastly, its latest replacement by the Trans-Atlantic Data Privacy Framework of 2022.

The chapter discusses the EU's 1995 Data Protection Directive. From its early years, the DPD was riddled with problems, most of them attributable to the borderless nature of the internet. Subsequently, the DPD was replaced by the GDPR. Nonetheless, despite worries about the Directive's jurisdictional restrictions, the Luxembourg courts did not hesitate to create new rights for data subjects and give DPAs more authority within the scope of their novel and daring interpretation of the Directive.[582] Through several seminal court judgments, they established the right to be forgotten, widened the territorial scope, declared the Safe Harbour agreement inadequate, and other issues.[583]

In part, the GDPR upholds decisions reached by EU legislators and some judgments of the CJEU in the context of the DPD.[584] Nonetheless, one of the salient elements is that the GDPR's territorial reach is broader than that of the Data Protection Directive. This dissertation will propose that Section 2 of the Namibia Data Protection Bill should be aligned with Article 3(2) of the GDPR. Thus, the dissertation endorses the targeting test/market principle and urges

[582] Yves Poullet op cit note 312 at 775.

[583] Ibid.

[584] Ibid.

a broader geographical scope for Namibia. This will allow for data protection to travel with the data wherever it winds up in a globalised world.

Furthermore, it has been noted that most nations around the world have widely embraced EU personal data protection principles. The 1995 Directive, the forerunner of the current GDPR that went into effect in 2018, has served as the ‘legal blueprint’ for many countries' legislation. The degree of adoption varies, with some nations closely adhering to the DPD (and consequently the majority of the GDPR), while others have only adopted key components. Around 75 non-European countries passed EU-style laws as of 2018, and more than ten of them had adopted the new GDPR principles.

South Africa, Namibia's neighbour, is one of the 75 nations that has adopted EU-style data privacy legislation. As indicated in chapter 1, Namibia and South Africa are not only neighbours, but they are also developing members of SADC, demonstrating a degree of integration based on comparable economic and social systems. The League of Nations gave South Africa legislative control over Namibia from 1920-1990. Today, South African, and Namibian privacy regulations are almost identical. This comparative analysis would be incomplete without examining South Africa's advancements in data protection and TBDF. The next chapter explores the theoretical, legal, and policy underpinnings of South Africa's Data Protection Law.

CHAPTER 6

Data Protection in South Africa: A Comparative Study

1. INTRODUCTION

Data protection legislation stems from technology and information usage. Slowly, countries, particularly in Europe, realised the perils of rapid technological advancement. Both substantive and procedural data protection rules have been adopted.[585] Numerous nations around the world followed suit in the years to come, including South Africa. Gilad Katzav says that the Protection of Personal Information Act, 2013 (4 of 2013) ('POPI Act'),[586] closely styled after EU developments in this field, is South Africa's legislative response to data processing operations. It demonstrates a strong commitment to protecting the right to privacy.[587]

Before the POPI Act, there wasn't a specific law in South Africa that protected personal data.[588] The common law, the constitution, and a few specific pieces of legislation in South Africa's legal system recognise some, albeit limited, forms of data protection.[589] Example, the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002),[590] the National Health Act 61 of 2002[591], the Consumer Protection Act 68 of 2008.[592] Additional to these is section 14 of the South African Constitution, which states:

> '[E]veryone 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.'

Although in South Africa, the recognition of privacy as a fundamental human right was enshrined in the South African Constitution in 1996, including informational privacy. Alas, the

---

[585] Gilad Katzav 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Personal Information Act' (2022) 139 *SALJ* 432-470 at 433.

[586] Promulgated in GEN 912 GG 37067/26-11-2013.

[587] Gilad Katzav op cit note 584 at 433.

[588] Ibid.

[589] Ibid.

[590] ss 50–1

[591] ss 14–17

[592] ss 51(1)*(j)(ii)*, 51(2)*(b)(ii)* and 107(1)

framework for guaranteeing informational privacy would not become a reality for another 20 years with the passing of the POPI Act on 1 July 2020.[593] The POPI Act was drafted largely on the recommendations of the South African Law Reform Commission ('SALRC').[594] In its discussion paper on privacy and data protection, the SALRC highlighted the importance of privacy in terms of the constitution and common law.[595] It further noted that while privacy is a fundamental right, it can be limited and balanced against economic and trade considerations. Data privacy should not only be seen as a domestic policy issue but also as a global issue.[596] On November 17, 2000, the SALRC took the first step toward enacting an omnibus piece of legislation dealing with the protection of personal data.[597]

This chapter comparatively examines the theoretical, legislative, and policy foundations of the South African Data Protection Law. It seeks to answer questions pertaining to the regulation of TBDF and the basis or rationalisation of the South African data protection regime. Whilst the author of this paper acknowledges that the South African jurisprudence on privacy and data protection is undoubtedly still evolving, as indicated in chapter 1, the demonstrable a degree of integration between Namibia and South Africa based on comparable economic and social systems makes it ideal.

2. THE RIGHT TO PRIVACY IN SOUTH AFRICA

As it has been argued many times in this paper, data protection law safeguards the right to privacy. This privacy-thinking is made plain in the SALRC's 2009 Report on Privacy and Data Protection.[598] After traversing the extant privacy laws in South Africa, the report asserts that 'data protection should be seen as a specific application of the conventional principles' that

[593] Elizabeth De Stadler et al op cit note 110 at 1.

[594] Lukman Adebisi Abdulrauf 'Data Protection in the Internet: South Africa' in Dário Moura Vincente and Sofia de Vasconcelos Casimiro (eds) *Data Protection in the Internet* (2020) at 350.

[595] Ibid.

[596] Ibid.

[597] Ibid.

[598] South African Law Reform Commission Discussion Paper 109 Privacy and Data Protection last accessed from *https://www.justice.gov.za/salrc/dpapers/dp109.pdf* last accessed on 23 July 2022. See also Gilad Katzav op cit note 465 at 433.

have been enhanced through legislative enactment.[599] As noted in the introduction, the right to privacy is safeguarded in South Africa by both the common law and section 14 of the Constitution.[600] The constitutional entrenchment of the right to privacy as an inalienable basic human right underscores its importance. According to section 2 of the South African Constitution, the Constitution is the supreme law, and any law or conduct in conflict with it is invalid.[601]

For a discussion on the normative background of the right to privacy in South Africa, the comprehensive work of Neethling on personality rights and the right to privacy as expressed in the South African constitution serves as a useful starting point.[602] According to Neethling, privacy consists of all personal information pertaining to a person's state of seclusion. In this context, what is defined as a 'personal fact' is a result of self-determination and the subjective viewpoints of the specific individual. Neethling argues that self-determination is an essential element of the right to privacy.[603]Accordingly, he formulates his definition of informational privacy as follows:

> *'Privacy is an individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself [or herself] determined to be excluded from the knowledge of outsiders and in respect of which he [or she] has the will that they be kept private.'*[604]

The South African privacy laws are based on Neethling's definition of privacy, which was upheld in the case of *National Media v. Jooste*.[605] In this case, the court held that the right is a personality right.[606] The court further held that the law protects normal senses, not delicate ones.[607] Those with extreme discomfort aren't afforded the same privacy rights as others. The

[599] Ibid.

[600]Ibid.

[601] Ibid.

[602] Johann Neethling,J M Potgieter & Annelise Roos *Neethling on Personality* Rights (2019).

[603] Ibid at 46.

[604] Ibid.

[605] *National Media Ltd v Jooste 1996 (3) SA 262 at 271-272ff.*

[606] Ibid

[607] Ibid

court rules that unauthorised parties listening in on confidential conversations violated privacy. The court in this case defined privacy as:

> *'The right to privacy encompasses the right to determine the destiny of private facts, which includes the right to decide when and under what conditions private facts may be made public.'*[608]

Similarly, the South African Court in Investigating Directorate*: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*: In re Hyundai Motor Distributors (Pty) Ltd v Smit, held that section 14 of the Constitution could also be interpreted as protecting an individual's interest in his/her informational self-determination. Information self-determination is an interest in restricting the collection, use of and disclosure of personal information.[609]

In *Bernstein & others v Bester NO & others,*[610] Ackermann J. emphasised that no one right is absolute, and since every right is constrained by the maze of other conflicting individual and communal rights, each individual right is 'already limited by every other'. The court concluded that a person's right to privacy only encompasses his or her 'inner sanctum', including family life, sexual preferences, and home surroundings. This portion of a person's life is secured from being infringed upon by other people's rights that are different from it.[611] Similarly, in *Ministry v Interim Medical and Dental Council of South Africa*[612], the Constitutional Court also restricted informational privacy. The constraints include intimate data invasively obtained or misused. Other restrictions include not disclosing personal information to the media, the public, or anyone with whom the applicant has a reasonable expectation of privacy.

AmaBhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others is the latest notable iteration of the privacy

[608] Ibid par.271.

[609] Ibid.

[610] *Bernstein & others v Bester NO & others 1996 (2) SA 751 (CC).*

[611] Ibid.

[612] *Ministry v Interim Medical and Dental Council of South Africa, 1998 (4) SA 1127 (CC). (SA*

paradigm in South Africa.[613] The court ruled that the Regulation of Interception of Communications and Provision of Communication-Related Information Act ('RICA') was unconstitutional for many reasons. The court's reasons included the unreasonable infringement of the right to privacy by RICA. Madlanga J held that:

> *'[R]ICA enables communication intercepts. The sanctioned interception does not differentiate between personal and non-personal communications. It doesn't distinguish between useful and irrelevant information. Privacy is invaded throughout the continuum.'*

O'Keefe v. Argus Printing & Publishing Co. Ltd[614] demonstrates that an individual's right to privacy is based on the circumstances of a given case. The decision also emphasises the need for consent before utilising personal information. In this case, a photograph was published commercially. The damages were quantified in terms of the content, publishing extent, and type.

3. THE POPI ACT

According to Roos, South Africa enacted the POPI Act on July 1, 2020, following a protracted legislative process.[615] The POPI Act is an omnibus data protection law that conforms to the 1995 EU DPD, which served as the previous international data protection benchmark.[616] At the time of developing the Draft Bill which would ultimately become the POPI Act, the SALRC stressed the significance of a South African data-protection Act that corresponds with universal norms on data protection, particularly the EU's DPD.[617]

The constitutional rationale for POPI is to give effect to the right to informational privacy that protects individuals (known as 'data subjects') against the unlawful collection,

---

[613] *AmaBhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & others 2021 (3) SA 246 (CC).*

[614] *O'Keefe v Argus Printing and Publishing (Pty) Ltd 1954 3 SA 247 (C).*

[615] Anneliese Roos op cit note 75 at 1.

[616] Ibid.

[617] Ibid

retention, dissemination, and use of their personal information.[618] In relation to transborder data flows, the Preamble to the POPI Act states that it regulates the flow of information:[619]

> *'[C]onsonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information.'*

Moreover, the POPI Act also provides for private as well as public enforcement of its provisions.[620]

4. TERRITORIAL SCOPE

The territorial scope of the POPI Act is addressed in section 3(1)*(b)* and applies to the processing of personal information, 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.'*

This provision determines the applicability of the POPI Act based on a distinction between responsible parties domiciled and not domiciled in the Republic.[621] The recourse to the use of automated or non-automated means 'in the Republic' suggests a territorial approach since a connection to the territory of the Republic of South Africa is required in all cases.[622] As deduced from this provision, processing activity must regularly be connected to the territory of South Africa to apply the POPI Act. As Jonas Baumann and Nazreen Ismail rightfully argue, this is quite a challenging requirement as the processing of personal information nowadays

---

[618] Preamble of the POPI Act. See also Pamela Stein, 'South Africa's EU-style Data Protection Law' (2012) 48 *Without Prejudice* 48-49 at 48.

[619] Stanley 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* 1-20 at 8.

[620] Jonas Baumann and Nazreen Ismail 'The concept of "personal information" in the Protection of Personal Information Act 4 of 2013 – a comparative analysis from a European perspective' (2021) 3 *TSAR* 718-739 at 719.

[621] Jonas Baumann op cit note 528 at 30.

[622] Ibid.

crosses borders easily via the internet and by using other technological means such as cloud services.[623]

Jonas Baumann and Nazreen have further observed that in the Law Reform Commission's findings on the reform of South Africa's data privacy law, this regulatory approach was not considered in detail.[624] Nonetheless, the SALRC's proposed legislation embraced the regulatory framework established under Section 3(1)*(b)* of the POPI Act.[625] This approach is related to the regulatory notion of Article 4(1)*(a)* and *(c)* of the DPD, which had similar provisions and essentially followed the territoriality principle.[626]

In cases where the responsible party is not domiciled within the Republic, the POPI Act applies by virtue of section 3(1)*(b)(ii)* when such a responsible party makes use of automated or non-automated means in the Republic. The POPI Act's technology-neutral approach to regulation is shown by the fact that the Act covers both automated and non-automated ways of processing.[627] The distinction between automated and non-automated means was recommended by the Law Reform Commission based on the concept of Article 3 DPD to address electronic and digital means of processing. It is important to note that the genesis of this provision, as well as POPI Act, is Article 4(1)*(c)* of the European Union DPD 1995, which was replaced by the GDPR.[628]

In the interpretation of this provision, the 'means' referred to in this provision are presumably used to either enter the personal information into a record or process the personal information. An interpretation based on the wording of section 3(1)*(b)(ii)* of the POPIA could, therefore, extend the (extra)territorial scope significantly, since every processing, even by devices of the data subjects located in the Republic, would lead to the application of the POPIA. In section 3(4) of the POPI Act, automated means are defined as 'any equipment capable of operating automatically in response to instructions given for the purpose of processing

[623] Ibid.

[624] Ibid at page 31.

[625] Ibid.

[626] Ibid.

[627] Ibid.

[628] See text of the former EU DPD *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046* last accessed on (16 August 2022).

information.' In this context, the POPI Act does not provide further guidance on the extent of the meaning of 'automated' means besides the highly abstract definition in section 3(4).[629]

At first glance, the POPI Act appears promising in protecting the rights to privacy of data subjects, even in the face of emerging technologies. It endorses a technology-neutral approach. However, the GDPR's Article 3(2), which covers third-generation rights, has been omitted, leaving out the new key elements from the POPI Act. The POPI Act's jurisdictional reach is territorial, like article 2 of the Namibian Data Protection Bill.[630] Both instruments lack provisions to protect citizens when goods or services are offered, or behaviour is monitored by data owners who are not based in their respective territories. Article 4 of the DPD on which Section 3 of the POPI Act is based, presented problems due to its jurisdictional limits. The POPI Act stands to face practical problems when regulating a non-domiciled data processor.[631]

5. EX ANTE ADEQUACY REQUIREMENT

Transfers of personal information outside of South Africa or transnational information flows are covered by section 72 of POPI. In essence, it states that unless certain safeguards are in place, a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country. The South African legal default position includes ex-ante adequacy requirements, just like the EU. Among other things, Section 72 declares that: 'a *responsible party in the Republic may not transfer personal information about a data subject to a third party unless it provides for adequate protection.'*

6. CONCLUSION

The POPI Act outlines how personal data may be processed. Importantly, the POPI Act gives effect to section 14 of the South African Constitution on the right to privacy. The POPI Act's TBDF (territorial scope and adequacy requirements) provisions are modelled after the EU DPD. However, the EU's DPD has been superseded by the GDPR. The GDPR introduces novel aspects necessary to ensure the comprehensive protection of data subjects. One of the novel aspects is Article 3(2) of the GDPR. Its goal is to make sure that data protection follows the data wherever it goes in the digital age.

---

[629] Last accessed from *https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf* last accessed on 16 August 2022.

[630] Jonas Baumann op cit note 528 at 31ff.

[631] Ibid.

Regrettably, South Africa could only offer minimal guidance despite its jurisprudence being more mature. Regardless, the lesson is to flag issues of this nature earlier in the legislative drafting process. Amending a law takes far longer than resolving all gaps before enactment. Although this study hoped for significant progress from South Africa in this area, Africa as a continent can nonetheless draw inspiration from other regional initiatives, like the EU. This means that there needs to be a balance between the need for TBDF and the need for better privacy protection.

CHAPTER 7

Summary, Conclusions and Recommendations

1. INTRODUCTION

This dissertation used a two-part theme to examine the Namibian Data Protection Bill (specifically TBDF provisions). The study started by outlining the regulatory typologies of the world's three most influential economies: the US, China, and the EU. Second, the dissertation focused on how to successfully regulate TBDF with the blurring of real and virtual worlds, where data crosses territorial borders with a click. Relating to the former, the dissertation argued for a holistic approach that strikes a balance between the individual's right to privacy and the economic imperatives of TBDF. In relation to the latter, the study focused on three primary instruments, namely, the OECD Guidelines, GDPR, and POPI Act. The comparative study sought to determine whether Namibia's Data Protection Bill matched up to these international standards.

The dissertation has shown that data protection laws seek to preserve privacy as a normative objective. [632] In chapter 1, it has been noted that national data protection texts, or travaux préparatoires, generally include privacy as one of their key goals.[633] Article 1 of both Convention No.108, the EU DPD of 1995, and the GDPR all stipulate that their objective is to safeguard the individual's basic right to privacy while allowing the free flow of data. Similarly, both the POPI Act and the Namibian Data Protection Bill's preamble refer to safeguarding the right to privacy. Other international instruments, like the OECD Guidelines, also put a lot of emphasis on the link between data protection and privacy.

The conventional argument for regulating TBDF is that if there were no constraints on the transfer of personal data to other countries for processing, storage, or usage, local data protection regimes would be compromised. Like how money gravitates toward tax havens, personal data may wind up in jurisdictions with the weakest or, more likely, no data protection rules. To extend the tax analogy, there may be no restriction on organisations creating 'data protection avoidance strategies' to facilitate the processing of personal information in data

[632] Maria Tzanou op cit note 31 at 24.

[633] Ibid.

havens. As a result, the difficulties of enforcing privacy regulations in foreign countries continue to threaten the original data protection principles' delicate balance, which was to guarantee privacy while stimulating data flow. This has rekindled skepticism over their capacity to safeguard customer data in an age of expanding digital footprints and data processing operations.

The evolution of society is of a dynamic nature, hence the difficulty of the law's keeping abreast with it.[634] New problems and new issues demand new solutions and new interpretations under changed circumstances.[635] A key premise of this dissertation is that data is the modern economy's sine qua non. With the advent of the fourth industrial revolution ('4IR'), interconnected processes of globalisation and rapid technological change, particularly the rise of networked technology, have significantly disrupted conventional business models.[636] This economic revolution has generated numerous new possibilities for the establishment of innovative corporate models, and disruptive technology has become one of the most important engines driving the modern economy.[637]

This dissertation explored the difficulties in reconciling these important legal and policy objectives. It has been argued that the new economic and social reality has created multiple regulatory challenges for policymakers who are struggling to come to terms with its rapid pace. Conventional notions of jurisdictional scope tied to territorial borders are becoming increasingly obsolete. The paradigm shift in the socioeconomic environment necessitates reconfiguring and developing alternative perspectives on the plethora of regulatory challenges that the new innovation-driven global economy is presently creating. As Spiros Simitis has argued, "effectiveness of data protection law crucially depends on the ability to react in a fashion that focuses on concrete situations of processing, and the ones that are especially important from the perspective of the affected party."[638]

With that said, this chapter addresses the underlying question of whether the Namibian Data Protection Bill is likely to cure the ills suffered by data protection laws, which is being

[634] Last accessed from *http://law.uok.edu.in/Files/5ce6c765-c013-446c-b6ac* on 16 August 2022.

[635] Ibid.

[636] Marcelo Corrales op cit note 7 at 2.

[637] Ibid.

[638] Qouted in Paul Schwartz op cit note 271 at 352.

labelled as a ‘dead letter of the law’. The answer is a comparative analysis of how this issue has been handled in other countries, with reference to the OECD Guidelines, GDPR, and POPI Act. Maintaining the balance between cutting-edge technology by permitting the free flow of data and privacy should be a goal for every lawmaker. This chapter offers Namibia some general recommendations. It suggests improving the Namibian Data Protection Bill by learning from abroad. The proposals provided are made with the view of strengthening and improving Namibia’s data protection legislative framework.

In the following section, I will discuss the similarities and contrasts between the international instruments covered in the prior chapters. In this section, the Namibian Data Protection Bill is compared and contrasted with the OECD Guidelines, the GDPR, and the POPI Act to determine the degree to which the Namibian Data Protection Bill falls short of these global standards.

2. A COMPARATIVE STUDY OF THE SELECTED INTERNATIONAL INSTRUMENTS

This subsection presents an elaborate comparative analysis, primarily referencing four instruments: the OECD Guidelines, GDPR, POPI Act, and Namibian Data Protection Bill. The comparative analysis synthesises the matter and evaluates if the Namibian Data Protection Bill can withstand the pervasive and borderless internet. To allow detailed comparative analysis, the table below outlines the major characteristics of the three instruments governing TBDF and the Namibian Data Protection Bill. This research maps their relationships. In so doing, the analysis identifies the commonalities among the selected instruments that facilitate their intersection, whilst acknowledging their distinct approaches and aims.

The key aspects for the comparison are the extent of coverage, regulatory objectives, default legal position, and extraterritorial jurisdictions where products and services are offered, or behaviour is monitored. The next sections examine how much of the comparable instruments' wording is contained in the Namibian Data Protection Bill. The table classifies each instrument as first, second, or third generation depending on when its principles first emerged in international instruments.[639] The method of comparison employed in this section has been borrowed from Greenleaf. ‘First-generation’ standards are those in the OECD Guidelines and Convention 108, notes Greenleaf.[640] The EU DPD and Amending Protocol to

[639] Greenleaf op cit note 136 at 26.

[640] Ibid.

Convention 108 of 2001 are 'second generation' standards. 'Third generation' refers to the 2016 EU GDPR and the 2018 Convention 108+.[641]

Table 1: The Major Characteristics of the Three Instruments Governing TBDF and the Namibian Data Protection Bill

INSTRUMENT	EXTENT OF COVERAGE	REGULATORY OBJECTIVES	TBDF DEFAULT LEGAL POSITION	EXTRATERRITORIAL JURISDICTION, WHERE GOODS OR SERVICES OFFERED OR BEHAVIO MONITORED
DATA PROTECTION BILL: NAMIBIA (Based on 2nd Generation standards)	Omnibus legislative approach that applies to both public and private sector	Dual Objectives: Economic -Promotion of the free flow of data whilst protecting the right to privacy in terms of article 13 of the Namibian Constitution (preamble of the Data Protection Bill).	Ex Ante Regulatory Approach (Adequacy)-Free data flow within SADC and adequate States. An ex-ante adequacy determination verifies that nations satisfy certain standards prior to data export. In cases when an adequacy assessment has not yet been made, businesses may transfer data based on other alternatives like binding corporate rules, contractual clauses, and consent.	_
OECD GUIDELINES (First Generation)	Non-binding guidelines	Economic Objectives	Ex Post Regulatory Approach - Assume that data flows should be generally permitted but provide regulators with an option to block or restrict them under conditions. This is achieved by utilising a risk-based methodology. (Guideline 17)	_

[641] Ibid.

GDPR: EU (3rd Generation)	Omnibus legislative approach that applies to both public and private sector.	Dual objectives: Economic objective that promoted the free flow of data and a rights-based objective based on fundamental rights (Article 7 of the ECHR Provides for the Right to Data Protection)	Ex Ante Regulatory Approach (Adequacy)-Free data flow within the European Union and adequate States; trade policy promoting free data flows. (Article 45-47) An ex-ante adequacy determination verifies that nations satisfy certain standards prior to data export. In cases when an adequacy assessment has not yet been made, businesses may transfer data based on other alternatives like binding corporate rules, contractual clauses, and consent.	Article 3(2)- The GDPR, wil apply to a controller or proce not established in the EU, wi the processing activities are to: (a) the offering of goods services, irrespective of whe payment of the data subject i required, to such data subjec the EU; or (b) the monitorin behaviour of European citize (known as the targeting test)
POPI:SA (Based on 2nd Generation standards)	Omnibus legislative approach that applies to both public and private sector (Long title of the POPI Act)	Dual Objectives: Economic -Promotion of the free flow of data whilst protecting the right to privacy in terms of section 14 of the Constitution (Preamble of the POPI Act.	An ex-ante adequacy determination verifies that nations satisfy certain standards prior to data export. In cases when an adequacy assessment has not yet been made, businesses may transfer data based on other alternatives like binding corporate rules, contractual clauses, and consent.	_

The above comparisons enable the conclusions below to be drawn, some of which are as follows. All examined instruments, except for the OECD guidelines, share several key features. First, both the Namibian Data Protection Bill, the GDPR, and the POPI Act, provide for both private and public enforcement of their provisions. Second, all instruments aside from the OECD guidelines, which are based on economic goals, have two goals: to promote the free flow of data to benefit businesses (an economic goal) and to protect individuals' privacy (a rights-based goal).

The default legal position provisions in instruments under examination represent the third area of convergence (except for the OECD guidelines). Thus, the OECD Guidelines presume that data flow should generally be allowed but give regulators the power to block or limit it in certain circumstances, while others, notably the GDPR, the POPI Act, and the Namibian Data Protection Bill, proceed from the assumption that personal data may not flow outside the jurisdiction unless a particular legal basis is present, also known as ex-ante

adequacy requirements.[642] Ex-ante refers to a situation's view before it's constructed.[643] As an illustration, a law or regulation is an ex-ante act that governs circumstances after the text of a decision or general disposition is adopted by an authority.[644] An ex-post is the reaction of the law to a situation or conduct.[645]

By contrast, the Namibia Data Protection Bill seems to be congruent with other international legislation, especially European ones. Although the international standards' original 'fundamental principles' have been retained in the Namibian Data Protection Bill, the additional salient components added by the GDPR in Article 3(2) have been left out. Thus, the Bill encompasses several second-generation DPD aspects but not the third-generation GDPR requirements.[646] South Africa's POPI Act is similarly dismal; like Namibia's, it is lagging. This is despite having a matured jurisprudence on the right to privacy in comparison to Namibia. It is important to note that the European standards have been bolstered and are now more strigent.[647]

Drafts of the proposed GDPR were accessible in progressively trustworthy versions since 2012; these drafts could have influenced the Namibian Data Protection Bill. [648] Regrettably, that did not happen. Be that as it may, the progression of EU data protection legislation may be used to strengthen Namibia's bill. The GDPR clarifies rights and duties while improving compliance and enforcement.[649] The territorial reach has been expanded to promote internet trust, which is vital to economic growth. Lack of trust discourages online purchases and new service growth.[650] Moreover, these dangers hinder emerging technological

[642] Christopher Kuner op cit note 361 at 22.

[643] Last accessed from *https://mafr.fr/en/article/ex-ante-ex-post2/* on 18 August 2022.

[644] Ibid.

[645] Ibid.

[646] Greenleaf et al op cit note 136 at 82.

[647] Ibid.

[648] Ibid.

[649] Costa-Cabral et al op cit note 13 at 15.

[650] EU explanatory Memorandum op cit note 307 at 1.

innovations. [651] It is believed that the new approach could help resolve enforcement challenges caused by the borderless internet.[652]

As noted intermittently in this paper, the ever-evolving nature of technological innovations poses a threat to maintaining the delicate balance that the traditional data protection principles tried to preserve.[653] The resultant effect is an upshot in the level of skepticism regarding the ability of these legal instruments to protect consumers from exploitation, while at the same time allowing for the free flow of data. It should be a legislative priority to preserve this balance in the era of digital footprints. The resultant policies and regulations should promote the free flow of data while respecting human rights.

Contrary to this view, I have argued that data protection laws and the regulation of TBDF may be bolstered by enacting stronger legislation (like the GDPR) and implementing solutions that effectively embrace the 4IR. As countries grapple with the challenge of developing a dynamic information economy that respects fundamental rights, the recognition of this new salient feature in Article 3(2) of the GDPR would pave the way for a more coherent approach to data protection in a digital society.[654]

The following section will examine whether the Namibian Data Protection Bill alleviates the negative effects of being labelled as dead. The Namibian Data Protection Bill does not predate the GDPR, though being initially released in 2013, to date it has not been passed up to date.Therefore, it is still not too late to incorporate these new important features introduced by the GDPR with the aim of embracing the 4IR. Hence, as far as the GDPR established new concepts, this can be used as an orientation point for further developments of the Namibian Data Protection Bill de lege ferenda.

3. THE NAMIBIAN DATA PROTECTION LAW: A BITTER PILL TO SWALLOW?

Few areas of law, according to Svantesson, are as contentious as the law governing data privacy and few areas of law are as complex as the jurisdictional dilemmas arising from the

[651] Ibid.

[652] Ibid.

[653] Global Digital 4 at 5.

[654] Ibid.

internet.[655] It is no surprise that there will be difficulties when the two areas are combined.[656] As mentioned intermittently throughout this dissertation, the law tends to be territorially specific by its own nature. Transborder data flows, on the other hand, are a worldwide phenomenon that mocks legal jurisdiction, defies its efficacy, and tests the law's ability to keep up with growing ICT developments.

The continued efficacy of current regulatory approaches is being called into question by emerging technologies. This research seeks to address the issue concerning the territorial limitation found in Article 2 of the Namibian Data Protection Bill and stresses the practical consequences that emerge from this conundrum. It examined whether the Namibia Data Protection Bill is likely to cure ills suffered by data protection laws around the world; being labelled as the dead letter of the law. Furthermore, the Namibian Data Protection Bill's ability to withstand the challenges faced by data protection law owing to the borderless nature of the internet was analysed. To answer these two issues simply, the answer is no.

The first observation is that the bill does not apply to data processors who offer services, goods, and monitor the behaviour of Namibian citizens, but are not physically present in Namibia. Such an omission has failed to consider the realities of data processing activities in the 21st century. Notably, not too long ago, the data controller, the data subject, and the methods employed to process data were all physically situated in the same territory.[657] Today, data can be 'remotely processed' utilising cloud computing and other innovative technologies.[658] The rise of e-commerce, disruptive technologies, and shifting models of international companies have raised the relevance of global data processing and transmission.[659]

Another important observation is that the provisions of the Namibian Data Protection Bill create an asymmetry in regulatory treatment relating to the data processing by international processors who do not have means located in Namibia. The Data Protection Bill fails to make provision for data controllers who are not established in Namibia and who do

[655] Greenleaf et al op cit note 331 at 6.

[656] Ibid.

[657] Azzi op cit note 54 at par. 5ff.

[658] Ibid.

[659] Ibid.

not have processing 'means' located in Namibia but offer goods or services to Namibian consumers or monitor the behaviour of Namibian data subjects. This 'soft approach' amounts to unequal treatment and places domestic data processors at a competitive disadvantage vis-a-vis international data processors.

It is argued that, in its present form, the Data Protection Bill does not effectively govern TBDF. Article 2 of the Namibia Data Protection Bill is difficult to apply to organisations that handle Namibian citizens data but don't have 'means' located in Namibia. In the digital age, territorial-based jurisdiction is becoming less obvious.[660] According to Paul de Hert and others, personal data processing used to be simple: a data controller, a data processor, a data subject, and all the data processing means were in the same country.[661] A solitary legal framework applied to all processing activities.[662] Potential jurisdictional disputes were rare, and the territoriality concept adequately protected personal data.[663] In the 1980s and 1990s, when Convention 108 and the EU DPD were created, this sort of processing procedure dominated.

However, due to the widespread introduction and usage of the internet in modern times, the situation has been altered considerably.[664] In a short time, the techniques and technical means for processing personal data have become transnational, posing a significant problem for national lawmakers.[665] As indicated in Chapter 2 of this research, linking the application of Namibian data protection legislation to physical equipment usage no longer matches reality. Digitisation requires new standards for protecting privacy. It's no mystery that the internet generates complex jurisdictional challenges, compounding problems regarding the effectiveness of laws tied to territorial borders. In matters involving the internet, there remains considerable uncertainty about which regulations should apply: the rules of the nation of origin or the rules of the state 'targeted' by the online material.

As it has been noted intermittently in this paper, cloud computing, AI, IoT, and other forms of disruptive technologies threaten conventional data protection principles and its

[660] Paul de Hert et al op cit note 489 at 230.

[661] Ibid.

[662] Ibid.

[663] Ibid.

[664] Ibid.

[665] Ibid.

corresponding jurisdictional reach. Innovations such as cloud computing, AI and the internet of things challenge the traditional approaches to data protection jurisdictional reach. The IT sector is drifting away from the personal computer paradigm in favour of cloud computing since the latter provides several benefits over the former.[666] Businesses are transitioning from local to cloud computing due to the convenience that cloud computing provides.[667] For instance, the data is stored on a permanent basis and all files are backed up regularly, so the risk of data loss is low.[668] The 'cloud' can collect massive amounts of data and decrease users' need to invest in new physical IT infrastructure.[669] In addition, basic cloud computing services may be offered for free, generating revenue via consumer-targeted advertising. Facebook, WhatsApp, Twitter, etc. use this model.[670] Cloud computing's remote nature poses legal issues that need extraterritorial legislation.[671]

In its present form, the bill is a bitter pill to swallow, and the author anticipates bottleneck conundrums for the future regulator if its applicability remains connected to territorial borders. I believe that there is hope to turn this trend around. This comparative research demonstrates how to cure these ills. Following the GDPR, the Namibian Data Protection Bill could be the next iteration of legislation that puts consumers on par with big technology companies.

4. POSITIVE LESSONS FROM ABROAD: RECCOMENDATIONS

This dissertation focused on two key issues: first, can the law govern ICT in the realm of data protection? Second, how best can the law's concept of jurisdiction be effectively tailored in the context of data protection in a borderless world? The first leg has been answered in affirmative. In this paper, I have argued that the internet and any acts conducted on it should be subject to the same legal scrutiny as any other human endeavour.[672] The main focus of this

[666] Ibid.

[667] Ibid.

[668] Ibid.

[669] Ibid.

[670] Ibid.

[671] Ibid at 355.

[672] Ana Gascon Marcen,op cit note 42 at 413.

section is to address the second leg on how best the law can govern TBDF in a borderless world where data transcends national borders with a simple click.

This part argues for amending section 2 of the Namibia Data Protection Bill to align with GDPR Article 3(2). The Namibian legislature may keep the present Data Protection Bill, which confines the geographical scope to Namibia's border, but doing so might lead to legal uncertainty. Legal certainty assumes that the law is clear enough to allow legal subjects to control their own behaviour and prevent arbitrary government action.[673] The concept is a cornerstone of the rule of law.[674] Legal certainty is vital for setting normative expectations, allowing individuals to interact, and defining individual freedom and government authority in contemporary states.[675]

It has long been acknowledged that in order to successfully regulate TBDF in cyberspace, national laws must adopt long-arm statutes with purported extraterritorial application of one state's law in another territory.[676] The GDPR's new significant feature, as stated in Article 3(2), in particular, allows for extraterritoriality when data processors are not physically present in the EU. As a result, the EU may claim jurisdiction over foreign data processors by referencing Article 3(2). As it has been discussed now and then in this dissertation and much in greater detail in chapter 5, the jurisdictional limits of the EU DPD have created several botteneck conundrums for the EU regulator.

Therefore, the GDPR is the EU's response to the issues brought about by the outdated Data Protection Directive. To this end, the new salient elements of the GDPR provides for increased protection of personal data and privacy. Paul de Hert rightfully argues that this method, notwithstanding its drawbacks and hurdles of enforcement and individual rights, tackles one of the main problems EU data protection legislation has today, which is a lack of jurisdiction over third a country's data controllers' processing. This is of course, notwithstanding the fact that significant numbers of EU data subjects are handled by data controllers in a third country.

---

673 Mark Fenwick and Stefan Wrbka *The Shifting Meaning of Legal Certainty* (2016) at 1.

674 Ibid.

675 Ibid.

676 Kirby op cit note 62 at 233.

There are authors who welcome GDPR's new criteria as a 'revolutionary game changer' and emphasise the need to ensure effective protection, which the current author also supports.[677] Contrary to my views, some privacy and data protection scholars have criticized the concept of personal data and the adoption of long-arm statutes for becoming overly broad and impossible to enforce.[678] Article 3(2) is likely the most contentious, misunderstood, and baffling of all the GDPR requirements. Two schools of thought have since emerged. One for the proponents of the unavoidable extraterritoriality of data protection legislation, owing to the ubiquitous nature of the internet, and another school which seems to have embarked on the misguided and contentious notion of data protection law being dead. The latter school of thought stresses the difficulties concerning the enforceability of the EU's jurisdictional claim.[679]

Critics like Benjamin Greze have argued that the extra-territorial reach of the GDPR and, more particularly, Article 3(2) disregards the enforcement component.[680] Consequently, the most significant obstacle to the GDPR's extraterritorial application is the efficacy of its enforcement, which is essential to its success.[681] In this dissertation, I argue that while enforcement is often seen as the data protection law's Achilles heel, it is not completely ineffective.[682] I argue further that Namibia should, at this point in time, be allowed to learn from the GDPR despite its critics. This is due to two factors. First, the second school of thought's exposition, while having merit, is, in my opinion, somewhat premature at this point.

In fact, the GDPR has revolutionised the EU's privacy enforcement system, which is now considered a key element of the digital economy to boost user and consumer trust.[683] The first piece of evidence is the legal and centralised enforcement system for data protection in TBDF processing instances.[684] To date, the enforcement toolkit of EU data protection

[677] Graça Canto Moniz op cit note 543 at 106.

[678] Benhard Maier op cit note 94 at 227, Christoher Kuner op cit note 95 at 227ff and Lokke Moerel op cit note 96 at 46.

[679] Graça Canto Moniz op cit note 543 at 106f.

[680] Benjamin Greze op cit note 449 at 110.

[681] Ibid.

[682] Ibid.

[683] Ibid at 113.

[684] Ibid.

authorities has enabled the EU to successfully regulate the behaviour of non-EU organisations that process the personal data of EU individuals. To provide just a few examples, on January 6, 2022, Google Inc. in California, which is not located in the EU, was fined €60 million for having cookie settings on the YouTube website that did not comply with the GDPR.[685] Furthermore, on January 6, 2022, the French data protection authority issued Facebook the second-largest fine under the General Data Protection Regulation (GDPR), totalling €60 million. Due to its failure to properly get cookie consent from its users, the social media giant was fined €60 million.[686]

Second, the exposition fails to recognise contemporary alternatives to enforcement that are available.[687] Because of its novel and sophisticated nature, even though conventional methods of enforcement may not be completely effective for data processors who are not present in a country, there are alternatives to direct or indirect enforcement. To strengthen privacy protection, indirect enforcement would entail the collaboration of regulators among jurisdictions, and potential global sanctions against non-compliance. The possibility of utilising international cooperation agreements, like the agreement on mutual legal assistance, is mentioned by some authors.[688] The 2007 OECD Recommendation expressly acknowledges:

> *'Given that cross-border cooperation can be complex and resource-intensive, this recommendation is focused on cooperation with respect to those violations of laws protecting privacy that are most serious in nature. Important factors to consider include the nature of the violation, the magnitude of the harms or risk,s as well as the number of individuals affected.'*[689]

In the contemporary, interconnected world that we live in, I don't think this is impossible. Indeed, extraterritorial data protection laws are acknowledged by a number of jurisdictions as having the advantage of providing consistent treatment for local vis-à-vis overseas organisations despite enforcement challenges. These laws act as a deterrent for

---

685 Last accessed from *https://www.tessian.com/blog/biggest-gdpr-fines-2020/* on 02 September 2022.

686 Ibid.

687 Gömann op cit note 97 at 568.

688 Dan Jerker B. Svantesson op cit note 103 at 98.

689 OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam (2017) last accessed from *https://www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm* on 03 September 2022.

foreign companies from engaging in illegal processing.[690] As noted elsewhere in this paper, there is a quality to morally justifiable laws that cannot and should not be disregarded, even if they cannot be enforced.[691]

Notably, it is not unprecedented for a country to pass a law having an extraterritorial effect (or a 'long-arm statute'). It has been implemented by most nations, including Namibia. Conversely, the growing interdependence of markets and economies means that market participants' actions and the consequences of those actions frequently transcend the borders of the nation in which they are. For example, when devising remedies to remedy domestic competitive harm, competition laws often have extra-territorial reach (whether it is in mergers, abuse of dominance, or cartel conduct). Not surprisingly, the Namibian Competition Act of 2003 (Act No. 2 of 2003) belongs to this class as well. Section 3(1) allows for extraterritorial reach. It states, inter alia, that:

> '[T]his Act applies to all economic activity within Namibia or having an effect in Namibia.'

Appropriating legal solutions from other domains has been praised, and in this situation, competition law and data protection law share numerous crucial characteristics.[692] While their material scope and normative objectives differ in many ways, data protection law and competition law all have a global dimension that requires extraterritorial application.To this end, the drafters of the Namibian Data Protection Bill should consider adapting the 'targeting test' as provided for in Article 3(2) GDPR. It is recommended that section 2 of the Data Protection Bill be reworded as follows:

> *'This Act applies to the processing of personal data of data subjects who are in Namibia by a controller or processor not established in Namibia, where the processing activities are related to:*
>
> > *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Namibia; or*

[690] Ibid at 59.

[691] Ibid.

[692] Costa-Cabral et al op cit note 13 at 11.

(b) the monitoring of their behaviour as far as their behaviour takes place within Namibia.'

With that said, we should be mindful that there are undeniable benefits of considering these lessons at the beginning of the legislative process and incorporating them into the Data Protection Bill de lege ferenda. As the saying goes, 'a stitch in time saves nine'. The analogy is to mend a small rip versus sewing an entirely new seam.[693] All through time, even the greatest of legal systems had to regularly adapt to technological advancements and shifting societal norms. The danger of maintaining obsolete laws is that it causes anarchy and leaves individuals unprotected.[694] Consequently, the rewording of the data protection bill will reflect an important step in the right direction for improved and robust protection for individuals in the framework of personal data protection in a fluid technological environment. Moreover, today's increasingly connected planet and mass cross-border data flows warrant an alignment of the various national laws on data protection with international standards.[695]

5. CONCLUSION

The proliferation of digital industries since the 1970's focused on the debate over law and the internet.[696]With the continuous blurring of lines between the physical and virtual worlds, companies are turning to web-based business models, and consumers are purchasing goods and services over the internet.[697] Today, almost every kind of e-commerce requires vendors to store and send sensitive customer and business information across borders.[698] This allows them to monitor orders and stock levels for their international clientele, etc.[699] In the academic world, there is a general consensus that the growth and rise of pervasive technologies, which offer

[693] See also EDB Guidelines op cit note 86.

[694]Marina Škrinjar Vidović op cit note 116 at 203.

[695] OECD Guidelines op cit note 39.

[696] TBDF has been discussed in numerous forums, including the OECD, the UN, Unesco, the World Administrative Radio Conference and the International Telecommunication Union see Gisela Moohan et al op cit note 131 at 27.

[697] Paul Voigt et al op cit note 440 at 1.

[698]Neha Mishrahe 'Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?' (2017) 20 *Journal of International Economic Law* 31–60 at 36.

[699] Ibid.

new online services, often lead to legal ambiguities and regulatory bottlenecks that have never been seen before.[700]

TBDFs are vital for the global economy and an indispensable component for most businesses in today's digital era when most trade occurs online and across multiple jurisdictions. A thriving economy underpins stability and order.[701] For most businesses, data flows both within and outside a country's boundaries. In a perplexing way, this is both a huge benefit of the technological era and a major barrier to efficient regulation. As a rule of thumb, the absence of data protection laws influences nations' willingness to export data to countries without them. The ease with which electronic data moves across borders raises concerns that data protection rules might be evaded by moving personal information to other nations where the national legislation of the origin country does not apply. These 'data havens' may handle this data without limitation. Consequently, digital commerce cannot thrive without data protection laws.

The Namibian constitution protects privacy as a core, inherent human right under Article 13.Vision 2030, Namibia's long-term development strategy, promotes sophisticated ICT for socio-economic change.[702] However, without data and its unimpeded flow across national borders, Namibia should forget about any ICT-dependent societal transformation. The dissertation examined how to achieve both aims concurrently. The Data Protection Bill reconciles the two issues. Despite the Bill's many benefits, it can be improved. The focus of this research has been on how exactly these improvements will appear.

This research aimed to evaluate the Namibian Data Protection Bill against international data protection instruments, focusing on TBDF regulation. It has considered the difficulties created by the global dimension of data flows.[703] This is owing to the global reach of the communications networks through which personal data is presently collected, conveyed, and utilised, and consequently, the pervasive aspect that it's processing often assumes.[704]

[700]Marcelo Corrales et al op cit note 7 at 2.

[701] Jan Xavier Dhont op cit note 573 at 598.

[702] Vision 2030 document op cit note 23 at 31.

[703] Dário Moura et al op cit note 5 at 30.

[704] Ibid.

The collection covers novel technology. Cloud computing, big data, IoT, AI, cryptography, sensors, robots, and algorithms are examples.[705]

As noted in this research, cloud computing powers most of these technologies. However, cloud computing's increasing popularity undermines the effectiveness of laws tied to territorial borders. Personal data processing has become much bigger and more complicated because of how quickly technology is changing. This puts pressure on the original data protection principles, which were meant to support free data flow while protecting people's rights to privacy. This dissertation sought to determine the best approach to leverage cutting-edge technology while respecting customer privacy.

In the conventional model, the law is territorial and legitimised by a nation-state with physical borders.[706] A government has legal authority inside its borders.[707] However, globalisation and technology make this paradigm challenging to maintain. The internet, for instance, was formed as a decentralised network with no central authority and runs according to technology standards, not governmental laws.[708] The internet is un-territorial or post-territorial in the sense that no nation-state governs it.[709] However, states maintain the right to regulate online behaviour when individuals, corporations, or internet-using equipment are located on their territory.[710] Given that the internet is used all over the world and those laws are based on territory, it is inevitable that rules about how to act online will affect people in other countries.[711]

This dissertation argues that section 2 of the Namibia Data Protection Bill should be aligned with GDPR Article 3(2). To reiterate, the dissertation endorses the targeting test/market principle and calls for a wider territorial scope for two reasons. First, this would safeguard personal data everywhere it flows in a global era. In the second instance, it is argued that

[705] Ibid.

[706] John Quinn 'Geo-location technology: restricting access to online content without illegitimate extraterritorial effects' (2021) 11 *International Data Privacy Law* 294-306 at 294f.

[707] Ibid.

[708] Ibid.

[709] Ibid.

[710] Ibid.

[711] Ibid.

adopting the targeting test/market principle may be advantageous for future enforcement difficulties that might arise owing to the borderless internet. The new GDPR provisions appear well-positioned to cover certain gaps in the Data Protection Bill and may be considered as enhancing and reinforcing the present TBDF provisions of the Bill.

As I have argued in this chapter, the goal of this dissertation is not to open up a Pandora's box of regulatory overreaching and to introduce 'market-destroying measures'.[712] The goal is to reconfigure the Bill's current approach and to generate alternative viewpoints on the regulation of the emerging innovation-driven global economy. And one regulatory approach to consider in a redrafted Bill might be extending the territorial scope to incorporate the targeting test/market principle of the EU. When one thinks about how data processing works in the twenty-first century, this kind of extraterritorial application is second to none.

Despite enforcement challenges, it is my argument that such restrictions deter multinational corporations from illegal processing and give local businesses some equivalence with foreign businesses. In light of this, I wish to emphasise Svantesson's argument that 'morally justifiable legislation, even unenforceable laws, has a character that cannot be disregarded'. In any case, I'm sure that harmonising and aligning data protection laws would make it easier for law enforcement agencies from different countries to work together.

[712] Dan Jerker B. Svantesson op cit note 103 at 98.

BIBLIOGRAPHY

A

Abdulrauf L 'Data Protection in the Internet: South Africa' in Dário Moura Vincente and Sofia de Vasconcelos Casimiro (eds) *Data Protection in the Internet* (2020)

Amoo SK *Introduction to Namibian Law* (2008).

B

Bamberger K & Mulligan D 'Privacy in Europe: Initial Data on Governance Choices and Corporate Practices' (2013)85 *The George Washington Law Review* 1529-1664

Barkan M 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016)23 *Maastricht Journal of European and Comparative Law* 812-841

Baumann J & Ismail N 'The (Extra-)territorial Scope Rules of the New European Data Protection Law from a Private International Law Perspective—A Model for South Africa?' (2021)54 *Comparative and International Law Journal of Southern Africa* 1-49

Bendiek A & Römer M 'Externalizing Europe: the Global Effects of European Data Protection' (2019)21 *Digital Policy, Regulation and Governance* 32-43

Bennett S 'The Right to Be Forgotten: Reconciling EU and US Perspectives' (2012) 30 *Berkeley Journal of International Law* 161-195

Bergkamp L 'EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy' (2002)18 *Computer Law & Security* 31-47

Booysen H 'Succession to Delictual Liability: Namibian Precedent' (1991)24 *The Comparative and International Law Journal of Southern Africa* 204-214

Bougiakiotis E 'One law to rule them all? The reach of EU data protection law after the Google v CNIL case' (2021) 42 *Computer law & Security Review* 1-13

Breunig C & Martin S 'Data Protection in the Internet: National Report Germany' in Dário Moura Vicente and Sofi a de Vasconcelos Casimiro (Eds) *Data Protection in the Internet* (Springer 2020)

Burri M & Schar R 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing their Fitness in a Data Driven Economy' (2016)6 *Journal of Information and Policy* 479-511

Bygrave L *Data Privacy Law: An International Perspective* (2014)

Bygrave L 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000)16 *Computer Law and Security Review* 252-257

Bygrave L 'The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, mechanics and prospect' (2021)40 *Computer Law and Security Review* 1-13

C

Celeste E & Fabbrini F 'Competing Jurisdictions: Data Privacy Across the Borders' in Theo L, Mooney J, Van der Werff, L and Fox G *Data Privacy and Trust in Cloud Computing* (2021)

D

De Hert P & Czerniawski M 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context' (2016) 6 230-243.

De Hert P and Papakonstantinou M 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016)32 *Computer Law & Security review* 179–194

De Stadler E & Esselaar P *A Guide to the Protection of Personal Information Act* (2015)

Dhont J 'Schrems II. The EU Adequacy Regime in Existential Crisis?' (2019) 26 *Maastricht Journal of European and Comparative Law* 597-601

E

Cunha M *Market Integration through Data Protection: An Analysis of the Insurance and Financial Industries in the EU* (2013)

F

Fenwick E and Wrbka S *The Shifting Meaning of Legal Certainty* (2016)

Fishman W 'Introduction to Transborder Data Flows' (1980) 16 *Stanford Journal of International Law* 1-26

Francisco C & Lynskey O 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 *Common Market Law Review* 11-50

G

Gady F 'EU/U.S. Approaches to Data Privacy and the "Brussels Effect"': A Comparative Analysis', (2014) *Georgetown Journal of International Affairs* 12-23

Gaglione G 'The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America' (2019) *Buffalo Law Review* 1133-1212

Goldsmith J 'Against Cyberanarchy' (1998)65 *The University of Chicago Law Review* 1199-1249

Goldsmith J and Wu T *Who Controls the Internet?: Illusions of a Borderless World* (2016)

Gömann M 'The New Territorial Scope of EU Data Protection Law: Deconstructing a revolutionary achievement' (2017)54 *Common Market Law Review* 567 – 590.

Greenleaf G and Cottier B, 'Comparing African Data Privacy Laws: International, African and Regional Commitments' (2020)32 University of New South Wales Law Research Series 1-39

Greenleaf G 'Modernised Data Protection Convention 108+ and the GDPR' (2018) 154 Privacy Laws & Business International Report 1-3

Greze B 'The Extra-territorial Enforcement of the GDPR: a Genuine Issue and the Quest for Alternatives' (2019)9 *International Data Privacy Law* 109-128.

Guynes J, Guynes S & Thorn R 'Conquering International Boundaries that Restrict the Flow of Data' (1990) 6 *Information Strategy: The Executive's Journal* 27-32

H

Holland B 'The Failure of the Rule of Law in the Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty' (2005)24 *J. Marshall J. Computer & Info. L. 1* 1-34

Hoofnagle C, Van der Sloot B and Zuiderveen Borgesius 'The European Union General Data Protection Regulation: What it Is and What it Means' (2019)*28 Information & Communications Technology Law* 65–98

Huptchinson T & Duncan N 'Defining and Describing What We Do: Doctrinal Legal Research' (2012)17 *Deakin Law Review* 83–120

I

Islam T & Karim M 'Extraterritorial Application of the EU General Data Protection Regulation: An International Law Perspective' (2020)28 *IIUM Law Journal* 531-565

Ismail N and Lee Yong Cieh E *Beyond Data Protection: Strategic Case Studies and Practical Guidance* (2013)

J

Jamison S 'Creating a National Data Privacy Law for the United States' (2019)10 *Cybaris Intellectual Property Law Review* 1-41

K

Kirby M 'Legal Aspects of Transborder Data Flows' (1991) 11 *Computer Law Journal* 233-246

Kohl U *Jurisdiction and the Internet: Regulatory Competence Over Online Activity* (2007)

Kong L 'Data Protection and Transborder Data Flow in the European and Global Context', (2010)21 *The European Journal of International Law* 441-456

Koops B ‘The Trouble with European Data Protection Law’ (2014)4 *International Data Privacy Law* 1-14

Kugler L ‘Online Privacy: Regional Differences’ (2015)58 *Communications of the Association of Computing Machinery* 18-20

Kuner C ‘Data Protection Law and International Jurisdiction on the Internet (Part 2)’, (2010)18 *International Journal of Law and Information Technology* 227-247

Kuner C ‘Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future’ (2011)187 *OECD Digital Economy Papers* 1-40

Kuner C *Transborder Data Flows and Data Privacy* (2013)

L

Landau S ‘Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations’ (2014)12 *Institute of Electrical and Electronics Engineers Security & Privacy* 62-64

Levin A & Nicholson M ‘Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground’ (2005)2 *University of Ottawa Law & technology journal* 357-395

Lynskey O *The Foundations of EU Data Protection Law* (2015)

Lyon D *Surveillance Society: Monitoring Everyday Life* (2001)

M

McQuoid-Mason D ‘Invasion of Privacy: Common Law v. Constitutional Delict - Does It Make a Difference’ (2000) 2000 *Acta Juridica* 227-261

Mercer S ‘The Limitations of European Data Protection as a Model for Global Privacy Regulation’ (2020) 114 *American Journal of International Law Unbound* 20-25

Maier B ‘How Has the Law Attempted to Tackle the Borderless Nature of the Internet?’ (2010)18 *International Journal of Law and Information Technology* 161-162

Marcen A ‘The Extraterritorial Application of the European Union Data Protection Law’ (2019)23 *Spanish Yearbook of International Law* 413-425

Moerel L ‘The Long Arm of the EU Data Protection Law: Does the DPD Apply to the Processing of Personal Data of EU Citizens by Websites Worldwide?’ (2011)1 *International Data Privacy Law* 28–46

Moniz G ‘Finally: A Coherent Framework for the extraterritorial scope of EU data protection law’ (2018)4 *UNIO - EU Law Journal* 105-115

Moohan G, Morton E, Rimmer S, Romano & Burton P ‘Transborder Data Flow: A Review of Issues and Policies’ (2007) 37 *Library Review* 27-37

Mouzakiti F ‘Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive’ (2015) 1 *Europe Data Protection Law Review* 39-51

N

Namandje S *Privacy and Rationality Standard in Namibia* (2021)

Naude, A & Papadoulos S ‘Data Protection in South Africa: The Protection of Personal Information Act 4 2013 in light of recent international Developments’ (2016) 79 *Journal of Contemporary Roman-Dutch Law*1-18

Neethling J, Potgieter J & Anneliese Roos *Neethling on Personality* Rights (2019)

P

Pernot-Leplay E ‘China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U’ (2020)8 *Penn State Journal of Law and International Affairs* 49-67

Phillips M ‘International Data-sharing Norms: From the OECD to the General Data Protection Regulation (GDPR)’ (2018)137 *Human Genetics* 575–582

Poullet Y ‘Transborder Data Flows and Extraterritoriality: The European Position’ (2007) 2 *Journal of International Commercial Law and Technology* 141-153

R

Reed C *Making Laws of the Cyberspace* (2012)

Robert L and Stevenson, B, ‘Plugging the Phishing Hole: Legislation Versus Technology’ (2005)5 *Duke Law & Technology Review* 1-14

Rodotà S ‘Data Protection as Fundamental Human Right’ in S Gutwirth, Y Poullet, P De Hert, C de Terwangne, and S Nouwt (eds), *Reinventing Data Protection?* (2009)

Roos A ‘Data protection: Explaining the International Backdrop and Evaluating the Current South African Position’ (2007)124 *South African Law Journal* 400-436

Roos A ‘Personal Data Protection in New Zealand: Lessons for South Africa?’ (2008)11 *Potchefstroom Electronic Law Journal* 62-109

Roos A ‘The European Union’s General Data Protection Regulation (GDPR) and its implications for South Africa Data Privacy Law: An Evaluation of Selected ‘Content Principles’ (2020)53 *Comparative and International Law Journal of Southern Africa* 1-37

Roux T ‘Judging the Quality of Legal Research: A Qualified Response to the Demand for Greater Response to the Demand for Greater Methodological Rigor’ (2014)24 *Legal Education Review* 1-29

Rule J *Privacy in the Peril: How We Are Sacrificing a Fundamental Right for Security and Convenience* (2007)

S

Schwartz P ‘Global Data Privacy: The EU Way’ (2019)94 *New York University Law Review* 771-818

Schwartz P ‘Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology’ (2011)15 *William and Mary Law Review* 351- 387

Schwartz P ‘Privacy and Democracy in Cyberspace’ (1999)52 *Vanderbilt Law Review* 1609-1701

Schwartz P & Peifer K ‘Transatlantic Data Privacy Law’ (2017)106 *The Georgetown Law Journal* 123–27

Shaffer G ‘Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards’ (2000)25 *The Yale Journal of International Law* 27–28

Sullivan C ‘EU GDPR or APEC CBPR? A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era’ (2019)35 *Computer Law and Security Review* 380-397

Svantesson D ‘A Jurisprudential Justification for Extraterritoriality in (Private)International Law’ (2015) 13 *Santa Clara Journal of International Law* 1-56

Swales L ‘The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock’ (2022)25 *Potchefstroom Electronic Law Journal* 2-32

Svantesson D ‘Extraterritoriality in the EU Data Privacy Law: the Weak Spot Undermining the Regulation’ (2015)5 International Data Privacy Law 226-234

Svantesson D ‘The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses’ (2014) 50 *Stanford Journal of International Law* 55-99

T

Tamburri D ‘Design principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and its evaluation’ (2020)91 *Information Systems* 1-14

Thouvenin F ‘Informational Self-Determination: A Convincing Rationale for Data Protection Law?’ (2021)12 *Journal of Intellectual Property, Information Technology and Electronic Commerce* 246-256.

Tzanou M *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance* (2017)

V

Vidović M ‘EU Data Protection Reform: Challenges for Cloud Computing’ (2016)12 *Croation Yearbook of European Law and Policy* 171-206

Voigt P & Von dem Bussche A *The EU General Data Protection (GDPR): A Practical Guide* (2017)

Voss G ‘Obstacles to Transatlantic Harmonisation of Data Privacy Law in Context’ (2019)2 *Journal of Law* 405-463

W

Wacks R *Privacy and Press Freedom* (1995)

Wang P & Morris R ‘Cybersecurity Incident Handling: A Case Study of the Equifax Data Breach’ (2018)19 *Issues in Information Systems* 150-159

Waples, E. and Norris, D.M ‘Information Systems and Transborder Data Flow’ (1992)43 *Journal of Systems Managemen*t 43-55

Wayne M *Handbook of Personal Data Protection* (1992)

White A ‘Control of Transborder Data Flow: Reactions to the European Data Protection Directive’ (2014)5 *International Journal of Law and Technology* 230-247

Whitman J ‘The Two Western Cultures of Privacy: Dignity versus Liberty’ (2004) 113 *Yale Law Journal* 1151-1196

Z

Zalnieriute M ‘Transborder Data Flows and Data Privacy Law’ (2014)30 *Computer Law & Security Review* 104–108

Ziegeldorf H, Morchon O & Wehrle K ‘Privacy in the Internet of Things: Threats and Challenges’ (2014)7 *Security Communication Networks* 2728-2742

Zweigert and Kötz *An Introduction to Comparative Law* (1998)

Law Reform Papers

South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).

Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /* COM/2012/011 final - 2012/0011 (COD)

Unpublished Dissertation

Clever Mapaure Water Wars: Legal Pluralism and Hydropolitics in Namibian Water Law (unpublished dissertation of the University of Namibia, 2009)

Roos Anneliese 'The law of data (privacy) protection: a comparative and theoretical study'(Unpublished dissertation of the University of South Africa, 2009)

Naude Adrian 'Data Protection in South Africa: the Impact of the Protection of Personal Information Act and Recent International Developments' (unpublished dissertation of the University of Pretoria, 2015)

Internet Sources

Adèle Azzi 'The Challenges Faced by the Extraterritorial Scope of General Data Protection Regulation' available at *https://www.jipitec.eu*

Amoo Sam and Isabella Skeffers 'The Rule of Law in Namibia' available at *https://www.kas.de/c/document_library/*

Bender David 'GDPR Harmonisation: Reality or Myth?'(2018) available at *https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/*

Berkay Karadoga 'GDPR and Convention 108 Article', (2019) last accessed from *https://www.researchgate.net/publication/336512782*_GDPR_and_COnvention_108_Article

Business Software Alliance 'Cross-border Data Flows' (2017) Last accessed from *https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf*

Chander A & Ferracane M 'Regulating Cross-border Data Flows – Domestic Good Practices. In: Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence' (2019) last accessed from *http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.*

Cannataci J 'Report of the Special Rapporteur on the Right to Privacy' (2019) last accessed from *https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur*

Global Digital Partner 'Travel Guide to the Digital World: Data Protection for Human Rights Defenders', (2018) last accessed from *https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf*

Christopher Kuner 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2015) last accessed from *http://eprints.lse.ac.uk*

Geraldine Mwanza Geraldo and Isabella Skeffers 'Researching Namibian Law and the Legal System' (2007) last accessed from *https://www.nyulawglobal.org/globalex/Namibia.html*

Kuneva M 'Roundtable on Online Data Collection, Targeting and Profiling' (2009) last accessed from *http://europa.eu/rapid/press-release_SPEECH-09-156*

Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri 'Review of the European Data Protection Directive' (2009) last accessed *from https://www.researchgate.net/publication/*

Penny Pritzker and Andrus Ansip 'Making a Difference to the World's Digital Economy' (2016) *https://www.commerce.gov/news/blog/2016/03/making-difference-worlds- digital-economy-transatlantic-partnership*

Sasa Jovanovic 'Governing the Internet: The Extraterritorial Effects of the General Data Protection Regulation' (2020) last accessed from *https://digitalcommons.bowdoin.edu/honorsprojects/175*

Roger Clarke 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) last accessed from *http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html*

UNCTAD 'Cross-border data flows and development: For whom the data flow' (2021) last accessed from *https://unctad.org/webflyer/digital-economy-report-2021*

G20 Digital Economy Task Force 'Mapping Approaches to Data and Data Flows' last accessed from *https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf*

UNCTAD 'Value Creation and Capture Implications for Developing Countries' (2019) last accessed from *https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.*

Links F 'Tackling Cybersecurity/Crime in Namibia: Calling for a Human Rights Respecting Framework' (2018) last accessed from *https://ippr.org.na/publication/tackling-cybersecurity-crime-namibia*

Olivia B. Waxman ‘The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights: That Outlook Has a Disturbing History’ (2018) last accessed from *https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/*

The World Economic Forum ‘Information Technology Report’ (2016) *https://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/*

Namibian National Planning commission ‘Vision 2030 Report’*https://www.npc.gov.na/vision-2030/?wpfb_dl=36*

Shinovene Immanuel and Okeri Ngutjinazo ‘SSC Leak Exposes Personal Information Online’ (2018) *https://www.namibian.com.na/178310/archive-read/SSC-leak-exposes-personal-info-online*

Pria Chetty ‘Presentation of the Draft Data Protection Policy for Namibia’ *https://www.itu.int/en/ITU-D/Projects/ITU-EC CP/HIPSSA/Documents/Incountry%20support%20documents/Namibia_Data_Protection_Draft_Policy_Chetty_Version1.pdf*

OECD ‘OECD Privacy Framework’*https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf last*

https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet last accessed on

Legal Assistance Centre *https://www.lac.org.na/laws/annoSTAT/Namibian%20Constitution.pdf*

OECD *https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*

ASEAN ‘ASEAN Human Rights Declaration’ (2013)*https://asean.org/wp-content/uploads/2021/01/6_AHRD_Booklet.pdf*

The European Union ‘The History of the General Data Protection Legislation’ https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

OECD ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ (1980) http://www.oecd.org/general/listofoecdmembercountries-ratificationoftheconventionontheoecd.html

NAMIBIAN BILLS AND STATUTES

Data Protection Bill, 2013

INTERNATIONAL INSTRUMENTS

Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982)

African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 , 4 November 1950, ETS 5

Universal Declaration of Human Rights Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995

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 (General Data Protection Regulation)

International Covenant on Civil and Political Rights,16 December 1966, United Nations, Treaty Series, vol. 999

Electronic Communications Transactions Act No. 25 of 2002 (South Africa)

National Health Act 61 of 2002 (South Africa)

Consumer Protection Act 68 of 2008 (South Africa)

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted 23 September 1980

TABLE OF CASES

Namibian Case law
S v Acheson 1991 NR 1 (HC)

Kauesa v Minister of Home Affairs 1995 NR 175 (SC).

ES v AC 2015 (4) NR 921 (SC)

South African Case law
National Media Ltd v Jooste 1996 (3) SA 262

Bernstein & others v Bester NO & others 1996 (2) SA 751 (CC)

Ministry v Interim Medical and Dental Council of South Africa, 1998 (4) SA 1127 (CC)

AmaBhungane Centre for Investigative Journalism NPC & another v Minister of Justice and Correctional Services & others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC & others 2021 (3) SA 246 (CC)

European Case law

Renor v ACLU US 844, 851 (1997)

Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems Case C-311/18

A V Google New Zealand Ltd [2012] NZHC 2352 [4].

Yahoo!, Inc. v. LICRA 169 F. Supp. 2d 1181, 1186 (N.D. Cal. 2001).

Z. v. Finland (1998) 25 EHRR 371.

Biriuk v. Lithuania, no. 23373/03, judgments of 25 November 2008.

Maximillian Schrems v Data Protection Commissioner Case C-362/14.

Google Spain SL v. Agencia Espan˜ola de Proteccio´n de Datos (AEPD) Case C-131/12

Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána Joined Cases C-293 & C-594/12